Newcastle University

COMPUTING SCIENCE

A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions

Simon Parkin, Aad van Moorsel, Philip Inglesant and M. Angela Sasse

TECHNICAL REPORT SERIES

No. CS-TR-1209 **July 2010**

TECHNICAL REPORT SERIES

No. CS-TR-1209 **July, 2010**

A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions

S. Parkin, A. van Moorsel, P. Inglesant, M. A. Sasse

Abstract

Recent strides in usability research have produced various solutions to assist computer users during interactions with IT security mechanisms. However, the usability concerns of users within organisations are not considered or simply not apparent to the one individual who can effect change, the IT security manager. Ideally these concerns would resonate with the IT security manager, and here we explore how that can be realised, through the design of a password policy decision-support tool. During two 2-hour sessions, 3 IT security managers discussed with us our mock-up prototypes and a range of potential usage scenarios (e.g. cloud-based password-cracking attacks and "hot desking" initiatives). We find that the experience of the end-user is currently not appropriately represented within the IT security manager's decision-making process, where the financial costs/benefits and business impacts of information security controls are foremost. Our tool design process elicits findings to help develop mechanisms to visualise these tradeoffs.

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., VAN MOORSEL, A., INGLESANT, P., SASSE, M.A.

A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions
[By] S. Parkin, A.van Moorsel, P. Inglesant, M. A. Sasse
Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2010.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1209)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1209

Abstract

Recent strides in usability research have produced various solutions to assist computer users during interactions with IT security mechanisms. However, the usability concerns of users within organisations are not considered or simply not apparent to the one individual who can effect change, the IT security manager. Ideally these concerns would resonate with the IT security manager, and here we explore how that can be realised, through the design of a password policy decision-support tool. During two 2-hour sessions, 3 IT security managers discussed with us our mock-up prototypes and a range of potential usage scenarios (e.g. cloud-based password-cracking attacks and “hot desking” initiatives). We find that the experience of the end-user is currently not appropriately represented within the IT security manager’s decision-making process, where the financial costs/benefits and business impacts of information security controls are foremost. Our tool design process elicits findings to help develop mechanisms to visualise these tradeoffs.

About the authors

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.

Philip Inglesant is a post-doctoral research fellow in the Human Centred Systems Group in the Department of Computer Science at University College London (UCL). Previously, Philip worked on an EPSRC funded project in Grid security, Easy Expression of Authorisation Policies This is part of the PERMIS Project, an integrated infrastructure for Grid security. Philip completed his PhD studies at UCL in June, 2007. His thesis investigated the relationships between public policy and lived experience in HCI. Before that he did an MSc in New Media, Information and Society at the London School of Economics. Philip's first degree was in Mathematics at the University of Exeter.

M. Angela Sasse is the Professor of Human-Centred Technology and Head of Information Security Research in the Department of Computer Science at University College London (UCL). Angela read psychology in Germany and holds an M.Sc. in Occupational Psychology from Sheffield University, and a PhD in Computer Science (on Users' Models) from the University of Birmingham. Angela worked as a Human Factors Specialist for Philips Corporate Industrial Design in 1990, and started as Lecturer in the Department of Computer Science at UCL in November 1990. Since 1996, Angela has been researching usability issues of security systems, and published research on effectiveness and usability of authentication mechanisms, access control mechanisms, user attitudes and perceptions to computer security, and human and financial cost of security mechanisms.

Suggested keywords

INFORMATION SECURITY
USABILITY
SECURITY POLICIES
PASSWORDS

A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions

Simon Parkin
Newcastle University
School of Computing Science
Newcastle-upon-Tyne. NE1 7RU
+44 0191 222 7972
s.e.parkin@ncl.ac.uk

Aad van Moorsel
Newcastle University
School of Computing Science
Newcastle-upon-Tyne. NE1 7RU
+44 0191 222 7972
aad.vanmoorsel@ncl.ac.uk

Philip Inglesant
University College London
Department of Computer Science
Malet Place, London. WC1E 6BT
+44 20 7679 7214
p.inglesant@cs.ucl.ac.uk

M. Angela Sasse
University College London
Department of Computer Science
Malet Place, London. WC1E 6BT
+44 20 7679 7214
a.sasse@cs.ucl.ac.uk

ABSTRACT
Recent strides in usability research have produced various solutions to assist computer users during interactions with IT security mechanisms. However, the usability concerns of users within organisations are not considered or simply not apparent to the one individual who can effect change, the IT security manager. Ideally these concerns would resonate with the IT security manager, and here we explore how that can be realised, through the design of a password policy decision-support tool. During two 2-hour sessions, 3 IT security managers discussed with us our mock-up prototypes and a range of potential usage scenarios (e.g. cloud-based password-cracking attacks and "hot desking" initiatives). We find that the experience of the end-user is currently not appropriately represented within the IT security manager's decision-making process, where the financial costs/benefits and business impacts of information security controls are foremost. Our tool design process elicits findings to help develop mechanisms to visualise these tradeoffs.

Categories and Subject Descriptors
H.1.2 [**Models and Principles**]: Human/Machine Systems – *human factors, human information processing.* C.2.0 [**Computer Communication Networks**] General –*security and protection*

General Terms
Management, Security, Human Factors.

Keywords
Information security, usability, security policies, passwords

1. INTRODUCTION
Over the past 10 years, there has been a significant body of research focussed on improving the usability of security mechanisms (e.g. [23], [24], [25].

Some effort has been made to understand the nature of usability problems with existing authentication mechanisms, such as passwords - Adams & Sasse's "Users are not the Enemy" [6] detailed how users were struggling with the number and complexity of passwords, and the impact of these problems on their productivity and attitudes to security. Since then, significant effort has been dedicated to providing alternative, more usable authentication mechanisms ranging from graphical authentication mechanisms (e.g. [27], [29], [30]), to video authentication (e.g. [31]), and to more unusual forms of authentication through brainwaves [32] and singing at the computer [33]. On the commercial side, there has been significant investment in biometrics to replace passwords with authentication via fingerprints.

However, most of this research effort and commercial investment has made little difference in practice. In a recent study on password use in organisations [34] it was found that, 10 years after the "Users Are Not the Enemy" paper, little has changed: single sign-on is at best partially implemented, there are short timeouts on services leading to a need for frequent re-authentication, and users are still required to generate complex passwords without regard to how it addresses the real threats.

It is often the case that enforced password changes interrupt users at inconvenient times; the user expends time and effort to generate and learn a new password and, if single sign-on is not implemented, it is likely that the user will be delayed while the new password is propagated [34].

Even where single-sign on mechanisms exist, legacy systems and increasing use of 3rd party services mean that individual users still have a high number of passwords to cope with. The consequence of this reality is that users are forced to organise their primary tasks around the password mechanism. With the increase in e-commerce, web-mail and other online services, users now have even more passwords in use than 10 years ago. Florencio & Herley [36] found that, considering only web-based services, the average user has an average 25 web accounts – since users cope by re-using passwords across several accounts, they have an average of 6.5 passwords each.

Within organisations, interviews with security decision makers, conducted as part of the Trust Economics project [35] confirmed that the usability of security mechanisms, and any resulting impact on end-user productivity, is generally not considered when security policies are decided and security mechanisms chosen [7]. Cormac Herley [28] found that ignoring the costs to the *user* of complying with security advice is to "*treat the user's attention and effort as an unlimited resource. … Each piece of advice may carry benefit, but the burden is cumulative*".

Why is this so? Are those in charge of security in organisations still ignorant about the impact that security measures have on individuals? Do they know, but simply don't care about the impact that security policies have on users? Our research with those who decide information security policies – generally referred to here as Chief Security Information Officers (CISOs) – has established that this is not necessarily the case. Rather, they do not know how to apply research findings on the usability and economic impact of security measures when making a decision about a specific security policy or measure.

This led us to the notion of packaging and presenting knowledge of the impacts that security has upon users within a tool that CISOs can draw on during the security management decision-making process, to make more informed choices about the security mechanisms they deploy within their organisations.

