Trust Economics

A systematic approach to information security decision-making

Contents

Background

The Trust Economics project has been a collaborative research project involving both industrial and academic partners including Hewlett-Packard Laboratories in Bristol, National Grid, University College London, the University of Bath, and the University of Newcastle. Our focus has been on combining the fields of Economics, Mathematical Modelling, Information Security, and Cognitive Modelling to provided a more complete and systematic approach to information security decision-making.

David Pym (initially with HP Labs, later Aberdeen University) was the scientific lead for the project.

This work has been funded by the Technology Strategy Board, the UK's government-funded national innovation agency whose goal is to accelerate economic growth by stimulating and supporting business-led innovation. For further information please visit www.innovateuk.org.

Problem Description

With information technology underpinning and enabling an unprecedented range of business processes and activities investment in information security is critical for any organization. Decision-making in this context is, however, increasing in complexity and difficulty. Resources are limited and there are a variety of important stakeholders, each with their own level of knowledge, expertise and incentives. While security professionals may have the abilities required to manage this complexity effectively, that is only part of the story. Security decisions are not made in isolation and must also reflect the needs of the primary production goals of the organization being protected. With many information security decisions being made based on the personal experience and knowledge of the security manager, there is a challenge in communicating these choices effectively to the business leaders. The reverse is also true: the decisions of the business team may be just as opaque to the security professionals. Additionally, any decision will necessarily involve the consideration of a huge range of interdependent factors, if an accurate appraisal of its costs and benefits, as well as likely impacts and outcomes, is to take place. The key problems then faced by decision makers are:

- How to account for the full range of factors affecting the decision-making process and the trade-offs that exist between them?
- How to predict the outcomes of various implementation options?
- How to share the decision making process effectively between all relevant stakeholders, in particular the business and security managers?

Standard approaches to information security decision-making are insufficient to master these urgent challenges. Even experts find it difficult to trade off multiple variables simultaneously and routinely employ non-systematic techniques such as externalising cognition through use of written materials in an attempt to cope with the burden. The Trust Economics project however has developed a unique and ground-breaking approach that allowed us to effectively tackle these problems. Our goals were:

- To position information security decision making within an economic framework based on utility theory thus creating a shared language accessible to all stakeholders;
- Deploy human factors expertise to augment existing technical knowledge so that a fuller range of inputs and impacts can be included in the decision making process;
- Utilize mathematical systems modelling to create a systematic methodology for exploring the potential outcomes of various choices;
- Develop tools that support information security decision-making by incorporating the knowledge and expertise used in the above processes.

The approach is iterative and so can be used to develop a complete solution, including solving any problems created by the deployment of the initial security measures. Figure 1 shows the overall approach from security problem to system model.

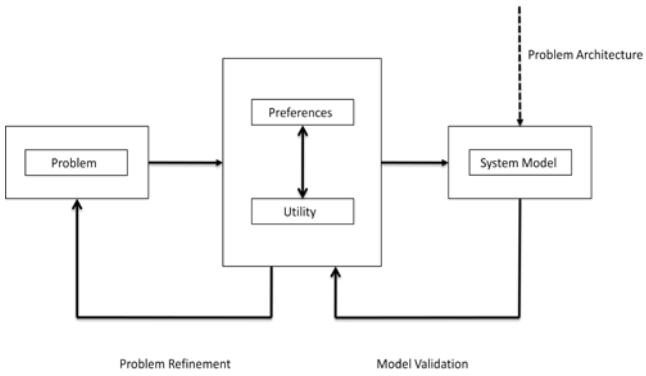

Figure 1: The methodology

We begin with a characterization of the problem, as presented by the decision-maker (e.g., the client organization's CISO). For example, the organization may be divesting itself of one of its constituent businesses and may wish to manage the change of status and access privileges of the affected staff. Associated with this divestiture, the CISO has a range of choices for the nature of the resulting system configuration (including security controls) and a range of preferences among the security outcomes. These preferences give rise to a formal expression of utility. The dynamics of this utility can then be explored by constructing an executable mathematical model of the system, in the context of its dynamic threat and economic environments. The construction of such a model must capture not only the

preferences of the decision-maker, such as the CISO, in respect of the desired outcomes but also the architectural (and policy, and business process) constraints inherent in the problem.

Having constructed the model, its behaviour is simulated in the presence of a (stochastic) representation of the dynamic threat and economic environments — including, in particular, security investments — and its predictions are validated against the preferences (expressed as a utility function) of the decision-maker (e.g., the CISO). The model may then be refined appropriately, as may the decision-maker's understanding of his preferences in response to the initial problem, which may itself be subject to reassessment and refinement.

To explore the methodology we have outlined and, in particular, to address a real challenge facing the security managers in a financial services organization, we describe a case study of the ongoing de-perimeterization of their organization. Within a de-perimeterization project, a typical example involves the divestiture of a business function or service, so that a business or service that initially existed entirely within the enterprise firewall, and which involved contracted employees, switches to being operated by third party employees accessing applications from outside the firewall. In such situations, the information security concern relates to the increased risk of breaches that may be introduced by more relaxed network access arrangements, changes in personnel culture, and changing contractual agreements.

Various security mechanisms can be considered to control communications between users (and their associated endpoints) and servers/applications. Such mechanisms cost money and can adversely affect the user or business process. In general, the problem is to determine which security portfolio will, at appropriate cost, provide the best trade-off between reducing risks and maintaining business priorities. The security controls that are often considered during the de-perimeterization of part or the whole of organization's network include the following: some type of virtual desktop environment with different restrictions and monitoring; controls enforcing stronger authentication for direct access (especially for servers and applications that cannot be moved to be accessible via the virtual desktop environment); intrusion detection systems (IDSs) to monitor and alert based on inappropriate network activity; regular access and privilege review to ensure there is no creep up of the number of users with multiple privileges. Different combinations of these controls will have different effects on different aspects of the system and its managers' confidence in its status, such as the likelihood or impact of certain types of breaches, the level of assurance/knowledge that breaches are detected, the performance of the business process, the costs of running the IT systems, or the security investment costs. For example, certain restrictions on the virtual desktop might be better at preventing malicious confidentiality breaches, whereas others will apply to inadvertent availability problems. Some mechanisms will make it more difficult for staff to inadvertently or maliciously cause breaches, but might also slow down their productivity. Alternatively, IDSs and other forms of monitoring might affect system latency, but improve awareness of the threat situation and so improve assurance.

