Trust Economics Feasibility Study

Robert Coles[*]
Merrill-Lynch

Jonathan Griffin
HP Labs

Hilary Johnson
University of Bath

Brian Monahan
HP Labs

Simon E. Parkin[†]
Newcastle University

David Pym
HP Labs & University of Bath

M. Angela Sasse
University College London

Aad van Moorsel[‡]
Newcastle University

ABSTRACT

We believe that enterprises and other organisations currently lack sophisticated methods and tools to determine if and how IT changes should be introduced in an organisation, such that objective, measurable goals are met. This is especially true when dealing with security-related IT decisions. We report on a feasibility study, Trust Economics, conducted to demonstrate that such methodology can be developed. Assuming a deep understanding of the IT involved, the main components of our trust economics approach are: (i) assess the economic or financial impact of IT security solutions; (ii) determine how humans interact with or respond to IT security solutions; (iii) based on above, use probabilistic and stochastic modelling tools to analyse the consequences of IT security decisions. In the feasibility study we apply the trust economics methodology to address how enterprises should protect themselves against accidental or malicious misuse of USB memory sticks, an acute problem in many industries.

1. INTRODUCTION

Resilience of computing systems can often only be addressed meaningfully within the context in which the system operates. That implies that benchmarking a system independent of that context is not always of great value–instead, computing systems need to be evaluated and optimised depending on the situation at hand. In this paper, we discuss resilience within an exterprise context, and we establish methodology to optimise IT decision-making based on the financial consequences of IT security decisions and policies.

Interesting enough, resilience is itself a term that is often used to denote the ability of an organisation to respond to and introduce changes [6]. These changes do not necessarily correspond to 'negative' events (failures, crimes) that require a reaction, but may often (and preferably) refer to proactive voluntary improvements of the business operations. In this paper we use such notions of enterprise resilience as a metric (the 'objective function'), but limit ourself to the role and impact of IT only in achieving such resilience. That is, how can an organisation manage its IT such that it improves the organisation (and its resilience), expressed through metrics such as employee productivity and financial risk. We focus on IT security in particular, trying to answer how security policies or solutions should or could be changed to improve enterprise resilience.

Senior managers (CEOs, CIOs, CISOs) with responsibility for information and systems security face two major problems. Firstly, there is poor economic understanding of how to formulate, resource, measure, and value security policies. There is also a poor organisational understanding of the attitudes of users to both information and systems security and of their responses to imposed security policies (as seen in the Final Report of the 'Trustguide' project [9] and the Foresight 'Cyber Trust and Crime Prevention' report [10]).

Consequently, the effectiveness and value of the policies with which users are expected to comply are very difficult to assess. To assess the effectiveness and value of security investments in a system, be they in people, processes, or technology, it is necessary to have a conceptualisation (i.e., a model) of the system and its economic environment. This model must also be accessible to those senior managers charged with making systems security decisions.

These observations lead us to establish a methodology (hereafter called *trust economics* methodology) that consists of the following main aspects:

1. identify possible IT solutions and the system properties

[*] All authors supported by UK DTI grant P0007 (Trust Economics). Contact author e-mail: aad.vanmoorsel@newcastle.ac.uk.

[†] Supported in part by UK EPSRC platform grant EP/D037743/1.

[‡] Supported in part by EU FP7 coordination action project 216295 (AMBER), EU FP6 network of excellence (ReSIST) and UK EPSRC e-science grant EP/C009797/1.

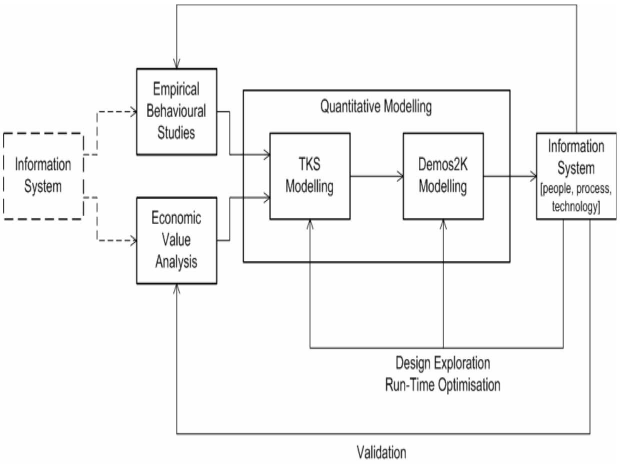

Figure 1: Combination of Modelling and Analysis Techniques

they achieve;

2. assess economic or financial impact of IT security solutions and policies;

3. determine how humans interact with or respond to IT security solutions, typically through empirical studies of human decision making;

4. apply probabilistic and stochastic modelling tools to determine the consequences of IT security decisions, using the understanding gained from item 1 through 3.