CISOs need to justify policy decisions to senior managers and other stakeholders within the organisation and communicate their decisions in appropriate language. An example of a process modelling tool that provides an integrated treatment of usability and business process factors within information security management can be found in [10]. The modelling tool accounts for the risk mitigation achieved not only through a security policy, but also through consideration of usability and productivity. But the model is an abstract trade-off of investment and operating costs vs. risk mitigation achieved. To effectively support CISOs in their decision-making:

- the model needs to be populated with data on the cost and benefit of specific security measures, and
- there needs to be an interface that allows CISOs to explore the impact of security policies on their organisation, in an interactive fashion.

In this paper, we describe a prototype tool that provides an integrated security, usability and economic perspective of information security policy management through the design of a graphical user interface (GUI) for use by CISOs. The tool exposes the human-behavioural and economic implications of observable, measurable information security policy decisions during policy review and management, while grounding information in terms that resonate with CISOs. To ensure that the tool delivers these fundamental aspects, we arranged for a small group of CISOs to participate in a user-centred design process.

The remainder of the paper is arranged as follows: Section 2 examines existing information security procedures and related work. Section 3 describes the methodology and notable results of our CISO consultations. Section 4 then details the design of the tool as applied to an example of password composition policy. Discussion of issues uncovered by the tool design follow in Section 5, with concluding remarks and thoughts on future work closing the paper in Section 6.

2. BACKGROUND

A number of areas of research and commercial interest offer insights that are pertinent to the work described here.

2.1 Usability and Compliance

The impact of usability problems with security on individual and organisational productivity has been highlighted previously. One of the first investigations into usability problems with passwords was prompted by the escalating cost of helpdesks for password resets [6], and established the number and complexity of password policies as a cause. This early investigation also found that the difficulty users experienced reduced their willingness to comply - a finding confirmed in a more recent study [7].

In [7] a more formalised model was developed, linking the effort required to comply with security mechanisms to the level of compliance achieved. Herley [28] investigated the link between effort required to comply, and actual risk reduction achieved, and concluded that the fact that the decision taken by most users - not follow security advice – is rational from an economic point of view, because the effort required to follow those rules is not worth expending for the risk reduction achieved. Ignoring the real cost of users' attention and effort is a stance that does not work with external customers, and is even more untenable in a corporate context.

2.2 Human Aspects of Information Security

The use of checklists is generally no substitute for a thorough understanding of risk, as emphasised by the ISO 27001 standard **[40]**. Information security cannot be reduced to "box-ticking", and in particular, must take into account *perception* of risks by organizational members and their security-related *behaviour* [21].

It has long been recognised that security policies cannot be seen as simply technical measures; to achieve their business objectives, they must consider the organizational, cultural, technological, and human elements as a dynamically interconnecting system [15]. Security mechanisms which fail to take into account the impact on the business processes or the users' primary tasks are potentially unusable, and are likely to be circumvented by users, thus creating new vulnerabilities [21].

2.3 Usability of Security Interfaces

Usability is also central to the *interfaces* used to manage security. Whitten & Tygar [41] found that interfaces for security implementations are unusable, even by highly computer-literate users (based on a case study of PGP 5.0). Security mechanisms are therefore either unused, or worse still, used incorrectly and so fail to provide the intended protection.

If this is so for tools aimed at users in general, it is no less so for tools for security professionals. The importance of the usability of tools for security practitioners has been recognised, for example by [42], [12], [14]. However, perhaps because they focus more on policy implementers such as system administrators alongside policy-makers, this earlier research concentrates on those aspects – primarily technical – which are of concern to practitioners.

Nohlberg & Backström [5] investigate delivery of information security policy information to an organisation's upper-level management. The need to tailor pertinent decision-making information to intended users was considered, by way of interviews of potential users and scenario-driven design that contributed to a staged interface design. The nature of the intended users served to frame security from a financial and strategic perspective. We concentrate here on using interface design as a means to elicit CISO perspectives on the relationships between security, usability and economic factors.

Our aim is to go beyond providing a tool to support the ways that security professionals work *currently*, to encourage them to take a more holistic approach, considering the user costs as well as the benefits of security policies. Our tool must be usable for the CISO if it is to equally improve usability from the point of view of the people who are expected to *comply* with security policies.

2.4 Using Tools to Explore Options

In describing our interface as a *tool*, we emphasise that a tool places the user and their task at the centre: "*the tool itself seems to disappear*" [26] - the objects of interest are displayed such that the user remains in the "high level" semantic domain. The CISO acts *through* the interface on the objects of interest [39].

Although in a very different application area, our tool draws on visualisation as a way to enable exploration in a way which is inspired by the Homefinder tool [11]. The interface, using sliders and graphical output, allows users to explore the impact of changing one or more parameters of their decision-making.

Visualisation enables the exploration and understanding of complex interactions of variables [16]. As with other complex decision-making processes, humans are prone to conceptual or execution errors and to forgetting key items of information. Visualisation can help to avoid these classes of human error. In this case, the objects of interest are themselves relatively abstract concepts relating to parameters of security policy, so another design aim is that visualisation will help to concretise these concepts.

Finally, visualisations also support *communication* [16] of tool output, which is important for CISOs looking for support from other senior managers.

2.5 Modelling the Human Factor in Information Security within Organisations

A number of modelling tools have been developed to support information security professionals to articulate policies within their organisations and foster a holistic decision-making approach in light of the increasingly strategic role of the CISO.

An integrated approach to information security management incorporating human factors and economics principles has been demonstrated within previous research ([9], [10]), investigating the use of USB devices by employees. By characterising a user's working locations and the security threats to data on a USB device, the authors determined that improper use of USB devices can result in a mixture of increased business flexibility and potentially costly breaches.

Shay & Bertino [14] provide a simulation model for investigating trade-offs within technical and human factors of password policy for users. The model is framed by an end-user's perception of an IT environment, modelling their interactions with various services and associated user accounts. This allows the authors to characterise users' attempts to memorise passwords for various accounts while they remain vigilant for signs of suspected attacks upon those accounts. Formalisation of password policy attributes and associated costs to the organisation – such as helpdesk support – expose the relationship between end-user password usage and the economic impacts of a particular password policy. This work exposed the need to balance security and usability for user passwords, for instance in terms of password character complexity.

Beresnevichiene et al [17] augment the CISO's decision-making process with mathematical modelling tools. A structured process of problem elicitation leads to identification of a CISO's policy preferences and utility, in terms of breach prevention, assurance, and business performance. This thereby characterises competing objectives, which in turn informs creation of a model to investigate policy trade-offs. These mathematical system models combine system equations to relate business processes, environmental factors and use of resources. A case study considers the activities of users in a scenario centred around use of SLA-assured services by third party employees, including associated support services. Modelling results identify that CISOs can achieve comparable security outcomes by balancing a multitude of security and process controls.

The aim of the tool described in this paper is to encapsulate these research findings in a tool to support security decision-making.

3. CONSULTATIONS

To effectively augment the task of deciding information security policies, we must first understand the CISO's goals and tasks, and how these influence their decision-making. To develop this understanding, we consulted three information security managers. Two of these CISOs (who we will refer to as *C1* and *C2*) have a wealth of experience working for large multi-national organisations in the financial sector. CISO *C3* is in an information security management position at a leading UK university.

Although this is a small group, the range of viewpoints represented provided us with sufficient insight into CISOs goals, tasks and decision-making for us to build a prototype interface.

3.1 Methodology

We structured the CISO consultations so that we could relate the insights of individual CISOs across similar points of discussion, comparing responses to build a more detailed picture of the policy management process and how it may be enhanced by an appropriate policy management tool. The consultation process was conducted in two stages, as described here.

Both stages centred on paper-printed versions of prototype tool screens created in drawing software [37] – mock-ups - of our proposed CISO interaction tool, which we printed out in large scale. We printed these in large scale and encouraged participants to interact with these mock-ups in describing how they might use our tool to investigate the implications of various information security events.

3.1.1 Semi-structured requirements analysis

This first stage constituted an informal walkthrough of a preliminary tool design. The interdependencies that we investigate in this work have rarely (if ever) been adequately exposed before in a form with which CISOs can make policy decisions. With that, choosing to approach CISOs with a tool design provided something tangible to discuss with the CISOs, around which they could articulate their thoughts. The tool design was inspired by the functionality of a process model being developed in tandem within the Trust Economics project [35].