Over the course of this document we will introduce the techniques and technologies developed during the Trust Economics project and outline how they could be used to tackle the scenario outlined above.

It should be emphasised that the purpose of this experiment id not to explore the efficacy of particular (and perhaps familiar) security solutions, but rather to explore the formulation and effectiveness of a methodology.

Components of Framework

The wide variety of expertise brought together under the umbrella of the Trust Economics project has allowed us to develop an inter-disciplinary approach to information security decision-making. In this section, we outline the key components of our approach, discussing along the way some key challenges.

Ontology

Acting as a foundation for the other components of the system our work on developing an ontology for security techniques and processes allows decision-makers to understand rapidly the range of options when faced with a security problem, including advice relating to user behaviour and its effective management. We have developed a tool — the 'CISO Tool' — to assist security managers in assessing and handling their security risks.

We also develop an ontological account of information security architectures that is inspired by economic models of trade-offs between confidentiality, integrity, and availability. Our approach clarifies the nature of the trade-offs by making a clear distinction between declarative and operational concepts in security. We integrate this approach with a semantically justified mathematical systems modelling technology, thus providing a basis for a systematic methodology to support operational decision-making in information security investments and trade-offs.

We argue that a key distinction within the concepts of information security is between the declarative and the operational, and that it is important not to confuse the two. In addition, we have argued that the concept of utility — from economics — provides an appropriate mechanism for assessing the value of both declarative objectives and operational implementations.

- The declarative concepts of information are those qualities that information security policies and architectures seek to achieve. The key declarative concepts — at least at the usual level of abstraction — are confidentiality, integrity, and availability, and different systems will seek to achieve these qualities to varying relative extents.

- The operational concepts of information security are the mechanisms that are used in order to implement the declarative objectives. For example, authentication is used to

protect confidentiality, and back-ups are used to protect availability.

- Utility functions are used to express preferences between different, possibly conflicting objectives, as well as the form and time-evolution of the objectives themselves.

Utility Theory

The disciplines of economics and security have been effectively interlinked for over a decade. We make effective use of this prior research by framing our work entirely in terms of utility theory. This allows us to derive solutions that are optimal for the system rather than from the viewpoint of any one stakeholder. By removing this source of decisions making bias we are able to offer up a systematic and repeatable approach to information security.

Once the decision-maker has adequately characterized the problem, with a range of (competing) attributes and objectives identified, it is necessary to determine to what extent the objectives must be achieved for a solution to the problem to be acceptable; that is, we must determine the decision-maker's preferences for acceptable trade-offs between the various attributes and express them in a quantifiable form.

We adopt standard techniques from economics [17], as described in the systems modelling context in [3, 12], and employ utility functions such as

$$U = \omega_1 f_1(C - \hat{C}) + \omega_2 f_2(A - \hat{A}) + \omega_3 f_3(I - \hat{I}),$$

where C, A, and I represent the outcomes — here, for example, confidentiality, availability, and investment — we care about, and $\hat{C}$, $\hat{A}$, and $\hat{I}$ represent the decision-maker's targets for these outcomes. The functions f_i $(1 \leq i \leq 3)$ represent the decision-maker's tolerance for variance from the targets. The weights ω_i $(1 \leq i \leq 3)$ represent the decision-maker's preferences between the component outcomes. Of course, the utility function may have many components. In the simplest case, we set the f_is to be quadratic functions. This choice, which has a well-supported theoretical basis [17], captures diminishing marginal utility and implies, since quadratics are symmetric about their maxima, that the decision-maker is equally tolerant for going over or under target. For example, if the outcome component is cost, overspending by £100 is just as bad as under spending by £100. In most practical situations, however, the decision-maker's preference will be asymmetric and it is necessary to use functional forms such as Linex functions [26, 28, 13], of the form $f(x) = (e^{ax} - ax - 1) / a^2$, which capture this asymmetry appropriately (a is a parameter).

Having established the form of the utility function, we consider its expected value as the components vary over time. The dynamic models employed in economics (for a security example, see [13]) employ a set of system equations that describe the dynamics of the components in the presence of stochastic shocks. Instead of a set of equations, we employ a mathematical system model which captures the structure of the system in terms of its key

components (see Section 4) and which can be executed in order to simulate the behaviour of the system in the presence of stochastic shocks. The structure of such a model allows the (expected) values of the components of the utility function to be calculated.

In the case of any particular model, such as that developed here, the components of a utility of interest must be identified. In our case study, these were identified via a process of multiple iterations with the decision-makers. The process sought to determine their primary concerns, the changes they expected over the future years of interest, their investment options, and the expected consequences of these investments, including the preferences between outcomes associated with each investment option. The process was implemented using structured discussion within which the consequences of focusing on certain components were considered

Initially, the components considered included cost, confidentiality, and availability. These attributes clearly trade off against one another, as each (confidentiality) mechanism that restricts or reduces access naturally makes the system less available, and vice versa. As different types of availability outcomes were discussed, it became apparent that the real issue was the effect on the business function (as opposed to system or network uptime, bandwidth, or latency). Similarly, confidentiality shifted to cover many forms of breaches, including the integrity of transactions, data leakage, and unauthorized or even unaccountable system activity. It was clear that for each of these there was a desire to reduce the number of breaches, but also to know (and communicate) the effectiveness of the methods of reducing breaches.

As a result of this empirical work, the utility components for the case study became *breach prevention*, *assurance*, and *business performance* — corresponding conceptually to the security components (such as *C*, *A*, etc.) in the utility expression above — and cost — corresponding to *I* in the utility expression above. In the case study, the business performance component of utility represents the performance of IT support staff in response to support–job requests. The next step was to elicit the tolerance for how much should be achieved in each of these components. For example, in order to elicit the decision-maker's preferences for the form (e.g., asymmetry, gradient) of marginal utility either side of target, the use of both quadratic and Linex formulations of the dependencies of the utility function on components were explored using a structured questionnaire.