Within this initial consultation we also introduced some general decision-making scenarios within which CISOs could potentially use the tool, so as to identify appropriate functional boundaries and understand the environment that the tool could be used in.

3.1.2 Scenario-driven design

A second set of consultations with the same CISOs considered how a functioning instance of the tool would be applied. The initial meetings served to clarify how CISOs express the interdependencies that we consider in this work, and it was necessary to go further to examine how these interdependencies aligned with policy- and environment-specific attributes in well-defined usage scenarios (e.g. maintenance costs of IT systems, ease of changing existing policies).

At this stage, we focussed attention on the scenarios that were discussed with the CISOs. The intention was to expose interdependencies as they exist in practice, and examine how contributory factors may be formalised and quantified. Associated discussion facilitated investigation of how manipulating these factors could be seen to have both positive and negative impacts upon the functioning of the organisation in a given situation. This then provided insights into the effective exposure of these interdependencies to inform and augment existing CISO knowledge.

We structured pre- and in situ- prompts specific to each scenario, to (1) understand any existing thinking about the interdependencies, and (2) align exposure of the interdependencies within the tool with the policy decision-making process.

The scenarios we described to CISOs are specific to the management of password composition policies, and are included in Appendix A. A brief description and the purpose of each scenario are as follows:

1. "Password Cracking in the Cloud" (e.g. [22]): "How do policy choices affect the organisation?"
2. "Introduction of Hot-Desking": "How do working practices affect security?"
3. "Passwords vs. Fingerprints": "How are business cases formulated and supported?"

3.2 Analysis

The consultations with CISOs were voice- and video-recorded. The video recordings enabled us to capture interactions which CISOs were encouraged to make with the paper mockups.

The voice recordings were transcribed and analysed using a variation on Grounded Theory [19]. Initial line-by-line coding produced 349 basic open codes. These were gathered around 21 core codes; open codes and core codes were finally drawn together in groups of codes capturing thematic relationships.

For example, we developed three code groups on themes of: "About the CISO", "About Users", and "About Passwords" (since our initial study took password policy as its object of focus). "About the CISO" contained codes such as "CISO is not [mainly] technical" – the position of the CISO in an organisation – and "what matters to the CISO". "About Users" gathered codes which marked points in the consultations in which CISOs discussed our concept of classifying users into classes (see section 4.1).

Our analysis produced the following findings which have implications for the design of the tool.

3.2.1 The CISO's Concern is to Support the Business

Our CISOs were clear that their aim is not to impose security, but to support the business of the organisation. An important part of this role is in making arguments, or, more formally -business cases - for senior managers in an organisation. Senior decision-makers are not interested in technical details, but in the business implications of security policies and the threats they aim to mitigate. The business case made by the CISO, therefore, draws on technical knowledge, but the essential point of interest is the financial implications of any security-related intervention.

Security may in some cases have a low priority for the organisation [13], yet information security failures can cause stakeholders to question a company's operations [38].

Ideally, there would be evidence to support any proposed expense, presented in terms that both IT professionals and financial representatives would understand. Decisions would then be set in a broader context, and making security decision-making more inclusive.

In reaching a decision on an aspect of security policy, a CISO will weigh up each possibility, not just in terms of security, but the overall business impact: C2, referring to password policies: "[*the] CISO is also there to support the business. He wants to make it as easy as possible for the business to do its job. Make it easier for the users but increase the complexity. Need to present the options, and the business case, like you're doing here*".

Our tool aims to encourage CISOs to new ways of thinking about security. CISOs are highly experienced; they are aware of benchmarks and can make decisions based on their experience or discussions with other information security professionals. Nevertheless, existing "best practice" can be questioned, particularly in terms of the balance of costs and benefits. Our tool provides a sound evidence base, and, by encouraging exploration, enables CISOs to review their decisions: C2, referring to policy decisions: "*The journey is more important than the destination … you might actually change your mind.*"

3.2.2 Trade-offs

Decisions-making invariably includes trade-offs between various costs and benefits. In the specific case of password policy, trade-offs mentioned by our interviewees include:

- If passwords are required are too long or too complex, this makes them more secure from cracking, but conversely might force users to write them down as the only reliable coping mechanism (this point is supported by [34]).
- Users' ability to recall passwords - and therefore, to be less likely to write them down - is related to the expiry time of a password; users must have a meaningful length of time to learn the password before expiry.

Thus there are trade-offs between frequency of use, expiry time, password length, and complexity. Our interviewees spoke, for example, of increasing the length and complexity of passwords, but at the same time - to "give something back" to the password user - increasing the password expiry time.

3.2.3 Risk Management

Another clear finding from our interviews is that CISOs are engaged in risk management, rather than risk prevention at all costs ("*it's not the Crown Jewels*").

One participant argued that in consumer web applications, passwords are often used to protect low-value information - access to a newspaper or crossword. He said there are similar situations in commercial organisations – giving an example where he replaced password authentication to a company intranet with cookies on users' machines.

However, our interviewees were clear that for employees of an organisation, unlike the situation in e-commerce, different balances of costs and benefits apply in different contexts. There are cases in which a breach could lead to serious loss of reputation, or involve external legal or regulatory authorities, thereby incurring high costs for incident management. Moreover, in principle, employees can be required to conform to the organisation's policies. Enforcement carries costs in terms of employee goodwill, however, and overly strong policies impact on productivity – for example, in time taken to reset passwords.

Moreover, there is always uncertainty around the level of risk; in practice, it is never possible to identify the full implications of all security risks: C1: "*That's a Nirvana question. We will never be able to give an exact answer to "How secure are we? Do we need to be more secure?*". The best that can be attempted is to make reasonable estimates of key factors such as Annualised Loss Expectancy (ALE) [4].

3.2.4 Managing the Employees' Security Practices

A core aim of our tool is to ensure that an organisation's security policies are usable from the point of view of *those employees who are expected to conform to them*. For this reason, the CISO's view of organisation members and their security practices was of particular interest to us.

As we detail in sections 4.1.2 and 4.3.2, the underlying process model incorporates the concept of user *categories*, which vary in terms of amounts of time spent working in different locations, with associated security risks. Participants were generally favourable to this concept, but expressed the need to be able to parameterise the numbers and types of user classes. We discussed with them other possible properties of users, beyond location, in particular the different levels of access to valuable assets. However, we concluded from responses by CISOs that it would be impractical to link users classes to assets at this level of granularity; besides, it is rarely easy to identify the cause of a breach: C2: "*The difficulty is, any incident that causes ... [a] large fine is impossible to attribute to a weakness in the password polic*y".

Yet different kinds of employee do have different levels of access: in a university, for example, C3, referring to the potential for loss of a university's intellectual property, states: "*The biggest risk is staff, because students have limited access, no access to finance. On the other hand, the likelihood is more*".

Employees also have differing levels of motivation and commitment to the organisation. Our participants were divided on the question of the impact of productivity losses resulting from difficulties in conforming to password policies. For one participant, this productivity loss is not a real cost to the organisation, since motivated employees will simply work longer, if necessary, or reorganise their time to accommodate the delay: C1: "*[a retail call centre] might be concerned about productivity, ..., but not knowledge workers, who will just add time to their day*".

Based on previous literature [15, 21] we argue that attempts to enforce secure behaviour in employees must be balanced against loss of employee time and goodwill. A key part of the CISO's role is to encourage secure practices by all sectors of the workforce and promote a security culture. Enforcing unusable policies antagonises users and exhausts their willingness to comply, ultimately leading to rejection of security practices. We demonstrate through the tool that there is a balance between compliance management [7] and enforcement, and getting this balance wrong, paradoxically, reduces effective security. Our tool is a useful addition to the CISO's armoury in achieving this balance.

3.2.5 Summary of Results from Prior CISO Sessions

In supporting CISOs by illuminating possible trade-offs, helping them to manage risk, and supporting a security culture, our tool aims to support decision-making, rather than to be prescriptive. This is in keeping with the essentially exploratory nature of the underlying model; it is heuristic, not in the sense of "rule of thumb", but in the stricter sense of being a technique for problem-solving.