As experience would suggest, the decision-maker's utility function in this case study is, to varying degrees, asymmetric in all of its components. For example, the marginal utility of breach prevention has steeper gradient below target than above. The assignment of form employed in this study is imprecise. Nevertheless, we were able to use this information to inform the design of the next questionnaire, used to elicit the decision-maker's preferences between outcomes.

Capturing the Decision-maker's Preferences

We have explained that, in the case study, the decision-maker's desired collection of attributes — essentially, this is the problem characterization — were elicited via structured discussion. It was also necessary to elicit the decision-maker's preferences between outcomes. To this end, we focussed on single measures that would represent each utility component, and presented each outcome as a 4-tuple, consisting of proportion of breaches against overall access activity (i.e., breach prevention), proportion of detected breaches against overall breaches, (i.e., assurance), proportion of SLA violations against overall job-requests (i.e., business performance), and cost. From these, we created simple preference questionnaires each consisting of around 100 value pairs related to the components in the 4-tuple. For example, value pairs were created for breaches and SLA violations, where values for the proportion of breaches against accesses ranged from 0.15 to 0.01 with different values for proportion of SLA violations. The decision-maker had to evaluate and rate each pair within the scale of 1–6, where 3 would represent an acceptable outcome, 6 would be strongly unacceptable, and 1 would be a highly desirable outcome.

Mathematical Systems Modelling

Systems modelling is a powerful tool that simulates the interaction of the resources and processes in an organization in such a way that allows predictions to be made about the outcomes of a course of action. The accuracy and predictive power of such models is heavily reliant on the accuracy and comprehensiveness of the information used to build them. By drawing on the expertise of world leaders in human factors in security we are able to populate our models with a far richer notion of user populations thus returning a more effective tool for simulation and analysis.

A key component of our approach is our mathematical modelling of the underlying architecture and processes. Our approach, the mathematical basis of which is presented in [5, 8, 9, 29, 30], is grounded firmly in mathematical logic, computation theory, and probability theory, but employs well-developed, implemented tools.

Our approach views a system as having the following key conceptual components:

- Environment: All systems exist within an external environment. We may seek to model the structure of the environment, in which case we treat the environment as a system of interest in itself; typically, however, we treat the environment as a source of events that are incident upon the system of interest according to given probability distributions;
- Location: The components (i.e., resources; see below) of a system of interest are typically, distributed around a collection of places. Different places are connected by oriented links;

- Resource: The notion of resource captures the components of the system that are manipulated by its processes (see below). Resources include things like the components used by a production line, the system operating staff, and money;
- Process: The notion of process captures the (operational) dynamics of the system. Processes manipulate resources in order to deliver the system's intended services.

This framework is appropriately captured by the Gnosis modelling tool.

The system model created for the case study represents the access activity of IT support staff in the de-perimeterized network environment and explores the outcomes for 4-tuple measurements as describe. These measurements are gathered through several simulations of the model, each under different combinations of the security controls.

Specifically, the model captures the process of IT staff responding to support-job requests and accessing numerous internal systems, via various access protocols. We assumed, guided by the experience of the managers, that untrustworthy staff would take opportunities to engage in unauthorized activities (including harmless, justifiable accesses, over-zealous trawling, or significant breaches) in addition to the legitimate job-related activities. Depending on the access protocol used, we also assumed, based on the experience and observations of the managers, certain success rate for a breach and its detection by monitoring controls. Any additional security controls introduced would either reduce the likelihood of a breach occurring (this would be with restrictions on virtual desktop access, and direct access controls), or improve would detection rate (any monitoring controls). At the same time, the additional controls put some burden on support staff, thus decreasing their job turnover rate. Additional access controls, for example, often require extra authentication. Also, these controls are usually centralized, thus requiring a central server to be always online. If it fails, the system becomes inaccessible for a number of hours. Figure 4 shows the general structure of the model. It consists of two main parts. One part models the activities of the IT support staff, mainly the job-request processing. This task requires multiple accesses to the systems either though a virtual desktop or direct access protocols. The other part evaluates each access and determines the likelihood of its resulting in unauthorized activity and breaches.

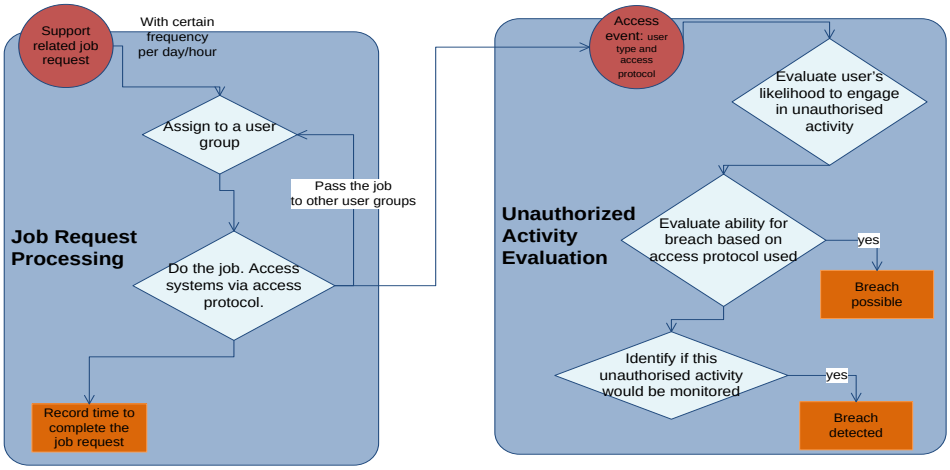

Figure 2: General structure of the system model

The diagrams should be interpreted as follows: the circular components represent events incident upon the system from the environment; the rectangular endpoints correspond to the resource components of the model, and provide the measurable quantities for utility calculations (we make no use of location in this model); finally, the process dynamics of the model is captured by the arrows connecting events to resources via key computation steps, denoted by diamonds.

The model requires some initial assumptions to be made about the initial state of access requirements, IT staff trustworthiness, and the general job-request frequency and turnover rate. Table 1 below summarizes these assumptions, which were based on the experience and observations of the IT operations and security managers in the organization and which elicited via multiple iterations of model-execution and model-refinement.

The job-request processing part of the model schedules new jobs every hour and assigns them to IT staff.

Table 1: Initial state assumptions for the model

For job-request processing
Support job frequency: 1 every hour
Time1 taken to do the job (1st user/pass): between 2h and 5h
Time2 taken to do the job (2nd and further users/passes): between 0.5 and 1 hours
Multi-group ratio (users in more than one group): 0.5 (i.e., 50% of users are in multiple groups)
Job redo ratio (more than one user works on it): 0.01/multi_group_ratio
Standard SLA required job processing time: 6 hours
For unauthorized activity evaluation
User trustworthiness: 90% trusted
Non-job-related access ratio: 0.005

Access protocol ratio: 55% of accesses go through virtual desktop, 45% are direct accesses
Ability to engage in unauthorized activity is at 0.4 via virtual desktop access with 0.7 detection rate (when monitoring is in place), and at 0.75 via direct access with 0.4 detection rate

Each IT staff member (corresponding to a system user) accesses the systems to work on the job using an access protocol selected based on the access protocol ratio in Table 1. Also, occasionally, non-job-related access is triggered, corresponding to 0.5% of overall accesses (ratio 0.005 in Table 1).

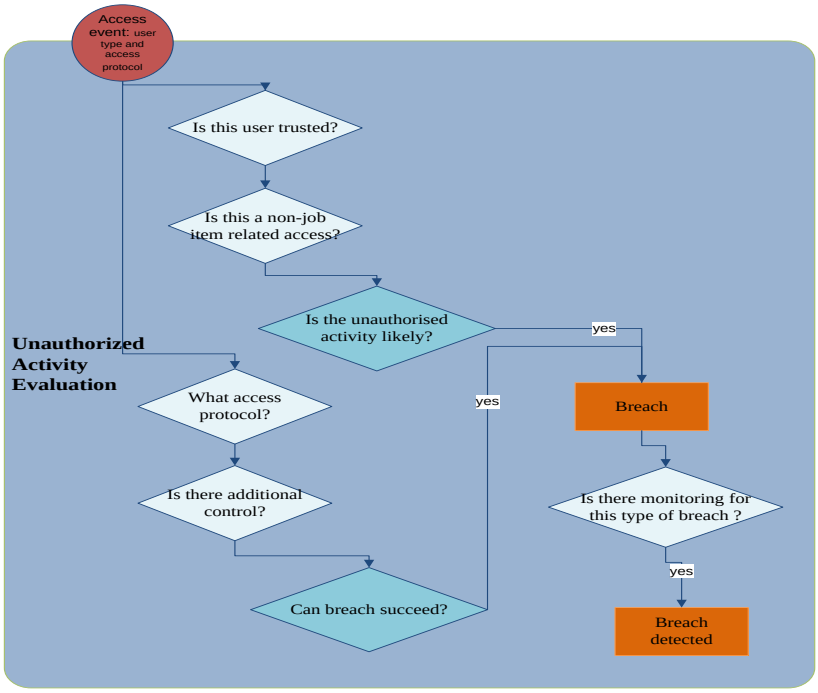

Figure 3: Detailed model for evaluation of unauthorized activity

Depending on to how many groups the user belongs, the job could be passed to another user after certain time (Time1 in Table 1). The second and any subsequent users take additional time (Time2) to finish the job. In the end we arrive at the measure of the overall time taken to complete a support job request. If it exceeds the SLA-dictated time, the task is registered as an SLA violation. The unauthorized activity evaluation part of the model is used to determine the likelihood of a user engaging in unauthorized activity and the ability of this user to successfully execute a breach. A detailed breakdown of this part of the model is shown in Figure 3.

Based on the advice of the managers, we assume, initially, that the overall likelihood for a user to engage in unauthorized activity is at 0.001. This increases 10-fold if the user accessing the systems is not trustworthy (based on the ratio in Table 1). It would double if the access were determined not to be job- relevant. Depending on the access protocol employed, the ability for the user to successfully execute a breach differs. We assume that breaches are

more likely to succeed via direct access to systems (with probability of 0.75) than via virtual desktop access (with probability 0.4).

This is, of course, a very simplified view on how breaches might arise. A more rigorous analysis, based on the attacks trees and hacker behaviour could be used to arrive at more grounded and realistic probabilities regarding the breach success rate. In this research, however, we have focussed not on analyzing the internal/external attacker behaviour, but rather on making reasonable assumptions. Assumptions were also made about the breach-detection rate related to each protocol (as in Table 1). These rates are used to determine the proportion of detected breaches.

Execution of Models: Simulation Experiments in Gnosis

In general, simulation tools are used to implement Monte Carlo-style experiments about system behaviour. From a theoretical perspective, the question of convergence of simulations must be considered. This is a difficult problem for Monte Carlo methods in general, where one is calculating an (abstract) integral whose integrand does not belong to a well-known class of functions. However, the value of simulation systems (including Gnosis) is precisely where such functions occur unavoidably in applied problems. From a more practical perspective, it is valuable to explore the properties of models less completely. There is a great deal of literature on these topics, well beyond the scope of this report.

First, we note that we are generally concerned with deploying our modelling approach to quite large and complex systems for which it is inevitably very easy to find unstable choices of parameter constellations. Whilst much of the literature on convergence for Monte Carlo-style methods is applicable to Gnosis, it is important to not that a significant area for research is open here. Specifically, an account of convergence for Core Gnosis should take account of the structural constraints that can be imposed by the underlying theory of location and resource distribution.