By providing an evidence base to support CISO decision-making, the wider aim, in our new paradigm, is to raise awareness of the costs as well as the benefits of security practices. Security requirements which are unusable incur hidden costs which are borne directly by the users and indirectly by the organisation. Our aim is to expose these costs and to show how they impact on the achievement of organisational goals.

3.3 Requirements

Based on our consultations with CISOs and a review of related work, the following requirements have been identified as necessary to improve policy decision-making in information security management:

- *Expose Interdependencies:* there is a need to represent the dependencies that exist between information security policies, human factors, and economic/business concerns:
    - Relationships between concepts must be captured in a more precise, quantitative manner to facilitate exposure of their interdependencies;
    - The relationships between well-defined human factors, economic factors and information security metrics should be related to the remit of the CISO.
- *Exploit Familiarity:* presentation of interdependent security, usability and economic expectations should be related to concerns that CISOs are familiar with.
- *Personalise Implications:* Each organisation is unique. Potential implications of policy decisions should be

made relevant to the individual organisation or they will not resonate with the CISO, who would in turn be unable to take suitably proportioned action.

- *Augment Experience:* any additional information for the purposes of decision-support should be presented to CISOs in a way that supports, but does not presume, the outcome of information security management decisions. CISOs should be encouraged to explore their policy options in a way that augments their existing wealth of knowledge.
- *Provide Clarity:* CISOs should only be presented with decision support technologies that they can readily understand.
- *Empower Communication:* CISOs should be able to generate evidence that can be communicated to other stakeholders (e.g. Human Resources, legal, IT) to gain support or facilitate negotiation of their proposed policy decisions.

The design of a policy composition tool should aim to address all of these requirements.

4. DESIGN

To satisfy the requirements identified in Section 3.3 we designed the Password Policy Composition Tool (PPCT), a prototype tool focusing on the management of password composition policies as applied to end-users with centralised IT system accounts. It is envisaged that such a tool could be used by CISOs to support them as they make decisions regarding information security policies. This interface tool envisages an internal systems modelling process, analogous to that detailed in [10], that must be communicated to CISOs in an appropriate manner. It also builds on previous attempts to integrate security and human factors into the policy implementation decision-making process [2].

The PPCT allows CISOs to configure core aspects of a provisional password policy to their own requirements, and to observe the quantified consequences of the policy management decisions that they may potentially commit to.

4.1 Password Policy Model

If the PPCT is to be useful to CISOs, it must allow them to configure relevant aspects of password composition policy and provide an informative representation of the potential consequences, with which they can make more informed policy management decisions.

The underlying model is built with the Gnosis modelling toolset [20][43], which aims to represent the security, usability and economic tradeoffs inherent in password composition policy, modelling policy implications projected over a fixed time-span. The behaviour of the model was informed by a combination of empirical data, existing literature, and expert knowledge. It is envisaged that such a model will operate within the PPCT, although for the purposes of our new paradigm, the actual implementation is not important.

CISOs might not necessarily consider how to articulate and communicate these interdependencies, and so a tangible representation proved useful for focusing discussion during the requirements-gathering and design consultation stages (Section 3).

4.1.1 Outline of the Password Usage Model

It is anticipated that users within the model move between different working locations over a predefined period of time, accessing password authentication systems at intervals to gain access to the organisation's IT systems and facilitate working with electronic information assets. Password authentication systems and the associated policy decisions are intended to limit a wide array of perceived information security threats within these various locations, instigated deliberately by malicious outsiders or colleagues. Interactions with the password authentication systems have the potential to secure or exacerbate access to IT systems. The organisation's IT systems and the associated authentication mechanisms are regarded as a single, centralised entity for simplicity.

The range of password-related security threats addressed in the model is limited to password cracking (e.g. dictionary, brute-force) and guessing ("shoulder-surfing", speculating). Whenever these threats manifest in the model, each instance may result in either of two distinct security breach events:

- Complete Password Capture (results in an unanticipated and fully-exploited breach)
- Partial Password Capture (where successive captures of the same password will eventually result in a Complete Capture, depending upon the attributes of the password policy)

Whenever a modelled user authenticates to the centralised IT system, one of five types of password authentication outcome is realised: "Authenticated"; "Unauthenticated"; "Failed" (due to e.g. forgetting a complex password; "Resetting password", or; "Locked out of account" (successive failed attempts).

4.1.2 Parameters in the Model

A limited (but representative) set of policy attributes and employee attributes are considered within the model. These properties are also exposed in the PPCT design:

- Four password policy controls:
    - Mandated minimum password length
    - Mandated password character-set composition
    - Mandated password frequency of change
    - Period of notification for employees before mandated password change
    - Number of permitted authentication attempts before account lockout
- Three (default) classes of employee using passwords to access organisation IT systems:
    - *Executive:* works mostly in the office, but also at home, with access to highly valuable information assets.
    - *Road Warrior (i.e. consultant):* typically in transit between locations, but also works in potentially insecure public places.
    - *Office Worker:* works only in an office environment, making up the majority of the organisation's workforce. May be subject to attacks by industrial spies etc.

- For each class of employee we represent 4 working locations from which authentication systems can be accessed (Office, Public, Home, In Transit).

The model informs IT security management decisions by providing a simple representation of the balance between account breaches, end-user productivity loss and running costs (e.g. salaried time lost to security administration activities such as resetting a locked account) resulting from enacted policies within the modelled threat environment.

4.2 Overview of the PPCT Interface

Configuration of any underlying password policy model should be obscured within the PPCT. Management of the model must not put undue expectations upon a CISO to interact directly with unfamiliar model technology and terminology. We herein examine the usability requirements of CISOs in terms of:

- Communicating to a CISO a range of security, productivity and economic factors and how they are interlinked.
- Supporting a CISO in making decisions about potential password policies, using the configuration and output of the underlying model as evidence in decision-making.

Consultations with CISOs encouraged the need to support CISOs during the policy decision-making process, e.g. *C1: "giving them a menu of things to tweak would actually prompt them thinking", C2: "the thinking of the CISO is going to be shaped by the process of going through this".*

The Password Policy Composition Tool (PPCT) design exposes policy-relevant details to CISOs, supporting exploration of the consequences of decisions within a limited view of information security specific to password policy management.

The PPCT is driven by configurable controls that correspond to policy management decisions. In practice these controls would be linked to an executable model – or pre-populated table of model results – to give direct feedback on the security, productivity and economic effectiveness of the tool over a projected period of deployment.

4.3 Configuration Properties

Within the PPCT design three distinct and interdependent groups of properties can be configured (as in the lower portion of Figure 1), each with their own separate tab in the configuration section of the interface:

- *(Security) Policy Properties:* identifiable, quantified password policy controls (Section 4.3.1).
- *User Properties:* different classes of employees come into contact with an organisation's IT systems within a range of working locations as part of differing working patterns. Configuring representative properties can help to generate results that inform how a prospective security policy would affect a real working environment (Section 4.3.2).
- *Support Properties:* these represent services within the organisation that support working patterns and policy associated with use of password authentication systems (Section 4.3.3).

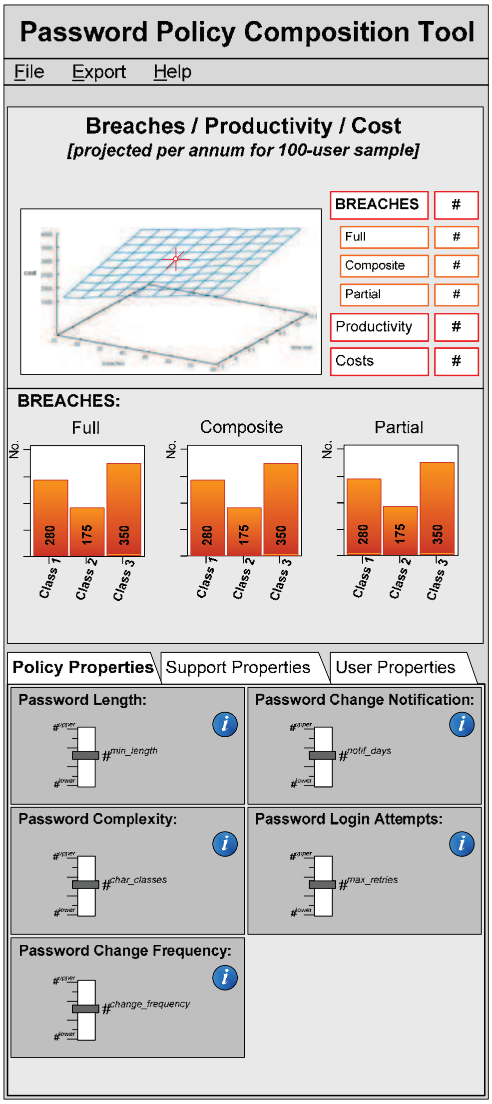

Figure 1. CISO Password Policy Composition Tool (PPCT) Interface (showing the "Policy Properties" view and "Breaches" output)

Note that the "Policy Properties" are aspects of information security policy that a CISO typically has the authority to change (within reason). "User Properties" and "Support Properties" aren't necessarily under the control of the CISO, but are nonetheless characteristics of the organisation that can have an effect upon the security posture of the organisation.

Dividing related organisation properties into these distinct groups provides a framework within which a CISO can understand the stakeholders affecting and affected by the security decisions they make. By changing interface controls in each of these groups and observing the results, a CISO can begin to relate observable changes in their provisional policies and the organisation around them to the security posture of the organisation's IT infrastructure.

By presenting quantifiable values for the various controls and model outputs (Section 4.4), the PPCT promotes evidence-based information security policy decisions and accountability. The proposed ability to export model configuration parameters and output results to an external file would facilitate the provision of supporting evidence when discussing potential decisions with other stakeholders in the organisation. That is not to exclude the possibility that many stakeholders including the CISO could operate the interface directly at the same time in a workshop setting.

4.3.1 Policy properties

CISO-defined "Policy Properties" may come in many forms (e.g. changes in variable controls, application or removal of "active or inactive" controls). Here we focus on quantifiable properties of information assets or security devices that can be varied across a discrete range of values, e.g. the "minimum password length" for end-user passwords across the organisation.

The policy controls are presented as "sliders" (as seen in Figure 1). This simple mechanism promotes investigation of policy measures across scales of increasing or decreasing security along different components of policy (e.g. "minimum password length", "password complexity"). This approach also encourages CISOs to consider the manner in which policy effects changes based upon alterations to individual policy controls. Associating related controls in the same panel also conveys that policy controls are at times co-dependent or may be altered in tandem to achieve varying effects. For instance, given a particular PPCT configuration a user of the interface may find that a one-character increase in "minimum password length" contributes more to the potential loss of end-user productivity than a 30-day decrease in the "password change frequency".

"Additional Information" accompanying each "Policy Property" control (the round blue "*i*" icons) can be used to provide information about the threats and vulnerabilities that each "Policy Property" should be used to address. These hints can also indicate any specific guidelines or regulations that the control addresses (e.g. "ISO 11.3.1d").

Additional information then serves to educate novice CISOs as to the situations within which to use a given policy control. It can also be used to structure the accountability process, highlighting where a control applies to a specific industry mandate or recommendation (e.g. minimum required password length) Such information may be stored in an ontology (e.g. [1]), populated either by the industry or internally within individual organisation using external tools (e.g. [2], [3]).

4.3.2 User properties

The "User Properties" tab (Figure 2) facilitates definition of organisation properties that relate to a proportioned sample of the different classes of end-user interacting with centralised authentication systems within an organisation.

Some of the content described in Figure 2 is highly sensitive (e.g. salary information). It is therefore important that the tool itself does not create a security vulnerability. As such the tool prompts the CISO for relative "proxy" salaries for each user class, making it unnecessary to retain sensitive information about actual salaries *(C2: "Have a sliding scale for salaries. Where you can get accurate data, show it, otherwise indicate an approximation")*. In turn such data may only be accessible by e.g. the organisation's human resources function. A similar approach of switching between absolute and relative numbers can be used where appropriate to define the distribution of users within the modelled system.

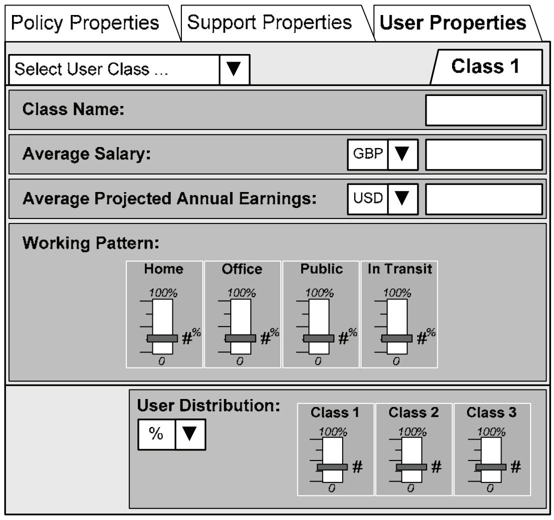

Figure 2: The PPCT Interface "User Properties" view

Salaries may be "banded" relative to each other, to remove the need to disclose salary information. Definition of projected earnings is optional, dependent upon the perceived value and working behaviour of individuals within a particular user class.

A CISO would not necessarily need to configure the User Properties, and can rely on the calibrated default controls within the underlying model (which form a consensus view of a generic organisation as agreed by human factors, information security and systems modelling experts, *C1: "if this is pre-populated with the average … this would be useful for CISO who's not doing it as a full-time role, who's not got lots of experience"*). However, should the CISO want to see tool output that is more applicable to their organisation, they are implicitly encouraged to gather relevant information, likely by communicating with relevant stakeholders in other departments.

4.3.3 Support properties

"Support Properties" (Figure 3) capture qualities of the organisation's support services which, although external to the password policy, may nonetheless impact upon its effectiveness. These "Support Properties" are primarily related to the one-off and ongoing costs of IT security policy decisions.

Specific to password policy, an organisation would ideally have helpdesk facilities of some description to address those instances where end-users need to activate, reset or unlock passwords/accounts. We make the simplifying assumption that there are helpdesk staff dedicated solely to answering password-related requests from staff. From our CISO consultations, the cost of running a helpdesk largely employed on password resets is one of the major security expenses: C2; "*In my experience, when we've tried to reduce costs, costs of running helpdesk is expensive"*, and escalating helpdesk costs were the motivation for the study conducted by Adams & Sasse [6]. But, as Adams &

Sasse found, these costs result from aspects of password policy; our tool will model these costs and expose them in ways that are clear to CISOs.

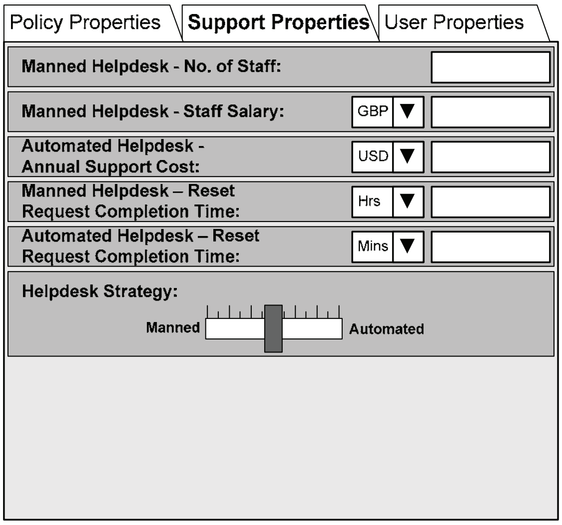

Figure 3: The PPCT Interface "Support Properties" view

Organisations are increasingly moving to the use of automated password resets, typically using pre-registered secret words; where such systems are in place, password users are encouraged to reset their passwords without the intervention of the staffed helpdesk. We model both automated and manual password resets, in proportions which can be adjusted by a slider on the interface.

Grouping "Support Properties" in this way gives a CISO a sense of how the infrastructure provisions within their organisation can ensure or threaten the success of an IT security policy. Conversely the CISO should appreciate that an effective security policy does not overburden other functions within the organisation without good reason (or in this context, good business sense).