Second, in practice, Core Gnosis is typically deployed in the following `what-if' analysis approach, which of course follows the classical modelling cycle:

- First, the parameter constellations required by a model are estimated using the best available information; that is, data and expert opinion;
- Second, the choice of constellation is refined in the light of expert review of the model's behaviour when executed;
- Third, the sensitivity of the model's behaviour to variations in the parameters is then systematically explored and statistically analyzed;
- Finally, and optionally, within sufficiently tightly identified spaces of choices for the parameters, Monte Carlo experiments can be performed.

This approach works well for dealing with quite large and complex systems for which there is little hope of obtaining globally convergent models -- indeed, we should not expect to do so -

– and has proved to be of significant value in range of industrial-strength applications of our approach.

The pragmatic use of statistics (including convergence, stability, and experiment design) is a well-established practice in simulation modelling.

Access Control

Users increasingly share information through informal structures such as social networking sites meaning the individual user has greater discretion over who has access to what information. Traditional security approaches such as Role-Based Access Control are therefore no longer appropriate and to minimize unauthorized access a greater understanding of how users manage access control tasks is needed.

In common with many security tasks, access control is an enabling task in that it serves as a way to complete the primary task of interest. This means that access control is often interleaved with other tasks and can interrupt these tasks. Thus, a complete understanding of access control requires an understanding of the way that users interleave between tasks and the likelihood that enabling tasks will be remembered and executed in a multitasking environment.

We have completed a program of controlled experimentation to understand the ways that users cope (and do not cope) with the requirement to interleave access control tasks with other typical office tasks. This enables the identification of general factors that will predict the likelihood of security breaches due to inappropriate access privileges being set. Further, the data from these experiments enable us to account for the lost productivity caused by poorly integrated security mechanisms and factor this into our utility calculations. This allows us to not only analyse existing systems for weaknesses but to make effective suggestions as to how to improve both security and productivity through improved systems design.

Cognitive Modelling

The Compliance Budget emphasises that users must weigh up the costs and benefits of complying with different security policies. This means that to understand and predict the likely rate of compliance with a security policy it can be helpful to consider the incentives and constraints that frame user behaviour. To address this we have constructed cognitive models of the security behaviour of different user groups. These models contrasted the security of passwords across different accounts and considered the factors that determine compliance with security guidelines.

The models were derived using a diary study, interview data and collaborative user modelling sessions with computer scientists, administrative staff and students. They indicated that memory, knowledge and motivation constraints were strong determinants of password security. Importantly, the models addressed the interaction of these different constraints with

each other and with the environment. For example, they indicated that users exploited features of memory to construct more secure passwords for frequently accessed services.

The user modelling also revealed that the goals for password behaviour differed importantly between users and that differences in the way goals were expressed affected the security of the passwords. Some users viewed passwords as an asset – a way of protecting their information whereas other users considered passwords as a cost that had to be endured or minimised. These differences in user representation affected security and suggested improvements that security professionals could implement.

A key part of the value of this work is as an illustration of the way that cognitive modelling can be applied to security and the consequent benefits. By extracting data from a number of sources, and modelling in collaboration with users from different groups, we were able to produce relatively sophisticated models that provide a starting point for more general models of security. The process of this modelling can yield key insights and the product (the model itself), can provide input for mathematical modelling or be drawn upon directly by a decision maker.

Interview Analysis

Through the contribution of the industrial partners (Hewlett-Packard, Merrill Lynch, and (latterly) National Grid) we were able to gain access to a large population of users that regularly interact with a variety of security measures. Approximately 200 security-related interviews were conducted giving us a large dataset for examining the attitudes and behaviours of employees when faced with security tasks. The findings from these interviews grant us a unique perspective on user behaviour, grounding our work with an understanding of the reality of the impact of security decision-making.

Employing a sophisticated understanding of human factors allows our measures of productivity to be represented with a superior level of realism. We understand that user effort is a finite resource and if security measures overburden employees then their productivity will suffer. Likewise by analysing workflow disruption and task interruption as a result of the implementation of security measures we can further refine our measure of the impact of such decisions on the productivity of the workforce.

The work mentioned here has led to a range of substantial publications and the development of the concept of the ‘compliance budget’. The key observation here is that a significant number of security breaches result from employees' failure to comply with security policies. Many organizations have tried to change or influence security behaviour, but found it a major challenge. Drawing on previous research on usable security and economics of security, we have proposed a new approach to managing employee security behaviour. We conducted interviews with 17 employees from two of our commercial partner organizations (Merrill Lynch

and Hewlett-Packard), asking why they do or don't comply with security policies. Our results show that key factors in the compliance decision are the actual and anticipated cost and benefits of compliance to the individual employee, and perceived cost and benefits to the organization. As a result, we have presented a new paradigm — the Compliance Budget — as a means of understanding how individuals perceive the costs and benefits of compliance with organizational security goals, and identify a range of approaches that security managers can use to influence employee's perceptions (which, in turn, influence security behaviour). The Compliance Budget should be understood and managed in the same way as any financial budget, as compliance directly affects, and can place a cap on, effectiveness of organizational security measures.

Validation

We conducted study with twelve experienced security professionals (accessed via the industrial partners) to examine how security decisions are made and justified. Including preparation of scripts and tools, practice runs, iterations, finding appropriately experienced security professionals, and conducting the actual interviews the study took over six months to complete. The study focused on the economic utility-based approach developed and described in our earlier work together with a system modeling and simulation based on the Gnosis toolset.

Our economic utility-based method aims to help decision makers identify and prioritize the trade-offs between the business outcomes of a security decision, and as a result extracts a form of utility relevant for a decision maker and/or their organization. We start from the assumption that at least three outcomes, such as cost, productivity and security risk, trade-off against one another. The decision maker is guided through multiple steps where he/she has to prioritize the outcomes, select appropriate measures that can be used as proxies for the outcomes, and finally express the targets for these measures and the preferences in meeting them. Results from Gnosis based system modeling and simulation are then used to help the stakeholders gain a better understanding of their assumptions and to show the predicted effect that a security decision has on the selected measures and business outcomes.

The study was designed so as to examine the difference (if any) these techniques make to the security decision-making process. Specifically, if and how they effect:

- The conclusions or decisions made,
- The thought process followed,
- The justifications given, and
- The confidence the stakeholder has in the final conclusions or decisions made.