4.4 PPCT Output

The tool presents the results of projected policy deployment as dictated by the controls described in Section 4.3. The output of the interface consists of:

- *Breaches:* the number of breaches that would occur as a result of the policy being deployed over a period of a year (the upper portion of Figure 1).
- *Productivity:* the total number of working hours lost over the simulated year across all of the user types defined as working within the organisation (Figure 4).
- *Costs:* a breakdown of the support costs (e.g. helpdesk staff) and projected losses of salary and potential earnings over the defined user classes (Figure 5).

The output of the tool is arranged in such a way that it allows a CISO to "drill down" from high-level results to more granular results (an approach encouraged by other investigations into IT security management tools [8]). Where results pertain to user behaviour, output data can be examined at a level specific to a particular user class. Varying levels of detail facilitate communication with other stakeholders according to levels of comprehension, but primarily support the CISO looking for particular categories of evidence to support their decisions (*C2: "People have a gut feel and look for confirmation"*).

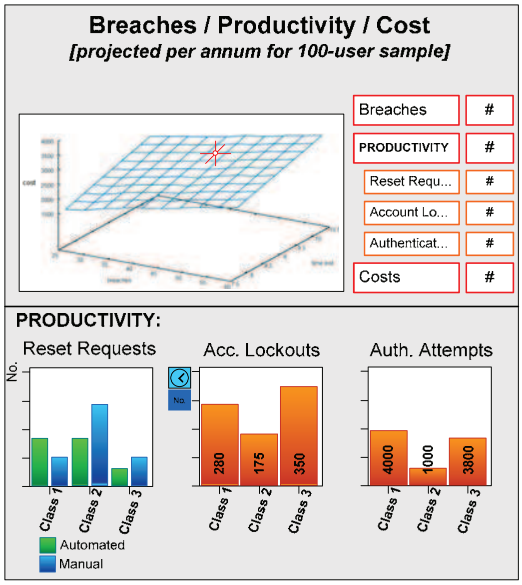

Figure 4: The PPCT Interface "productivity" modelling output

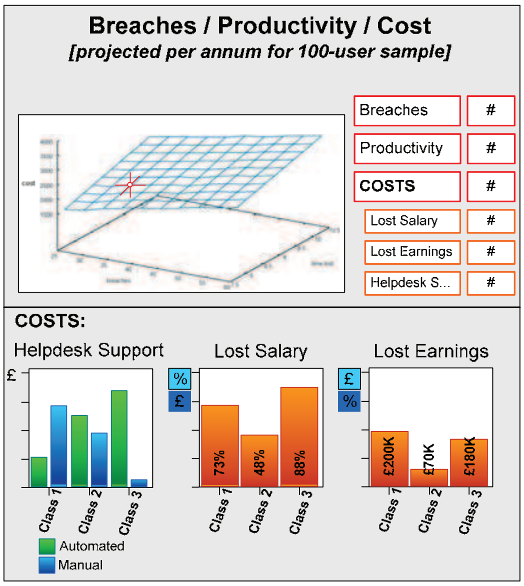

Figure 5: The PPCT Interface "costs" modelling output

The manner in which output is presented in the PPCT also promotes exploration of the "decision space". The top-level is an integrated treatment of breaches, productivity and costs, represented as a 3D plane. It is envisaged that a CISO would be able to examine output datasets across this plane to support speculative policy decision-making.

The consulted CISOs all suggested that the tool could be used to support a business case, wherein the tool's output is used to justify expenditure for further security programmes.

The intuitive correlation of the quantified properties of a provisional policy (properties represented in the control panels) to the quantifiable and identifiable consequences of that same policy (the tool output) promotes an approach of proportional security, and of articulating the effects of policy decisions *(C3: "I am only gut feel. I am only one person.")*. The effects of those decisions are communicated to a CISO with even sharper clarity with the facility to personalise many of the PPCT controls to a specific organisation, encouraging individual CISOs to understand the organisation around them not just in terms of security, but also usability and economic impacts (*C1: "Want a starter for 10, based on somebody's view, that can be tweaked. - naive vs. sophisticated user")*.

5. DISCUSSION

There are aspects of the tool design and the design process that warrant further discussion.

In the previous section we detailed the functionality and interfaces of our proposed tool. In section 3 we described the results of consultations which we undertook, using scenarios and paper prototypes of our proposed tool. Here we present implications of these findings for the design of the tool.

5.1 Tool Design

Broadly, the participating CISOs were very much in agreement that the functionality of the tool was adequate to expose the interdependencies between security provision, end-user capabilities, and the enablement of business processes. We do however accept that this was a small group of CISOs, and are open to reporting extensions or revisions to the tool and associated model both for and from further CISO consultations.

In particular all three CISOs were interested in the potential of the tool to make a business case – which they expressed as a major requirement (recall section 3.2.1). However, there were different approaches to decision-making, ranging from focused to more serendipitous. Our participants differed in how open they were to revising their initial decision in response to insights gained through exploration of the tool.

The finding that linking user classes directly to assets (section 3.2.4) is one example of a more general concern with an appropriate level of granularity. Participants particularly liked our suggestion (section 4.4) of enabling a CISO to "drill down" into the results, as a way of catering for different granularity requirements. Participants made a number of specific suggestions about how the interface could handle both data which is known with a high degree of accuracy and other input data known only in gross terms. For example, sliders, perhaps measuring simply percentiles, could be used to register approximate values, or actual numbers could be used where these are available.

5.2 Stakeholders

The representation of policy and environment attributes is key to the success of the tool in facilitating communication with other stakeholders in the organisation. The tool is designed so as to formally represent and relate these attributes, which serves to remove ambiguity. This may prove useful when presenting a case for IT security investment *(C3: "Often pitching to finance officer. IT often comes under finance … you've got to show what the risk is financially, to be taken seriously. In financial terms", C2: "Need to present the options, and the business case, like you're doing here.")*.

CISOs must communicate policies to other stakeholders (including department managers and employees) to achieve actionable security measures. It is also necessary to relay policies to external auditors, regulators and perhaps even shareholders. Thus, a CISO needs to be able to communicate both with technical implementers and with budget-holders and other decision-makers who do not understand the technical language of IT and security [38].

There may be a need to approach these other stakeholders within the design process to assess their expectations of security. For instance, potential breaches may result in per-event or per-record breach conditions which legal representatives would need to evaluate, as well as costs incurred for investigating particular kinds of breaches *(C1: "impact is not only value, also loss of reputation, legal impact, regulatory impact. E.g. could lose licence", C3: "Cost of breach can go through the roof, because of cost of accountants etc.")*. Our tool does not as yet model breaches with this level of granularity, as the "complete picture" of breach costs is informed by many parties, not just CISOs.

5.3 Decision-making Process

The tool design, and indeed the underlying model, may implicitly incorporate assumptions about how CISOs actually make policy decisions. Appropriate decision-making strategies should be supported, and doing so should also limit the cognitive effort required by users of the tool to analyse complex information [18]. In this sense our consultations identified factors in the CISO's decision-making process which we made efforts to support rather than supplant.

The output of the tool may be more useful if exposed in different ways, depending upon the background of the user. For instance breach results displayed over the projected lifetime of the policy would allow CISOs to identify temporal trends in user or system behaviour which are likely to impact upon the effectiveness of the organisation depending on when they are expected to occur. Exposing characteristics of the output throughout the model lifetime would add to the ability to "drill down" into the output to reveal further levels of detail.

5.4 Organisational Culture

We make no assumptions in the design of the tool about the working culture of the organisation that a CISO works in. For instance we do not consider application to specific industries *(C1: "utilities … not a lot of data worth stealing … so unlikely to steal password to get data, contrast with investment banking [where] risk of malicious tampering with data is lower")*. However, this could potentially be exposed through further analysis of the utility of security mechanisms, as embodied by a CISO's preferences for security, productivity or cost information.

The balance between the benefits (in terms of breaches avoided), support costs, and productivity losses, arising from security policy decisions, is made, in our underlying model, towards the end of the mathematical process, at which point the output from the model is applied to a utility function – see [10] for an explanation of how this is implemented in a similar model. The culture of the organisation – such as its risk aversion, the value of its assets, and the appetite for expenditure on security – could be reflected in our tool by adjusting coefficients of the utility function. We note this here as a possible future refinement for a working version of the tool.

The tool and the underlying model also make no assumptions about how people react to security mechanisms. For instance: *C1: "in banking people are motivated. Password might irritate people but won't cost people"*; *C3: "the more complex the passwords, the more people write them down. So there's a balancing act"*; *C3: "engineers, keen on IT, they do workarounds"*.

Also, for simplicity we assume that if a user is e.g. locked out of their IT system account due to a failed login, they are unable to do any work until the account is reinstated. This leads to discussion of the reliance on IT systems, and the technical capabilities and respect for policy according to end-users (as further discussed in [7]).

5.5 Instrumentation

Many of the parameters in the tool assume that the organisation's infrastructure has been instrumented to provide the necessary values (e.g. helpdesk call duration, etc.). However at present the activities of end-users and security mechanisms as represented by the tool are represented by a mixture of CISO opinion and unexposed model constants, and do not facilitate the submission of real monitoring data from relevant sources within the organisation. This is beyond the remit of this paper.

5.6 How the Tool might be used in Small and Large Organisations

While CISOs have rapidly become part of senior management of most large organisations, in small and medium-sized enterprises there are no dedicated positions for an information security specialist. For such organisations, the tool might be a repository of evidence which can partially overcome the lack of specialist skills. Conversely, larger organisations, with a dedicated CISO, might use the tool as a base which could be parameterised to reflect their actual situation.

Even in large organisations, it is unlikely to be possible to obtain accurate figures for all of the parameters in the model. However, this does not necessarily detract from its usefulness, since some parameters are likely to be insignificant in practice, while others - restricted data such as the costs per hour of different user classes, for example - can be expressed as gross figures in relative, rather than absolute, terms.

6. CONCLUSIONS

Chief Information Security Officers (CISOs) and other IT security managers are usually not aware of the effects that their security policies might have on the abilities of end-users within the organization to use IT mechanisms effectively. These security managers must cultivate an awareness of how end-user usability enters into the interdependencies between security provision, end-user usability and economic requirements within their organisation. We investigate the capacity to actively inform CISOs of these factors during IT security policy composition, by way of a prototype Password Policy Composition Tool (PPCT) user interface.

This tool facilitates exploration of changes to quantified password construction policy mandates, supporting services and end-user capabilities, providing feedback as to the impacts of these changes upon each other and the organisation as a whole. The usability of the tool is also considered, as it must support exploration of policy choices, provide clarity, and facilitate communication with stakeholders within the organisation.

Discussion and qualitative evaluation of the tool design by consulted CISOs demonstrate that it intuitively conveys elements of end-user usability, security and economic concerns within the information security policy decision-making process.

We intend to consult with additional CISOs to progress an implemented version of the tool. Any resultant implementation of the tool could be repackaged to cover not only password policy, but other aspects of information security with human and economic factors, such as endpoint and information asset protection policies.

It may also be conceivable to change the focus of the tool from CISO-oriented policy composition towards guiding end-users during password creation, thereby shifting the emphasis of the tool to security awareness and education.

7. ACKNOWLEDGMENTS

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").

We thank Adam Beautement (UCL), Simon Arnell, Brian Monahan, David Pym, Simon Shiu (all HP Labs), Hilary Johnson and Geoffrey Duggan (Bath University) for their comments on this work. We also thank our participating CISOs, who wish to remain anonymous.

We thank Brian Monahan and Simon Arnell (both HP Labs) for their contributions to the password model and associated development work with the Gnosis toolset.

8. REFERENCES

[1] S. Parkin, A. van Moorsel & R. Coles, "An Information Security Ontology Incorporating Human-Behavioral Implications", Proceedings of the 2nd International Conference on Security of Information and Networks (SIN), October 2009

[2] D. Stepanova, S. Parkin, and A. van Moorsel, "A Knowledge Base for Justified Information Security Decision-Making", Proceedings of the 4th International Conference on Software and Data Technologies (ICSOFT), July 2009

[3] J. Mace, S. Parkin, & A. van Moorsel, "Ontology Editing Tool for Information Security and Human Factors Experts", CS-TR No 1172, School of Computing Science, Newcastle University, Sep 2009

[4] B. Blakley, E. McDermott, D. E. Geer Jr., "Information Security is Information Risk Management", In Proc. 2001 Workshop on New Security Paradigms, 2001

[5] M. Nohlberg & J. Backström, "User-centred Security Applied to the Development of a Management Information System", Information Management & Computer Security, Vol. 15, No. 5, pp. 372-381, 2007

[6] A. Adams, M. A. Sasse, "Users are not the Enemy", Communications of the ACM, Volume: 42, Issue: 12, pp 40-46, 1999

[7] 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

[8] P. Jaferian, D. Botta, K. Hawkey, K. Besnosov, "Design Guidelines for IT Security Management Tools", SOUPS Workshop on IT Security Management (USM), 2008

[9] 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

[10] 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

[11] C. Williamson, B. Shneiderman, "The dynamic HomeFinder: evaluating dynamic queries in a real-estate information exploration system", Proceedings of the 15th annual international ACM SIGIR conference on Research and development in information retrieval, pp 338 – 346, 1992

[12] P. Jaferian, D. Botta, F. Raja, K. Hawkey, K. Beznosov, "Guidelines for Designing IT Security Management Tools", Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology, 2008

[13] R. Werlinger, K. Hawkey, and K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", Human Aspects of Information Security and Assurance (HAISA'08), Plymouth, UK, July 2008,.35-48.

[14] R. Shay & E. Bertino, "A Comprehensive Simulation Tool for the Analysis of Password Policies", International Journal of Information Security, 8:275-289, 2009

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

[16] R. K. E. Bellamy, T. Erickson, B. Fuller, W. A. Kellogg, R. Rosenbaum, J. C. Thomas, T. Vetting Wolf, "Seeing is believing: Designing visualizations for managing risk and compliance", IBM Systems Journal, VOL 46, NO 2, 2007

[17] Y. Beresnevichiene, D. Pym, and S. Shiu, "Decision Support for Systems Security Investment", To Appear, Proc. Of the 5th International Workshop on Business-driven IT Management, IEEE, 2010

[18] J. W. Payne, J. R. Bettman, and E. J. Johnson, "The Adaptive Decision Maker". New York: Cambridge University Press, 1993

[19] K. Charmaz, "Constructing Grounded Theory: A Practical Guide through Qualitative Analysis", Sage Publications, London UK, 2006

[20] Hewlett Packard Development Company, L.P., "A brief introduction to structured modelling with Core Gnosis", http://www.hpl.hp.com/research/systems_security/gnosis.html, 2010, last viewed 13/02/10

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

[22] Electric Alchemy Limited, "Cracking Passwords in the Cloud: Insights on Password Policies", http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html, last viewed 2002/10

[23] M.E. Zurko and R. T. Simon. "User-Centered Security", In Proc. 1996 Workshop on New Security Paradigms, 1996

[24] A. Whitten, J. D. Tygar, "Why Johnny can't encrypt: a usability evaluation of PGP 5.0". Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, 1999

[25] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link': A human/computer interaction approach to usable and effective security", BT Technology Journal, (19):122-131, 2001

[26] C. Rutkowski, "An Introduction to the Human Applications Standard Computer Interface: Part 1: Theory and Principles", Byte Vol 7, Number 10, (October 1982), 291-310

[27] R. Dhamija, A. Perrig, "Déjà Vu: a user study using images for authentication", Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, 2000

[28] C. Herley, "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users", In Proc. 2009 Workshop on New Security Paradigms, 2009

[29] S. Wiedenbeck, J. Waters, J.Birget, A. Brodskiy, N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, vol 63, 102–127, 2005

[30] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords", Proceedings of 28th international conference on Human factors in computing systems (CHI '10), Atlanta, GA, USA, April 2010, 1107-1110

[31] P. K. Atrey, W. Yan, M. S. Kankanhalli, "A Scalable Signature Scheme for Video Authentication", Multimedia Tools and Applications, Vol. 34:1, pp. 107-135, Springer, 2007

[32] J. Thorpe, P.C. v Oorschot, A. Somayaji, "Pass-thoughts: Authneticating with our Minds", In Proc. 2005 Workshop on New Security Paradigms, 2005