The focus of the validation study was upon the way our methodology and related software tools influence the security professionals as a precursor to understanding how in turn this may influence organizational decision processes. To this end, the security decision problem for the

study and the possible alternative solutions were chosen to require participants to make different trade-offs between security, productivity and cost. There was not an expectation that the use of the methodology and tools should lead to any particular decision outcome to be favored. This reflects the multi-factorial and often ill-specified decision making typically undertaken by the security professionals

The results of the study indicated that the interventions changed the decision processes for these experienced security professionals. Specifically, a broader range of factors were accounted for and included as justifications for the decisions selected. The security professional is one (important and influential) stakeholder in the organization decision-making process, and arguably the richer arguments are more suitable for persuading a broader business audience. More generally, the study complements all research in security economics that is aimed at improving decision-making, and suggests ways to proceed and test for the impact of new methods on the actual decision-makers.

Commercial and Societal Impact

1. HP's Information Security business unit has introduced a new security consulting service based directly upon the output of the Trust Economics project and its parallel project within HP Labs. The service is called 'Security Analytics'. The service provided by HP Information Security delivers the methodology illustrated in this report in specific industry contexts. Please see http://h10131.www1.hp.com/uk/en/information-security/security-innovation/ and http://h20195.www2.hp.com/V2/getdocument.aspx?docname=4AA3-2046EEW.pdf for HP's presentation of the service.
2. All of the academic partners have introduced ideas from the project into their teaching programmes, mostly at the Master's level: these developments will have long-term cultural impact. Several ongoing PhD projects have been directly influenced by the project.
3. Several of the project's staff are now advisers to governments and other bodies, where the perspectives developed by the project are have both immediate and longer term cultural impacts.
4. Several staff, from all of the academic partners (including Aberdeen), are now exploring consulting and training business opportunities, alongside publication of the ideas developed in less academic, more popular forms.
5. Members of the project are now regular and influential contributors to and/or organizers of the leading conferences in the relevant areas.

Publications

Economic methods and decision making by security professionals. Simon Shiu, Adrian Baldwin, Yolanta Beres, Marco Cassa Mont, Geoffrey Duggan, Hilary Johnson and Christopher Middup. To appear, Proc. WEIS 2011, George Mason University, Fairfax, Virginia, 14-15 June, 2011: WEIS 2011.

Fixed Costs, Investment Rigidities, and Risk Aversion in Information Security: A Utility-theoretic Approach. Christos Ioannidis, David Pym, and Julian Williams. To appear, Proc. WEIS 2011, George Mason University, Fairfax, Virginia, 14-15 June, 2011: WEIS 2011.

Economics of Information Security and Privacy. Tyler Moore, David Pym, and Christos Ioannidis (editors). Springer New York Dordrecht Heidelberg London, 2010. doi: 10.1007/978-1-4419-6967-5.

How Secure Is Your Password? Towards Modelling Human Password Creation. Grawemeyer, B., Johnson, H.In Proceedings of the First Trust Economics Workshop, University College London, England 23 June 2009. www.trust-economics.org/p3.pdf

A Collaborative Ontology Development Tool for Information Security Managers. John Mace, Simon Parkin, Aad van Moorsel. Proceedings of the ACM Symposium on Computer Human Interaction for Management of IT (CHIMIT), San Jose, CA, USA, 2010.

Ontology Editing Tool for Information Security and Human Factors Experts. John Mace, Simon Parkin, Aad van Moorsel. To appear in the Proceedings of the International Conference on Knowledge Management and Information Sharing (KMIS), Valencia, Spain, 2010.

A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions. Simon Parkin, Aad van Moorsel, Philip Inglesant, M. Angela Sasse. Proceedings of the New Security Paradigms Workshop (NSPW) 2010, Concord, MA, USA, 2010.

Information Stewardship in the Cloud: A Model-based Approach. David Pym, Martin Sadler, Simon Shiu, and Marco Casassa Mont. To appear, Proceedings of CloudComp 2010, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST) series, Springer, 2010.

Information Stewardship in Cloud Computing. David Pym, Martin Sadler. International Journal of Service Science, Management, Engineering, and Technology 1(1), 50-67, 2010.

Security Analytics: Bringing Science to Security Management. David Pym and Simon Shiu. IISP Pulse 4, Summer 2010: 12-13.

Semantics for Structured Systems Modelling and Simulation. Matthew Collinson, Brian Monahan, and David Pym Proc. Simutools 2010, ACM Digital Library and EU Digital Library. ISBN: 78-963-9799-87-5.

Structured Systems Economics for Security Management. Adam Beautement and David Pym. Proc. WEIS 2010, Harvard University.

A Discipline of Mathematical Systems Modelling. Matthew Collinson, Brian Monahan, and David Pym. To appear: College Publications, London, 2011.

Decision Support for Systems Security Investment. Yolanta Beresnevichiene, David Pym, Simon Shiu. Proc. Business-driven IT Management (BDIM) 2010. IEEE Xplore, 2010.

Economics of Identity and Access Management: Providing Decision Support for Investments. Marco Casassa Mont, Yolanta Beresnevichiene, David Pym, Simon Shiu. Proc. Business-driven IT Management (BDIM) 2010. IEEE Xplore, 2010.

Implementation of User-Managed Access Framework for Web 2.0 Applications. Maciej Machulak, Lukasz Moren, Aad van Moorsel. In MW4SOC'10: The Fifth Middleware for Service Oriented Computing Workshop of the 11th International Middleware Conference 2010, Bangalore, India, 2010.

User-Managed Access to Web Resources. Maciej Machulak, Eve Maler, Domenico Catalano, Aad van Moorsel. In ACM CCS-DIM 2010: The Sixth ACM Workshop on Digital Identity Management, Chicago, IL, USA, 2010.

Architecture and Protocol for User-Controlled Access Management in Web 2.0 Applications. Maciej Machulak and Aad van Moorsel. In ICDCS-SPCC 2010: The First Workshop On Security And Privacy In Cloud Computing, Genoa, Italy, 2010.