[33] M. Gibson, K. Renaud, M. Conrad, C. Maple, "Musipass: Authenticating me Softly with "My" Song", In Proc. 2009 Workshop on New Security Paradigms, 2009

[34] P.G. Inglesant, and M. A. Sasse, "The true cost of unusable password policies: password use in the wild", Proceedings of

28th international conference on Human factors in computing systems (CHI ‘10), 383-392

[35] Newcastle University, “Trust Economics Economically justified security investments”, http://www.trust-economics.org/, last viewed 15/04/10

[36] D. Florêncio, and C. Herley, “A Large-Scale Study of Web Password Habits” Proceedings of the 16th international conference on World Wide Web (WWW 2007), Banff, AB, Canada, May 2007

[37] C. M. Karat, C. Brodie, J. Karat, “Usability Design and Evaluation for Privacy and Security Solutions”, Ch 4, Security and Usability, O’Reilly, 2005

[38] R. Condon, “Got what it takes to be a CISO?”, Infosecurity,Vol 4 Issue 2 (March 2007), 30-32

[39] S. Bødker, “A Human Activity Approach to User Interfaces”, Human Computer Interaction, Vol 4, 171-195, 1989

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

[41] A. Whitten, J.D. Tygar, “Why Johnny Can’t Encrypt: a Usability Evaluation of PGP 5.0”, Proc. Of the 8th Conference on USENIX Security Symposium, 1999

[42] S. Chiasson, R. Biddle, and A. Somayaji, “Even Experts Deserve Usable Security: Design guidelines for security managements systems”, Workshop on Usable IT Security Management (USM ’07), held in conjunction with the Symposium on Usable Security and Privacy (SOUPS 2007), Pittsburgh, PA, USA, July 2007

[43] M. Collinson, B. Monahan, and D. Pym, “Semantics for Structured Systems Modelling and Simulation”, Proc. Simutools 2010, ACM Digital Library and EU Digital Library. ISBN: 78-963-9799-87-5.

Appendix A

A1. Scenario 1: Password Cracking in the Cloud

“A senior manager of your organisation has come to you having read an article claiming that password cracking attempts can be run within “cloud” computing environments, making it easier to find the financial and computational resources to brute-force attack a password.

The senior manager does not trust the precautions you have taken to protect the central password tables or passwords in transit between user workstations and the authentication systems. The senior manager then demands that you take action to strengthen the organisation’s employee account passwords from the threat of exposure through this “cloud cracking” method (with the assumption that such an attack can be tailored to target enterprise authentication systems).

From reading the article, you believe that in order to keep passwords safe from cracking using the “cloud” (at least for the foreseeable future), there are three password options available to protect your organisation from such an attack.

- If mandated passwords contain both lower-case letters and numerical characters, maintain a minimum mandated password length of 12 characters.
- If mandated passwords contain lower-case letters, upper-case letters and numerical characters, maintain a minimum mandated password length of 11 characters.
- If mandated passwords contain lower-case letters, upper-case letters, numerical characters and special characters, maintain a minimum mandated password length of 10 characters.

Your organisation currently mandates 8-character passwords consisting of lower-case letters and numerical characters, so any one of these suggested mitigations represents a potentially disruptive increase in security effort for staff.

Further information associated with the original article suggests that using cloud technologies, an 8-character password consisting of lower-case letters, upper-case letters and numerical characters may be cracked within 100 days. With this you may also wish to explore your options for the frequency with which staff have to change the passwords they use to access accounts on your organisation’s IT systems.

You must investigate the options available to you, while considering the effects upon staff productivity and supporting costs of increasing the effort they must expend to maintain the level of security you believe is appropriate.”

A2. Scenario 2: Effects of a Hot-Desking Policy on Password Policy

“The lease on your organisation’s HQ in Central London is coming to an end, and the leaseholder wants to significantly increase the rent. This has prompted your CEO to hire a Space Utilisation Consultancy to assess how well the available space is used. The consultancy’s report states that on average 37% of desks are not occupied during the hours of 9am-5pm.

Your CEO has calculated that your company can give up 3 of its 6 floors, saving the company £1.5 Million in rent p.a., and is determined that the company should achieve this through “hot desking” and by abolishing all meeting rooms (except for the board room). At the moment, the company has a traditional perimeter security, with no remote access to systems, except for sales staff, who are able to enter their sales into the company’s systems from home via a dedicated web service. A review conducted by the head of departments in HQ reveals that to achieve this, the company has to make the following changes:

- All sales staff (20) will no longer have any desk space in HQ. They will now exclusively work from home or access systems on-the-road. Apart from entering orders, this involves access to inventory and price information, quotations, customer databases.
- 75 employees who previously only could access systems from within HQ will now have to hot-desk and work from home. For informal meetings and/or when they need to be close to the office but no desks are available, they will have to use coffee shops close to HQ, using remote access systems. They will now have to share computers, instead of each having their own. 30% of the previously office-bound staff have said that

they will not be able to work from home and so they will have to use coffee shops or other public places near to their home or the office.

- The 5 board members will have to book space in meeting rooms for formal meetings in commercial centre, and access systems remotely to present relevant information.

Major stakeholders have been given a limited amount time to lodge any objections to the "hot desking" initiative. You are in a prime position to inform the CEO of any serious security implications that this initiative may introduce. As such you should be able to explore the security implications of these new working conditions and report to the CEO any findings that you think may influence their final decision."

A3. Scenario 3: "Password Authentication vs. Fingerprint Readers"

"A new fingerprint-reading technology has become available that is cheaper to purchase than previous incarnations. It may be worthwhile investigating the possibility of replacing your organisation's password authentication systems with this new biometric-based authentication system.

The cost of each fingerprint reader is still being negotiated, so you do not need to consider it in the model. The manufacturers have also mentioned the possibility of being able to negotiate discounts if the central fingerprinting system and associated employee fingerprint readers are bought in bulk for use across your entire organisation.

However, there are a number of issues to consider in deciding whether to purchase a completely new fingerprint authentication system for your organisation:

- There would be no requirement for staff to recall a password when authenticating to the IT systems. This might result in fewer helpdesk calls.
- Systems staff will have to visit every desktop computer in the organisation to install the fingerprint readers and associated software. You plan to do this on a rolling programme over 6 months. There are 2000 desktop computers in your organisation; assuming 2 staff people work weekends, each could do 5 per hour or 35 per day, 70 per weekend, equivalent to work spanning 28 weekends.
- All employees will have to enrol their fingerprints with the system. Existing staff will do this on the first working day following installation of a reader on their desktop computer. New staff will enrol on their first day of employment. This can usually be done by the employees on their own, but you expect that 25% of them will have problems doing this, requiring a visit from a member of the helpdesk staff.
- The fingerprint readers you are considering have a typical false negative rate of around 5%, and a failure rate of 10% per year, related to how accurately people were enrolled initially. This is analogous to the problem of users re-typing or forgetting their account password. If a password reader has failed and a member of staff cannot authenticate, that would require intervention by support staff to resolve any such issues. However, with fingerprint readers, all such faults are likely to require physical intervention by support staff, resulting in longer fault resolution times. There are then typical support costs and procedures associated with biometrics, just as there are for password authentication systems (in the form of automated or manned helpdesks).
- Fingerprint readers can suffer from false positives, where an operator of a fingerprint reader may be authenticated as someone else; these readers have a typical rate of around 1%. However, a targeted attack, for example using a silicone copy of a genuine fingerprint, could have a success rate of 5%. This is analogous to the threat of passwords being guessed, in that the authentication system believes the operator and the owner of the authenticated identity are one and the same (much like when someone else knows the "something you know" that constitutes a user's password).
- Employees with no one fixed working location will have to guarantee that any portable fingerprint readers they use (for instance as found in some makes of laptop) function correctly outside of the organisation's premises. Faults in authentication systems for biometrics have much greater implications than problems of passwords being forgotten. However the security benefits of using biometric authentication in public places over password authentication are obvious.

It is your responsibility to investigate whether your organisation should introduce a completely new fingerprint authentication system for all employees' IT accounts, replacing the existing password authentication system.

As part of this investigation it is worthwhile to consider whether the existing password authentication policy can be altered to give comparable security, productivity and cost advantages to those offered by the fingerprint system."