Algebra and Logic for Resource-based Systems Modelling. Matthew Collinson and David Pym Mathematical Structures in Computer Science 19:959-1027, 2009. doi:10.1017/S0960129509990077.

Algebra and Logic for Access Control. Matthew Collinson and David Pym. Formal Aspects of Computing 22(2), 83-104, 2010. Erratum: Formal Aspects of Computing 22(3-4), 483-484, 2010. Available as an HP Labs Technical Report (with erratum incorporated): HPL-2008-75R1.

A Logical and Computational Theory of Located Resources. Matthew Collinson, Brian Monahan, and David Pym. Journal of Logic and Computation 19(b):1207-1244, 2009. DOI: 10.1093/logcom/exp021. For preprint see HP Labs Technical Report HPL-2008-74R1

An Information Security Ontology Incorporating Human-Behavioural Implications. Simon Parkin, Aad van Moorsel, Robert Coles. Proceedings of the 2nd International Conference on Security of Information and Networks (SIN), ACM, October 2009.

Risk Modelling of Access Control Policies with Human-Behavioural Factors. Simon Parkin and Aad van Moorsel. Proceedings of the 9th International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS), September 2009.

A Knowledge Base for Justified Information Security Decision-Making. Daria Stepanova, Simon Parkin, Aad van Moorsel. Proceedings of the 4th International Conference on Software and Data Technologies (ICSOFT), July 2009. Institute for Systems and Technologies of Information, Control and Communication (INSTICC).

Information Security Trade-offs and Optimal Patching Policies. Christos Ioannidis, David Pym, Julian Williams. To appear: International Conference on Global Trends in the Efficiency and Risk Management of Financial Services. Submitted to a journal.

Investments and Trade-offs in the Economics of Information Security. Christos Ioannidis, David Pym, Julian Williams. Proceedings of Financial Cryptography and Data Security 2009, LNCS, Springer.

The Compliance Budget: Managing Security Behaviour in Organisations. Adam Beautement, Angela Sasse, Mike Wonham. New Security Paradigms Workshop (NSPW) 2008, Plumpjack Squaw Valley Inn, Olympic, California, USA. 22-25 September 2008.

Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. Adam Beautement, Robert Coles, Jonathan Griffin, Christos Ioannidis, Brian Monahan, David Pym, Angela Sasse, Mike Wonham. Workshop on the Economics of Information Security. Hanover, NH, USA, 26 June 2008.

Trust Economics Feasibility Study. Robert Coles, Jonathan Griffin, Hilary Johnson, Brian Monahan, Simon Parkin, David Pym, Angela Sasse and Aad van Moorsel. DSN 2008 Workshop on Resilience Assessment and Dependability Benchmarking. Anchorage, Alaska, USA, 25 June 2008.

The Impact of Unavailability on the Effectiveness of Enterprise Information Security Technologies. Simon Parkin, Rouaa Yassin-Kassab and Aad van Moorsel. In Service Availability. 5th International Service Availability Symposium, ISAS 2008, Tokyo, Japan, May 19-21, 2008.

An Update to Located Demos2k. Matthew Collinson, Brian Monahan, David Pym. HPL-2008-205, HP Laboratories, 2008.

Identity Analytics: Using Modeling and Simulation to Improve Data Security Decision Making. Marco Casassa Mont, Adrian Baldwin, Jonathan Griffin, Simon Shiu, Yolanta Beres. HPL-2008-188, HP Laboratories, 2008.

Towards Identity Analytics in Enterprises. Marco Casassa Mont, Adrian Baldwin, Jonathan Griffin, Simon Shiu. HPL-2008-186, HP Laboratories, 2008.

Security Analytics: Analysis of Security Policies for Vulnerability Management. Yolanta Beres, Jonathan Griffin, Simon Shiu. HPL-2008-121, HP Laboratories, 2008.

Modelling Task Knowledge Structures in Demos 2000. Jean Paul Degabriele, David Pym. HPL-2008-94, HP Laboratories, 2008.

Algebra and Logic for Access Control. Matthew Collinson and David Pym. HPL-2008-75R1, HP Laboratories, 2008.

A Logical and Computational Theory of Located Resource. Matthew Collinson, Brian Monahan, David Pym. HPL-2008-74R1, HP Laboratories, 2008.

User-Managed Access to Web Resources. Maciej Machulak, Eve Maler, Domenico Catalano and Aad van Moorsel. CS-TR No 1196, School of Computing Science, Newcastle University, Mar 2010

Architecture and Protocol for User-Controlled Access Management in Web 2.0 Applications. Maciej Machulak and Aad van Moorsel. CS-TR No 1191, School of Computing Science, Newcastle University, Mar 2010

Use Cases for User Centric Access Control for the Web. Maciej Machulak and Aad van Moorsel. CS-TR No 1165, School of Computing Science, Newcastle University, Aug 2009

Architecting Dependable Access Control Systems for Multi Domain Computing Environments. Maciej Machulak, Simon Parkin, Aad van Moorsel. CS-TR No 1156, School of Computing Science, Newcastle University, Jul 2009.

A Novel Approach to Access Control for the Web. Maciej Machulak and Aad van Moorsel. CS-TR No 1157 , School of Computing Science, Newcastle University, Jul 2009.

Risk Modelling of Access Control Policies with Human Behavioural Factors. Simon Parkin, Aad van Moorsel. CS-TR No 1155, School of Computing Science, Newcastle University, Jul 2009.

Proceedings of the First Trust Economics Workshop. Philip Inglesant, Maciej Machulak, Simon Parkin, Aad van Moorsel, Julian Williams (Eds.). CS-TR No 1153, School of Computing Science, Newcastle University, Jun 2009.

A Knowledge Base for Justified Information Security Decision-Making. Daria Stepanova, Simon Parkin, Aad van Moorsel. CS-TR No 1137, School of Computing Science, Newcastle University, Feb 2009.

An Information Security Ontology Incorporating Human-Behavioral Implications. Simon Parkin, Aad van Moorsel. CS-TR No 1139, School of Computing Science, Newcastle University, Feb 2009.

Trust Economics Feasibility Study. Robert Coles, Jonathan Griffin, Hilary Johnson, Brian Monahan, Simon Parkin, David Pym, Angela Sasse and Aad van Moorsel. CS-TR No 1101, School of Computing Science, Newcastle University, Jun 2008.

The Impact of Unavailability on the Effectiveness of Enterprise Information Security Technologies. Simon Parkin, Rouaa Yassin-Kassab and Aad van Moorsel. CS-TR No 1081, School of Computing Science, Newcastle University, Mar 2008.

A Trust-economic Perspective on Information Security Technologies. Simon Parkin, Aad van Moorsel. CS-TR 1056, School of Computing Science, Newcastle University, Oct 2007.

Using and managing multiple passwords: A week to a view. B Grawemeyer & H.Johnson. Accepted subject to revisions Interacting with Computers.

Rational security: Modelling everyday password use. G.Duggan, H.Johnson & B. Grawemeyer. Accepted subject to revisions International Journal of Human Computer Studies.

"Pick 4 Squares" - A Usability Study of the GrIDsure PIN Replacement System. Sacha Brostoff, Philip Inglesant, and Angela Sasse. University College London (UCL), 2009.

Information Security Trade-offs and Optimal Patching Policies. Christos Ioannidis, David Pym, Julian Williams.

A Psychometric Study of Information Technology Risks in the Workplace. Robert Coles, Gerard P. Hodgkinson. Risk Analysis, Vol. 28, No. 1, 2008.

Towards Modeling Individual and Collaborative Construction of Jigsaws Using Task Knowledge Structures (TKS). Hilary Johnson, Joanne Hyde. ACM Transactions on Computer-Human Interaction, Vol. 10, No. 4, December 2003, Pages 339–387.

Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. Martina Angela Sasse, Sacha Brostoff, Dirk Weirich. BT Technology Journal Vol 19 No. 3, July 2001.

Users Are Not The Enemy. Anne Adams, Martina Angela Sasse. Communications of the ACM December, Vol. 42, No. 12, 1999.

Using Security Metrics Coupled with Predictive Modelling and Simulation to Assess Security Processes. Yolanta Beres, Marco Casassa Mont, Jonathan Griffin, Simon Shiu. HPL-2009-142, HP Laboratories, 2009.

Identity Analytics - User provisioning Case Study: Using Modelling and Simulation for Policy Decision Support. Marco Casassa Mont, Adrian Baldwin, Simon Shiu. HPL-2009-57 (extended version containing a full D2K model), HP Laboratories, 2009.

Using Modelling and Simulation for Policy Decision Support in Identity Management. Adrian Baldwin, Marco Casassa Mont, Simon Shiu. HPL-2009-56, HP Laboratories, 2009. (also accepted at IEEE Policy Symposium 2009)

Towards an Analytic Approach to Evaluate Enterprises' Risk Exposure to Social Networks. Anna Squicciarini, Marco Casassa Mont, Sathya Dev Rajasekaran. HPL-2009-138, HP Laboratories, 2009.

Model-Based Assurance of Security Controls. Yolanta Beres, Adrian Baldwin, Simon Shiu. HPL-2008-7, HP Laboratories, 2008.

Economics of Information Security. Economic & Social Research Council (ESRC) & Cyber-Security Knowledge Transfer Network (KTN), ESRC Seminar Series, 2008. (includes articles by Christos Ioannidis and David Pym)

Mitigating Provider Uncertainty in Service Provision Contracts. Chris Smith, Aad van Moorsel. Workshop on Economic Models and Algorithms for Grid Systems (EMAGS) 2007, Institute of Information Systems and Mangement, pp 1-8, September 2007.

Adaptive SSL: Design, Implementation and Overhead Analysis. Christiaan Lamprecht, Aad van Moorsel. First International Conference on Self-Adaptive and Self-Organizing Systems (SASO) 2007, IEEE Computer Society, pp 289-292, July 2007.

About the Authors

HP Labs

Professor David J. Pym, MA, PhD, ScD, CMath FIMA, CITP FBCS, CSci is 6th Century Chair in Logic and SICSA Professor of Computing Science at the University of Aberdeen. Pym has previously held chairs in logic and theoretical computing science at the Universities of London and Bath. He has also been a senior member of the research staff at HP Labs. He continues to lead research projects in logic and in information and systems security, both in the academic world and with HP Labs, via the Cloud Stewardship Economics and Trust Domains projects.

Simon Shiu (M.Inst.ISP) is a senior research manager at HP Labs. He has worked in security for the last 10 years and published a number of papers in the area.

National Grid

Robert Coles, PhD, is Chief Information Security Officer and Head of Digital Risk and Security at National Grid. His main areas of research interest are in Critical National Infrastructure Policy and perceptions of information and IT risk.

Newcastle University

Aad van Moorsel is a Professor of Distributed Systems, Director of the Centre for Cybercrime and Computer Security, and a specialist in quantitative tools and techniques, including modelling, measurement and decision-making.

University College London

M. Angela Sasse is the Professor of Human-Centred Technology and Head of Information Security at UCL. A usability researcher by training, her research has focused on usability issues in security systems for the past 15 years.

Bath University

Dr Hilary Johnson is a Reader in Human Computer Interaction in the Department of Computer Science at the University of Bath. She has worked in HCI for over 20 years. Her research interests include user and task modelling, creativity, learning by typically developing and special needs groups, and developing approaches to involving multiple stakeholders in design processes.

Project Contributors

Bath University - Prof. Christos Ioannidis Dr Beate Grawemeyer, Dr Geoff Duggan
Newcastle University - Dr Simon Parkin, Maciej Machulak
UCL - Dr Philip Inglesant and Adam Beautement
HP Labs - Simon Arnell, Dr Brian Monahan, Jonathan Griffin, Marco Casassa Mont
HP Labs and Aberdeen University – Dr Matthew Collinson
Aberdeen University – Dr Julian Williams.

For more information about HP Labs visit:
www.hpl.hp.com