We discuss the trust economics methodology in detail in Section 2. We then apply this methodology in an information security feasibility study of USB memory stick usage (Section 3). This simple example addresses one of the main threats companies have identified, namely the inappropriate use of sensitive internal and external information. We end the paper with a discussion of open issues and main challenges in implementing the trust economics methodology.

2. TRUST ECONOMICS METHODOLOGY

Our proposed methodology relies on techniques from various disciplines, namely finances, economics, human science, computer science, and mathematics, as is apparent from the depiction of the trust economics methodology in Figure 1. Figure 1 is to be read from 'left to right', starting from a base 'Information System'. This initial information system may be a running system or a system design, although in our scenarios we would assume systems users are familiar with. 'Empirical Behavioural Studies' are used to understand how humans use information systems and would react to proposed changes or new technologies. 'Economic Value Analysis' sets the objectives and identifies the links with business goals. A deep understanding of the IT system and these two analysis (that is, the behaviourial and economic value analysis) form the input to the 'Quantitative Modelling'. In our specific methodology, we propose to use TKS and Demos2K, as we explain in Section 2.3. The results from the modelling are fed back into improving the 'People, Processes, Technology' within the information system. A 'Design Exploration' and a 'Run-time Optimisation' loop can be envisaged, as well as a 'Validation' feedback loop, as depicted.

We now discuss in detail the challenges and opportunities behind the main facets of our trust economics methodology.

2.1 Economic Value Analysis

A challenging aspect of the trust economics methodology is to identify the link between IT security decisions and economic or financial consequences. The most common way in which IT is related to business consequences is through service level agreements (SLAs) that include monetary awards and penalties for making or missing service level objectives. Such SLAs provide a very powerful mechanism to determine the financial implications of IT decisions, for instance allowing one to determine the financial benefit of improving system monitoring and performance prediction in service provision systems [16].

It should be noted that SLAs are not yet very well established in the security area, and to assess the impact of security mechanisms and policies we would need to develop meaningful security SLA descriptions first. When SLAs are not present, establishing the economic or financial consequences of IT decisions is much harder. Some literature exists relating software security vulnerability disclosures with their impact on stock prices [18], but such results are difficult to obtain and equally difficult to make use of in our models. (See [2] for a discussion of metrics.) The feasibility case study of Section 3 will underline the challenges this aspect of our methodology faces.

2.2 Empirical Behavioural Studies

The effectiveness of enterprise security policies and technologies very much depends on the way humans (employees as well as operations staff) implement and use these policies. To determine in a meaningful way if a proposed security policy makes trust economic sense, human behaviour needs to be predicted. In our methodology, empirical studies are used to create a model of the human decision-making related to the proposed security policies and technologies.

In our case study, we interviewed users of proposed information security solutions to identify how they acted (or would have acted) in various situations. The empirical studies have shed light on which attack scenarios that the specialist thought was most likely or important. Obviously, not all human behaviour can be expected to surface in interviews, especially not planned criminal behaviour or outlines for security attacks, but we have obtained insight into the threats perceived by IT staff.

The empirical behavioural studies, together with the economic value analysis form the input to the quantitative models we use to decide about IT plans. Moreover, a continuous validation feedback must exists from observation of the IT systems to the empirical studies and the economic analysis.

2.3 Quantitative Modelling

The trust economics methodology contends that investment decisions should be based on analytic models of the behaviour of information systems in the context of the environmental threats they face. We therefore introduce a mathematical framework, together with a modelling philosophy, for capturing the structural and dynamical properties of systems and their associated security operations. The main challenge that we aim to confront is in developing a method for integrating mathematical modelling of the technological aspects of a system, with user models and economic models, as a means to evaluate a system.

Computing science research has established a set of tools for quantitative modelling using discrete-event dynamic systems. Discrete-event dynamic systems is a natural modelling formalisms for man-made systems [7], in which events and corresponding system state changes happen at discrete points in time. To obtain interesting metrics from such models, state probabilities can be computed, either through numerical algorithms or discrete-event simulation. Well-established software tools such as Sharpe [15], Möbius [4] or Demos2K [5] exist to develop the model (using various formalisms, including Petri nets and stochastic process algebras).

One of the challenges the trust economics methodology tries to address is intuitive modelling of the non-formal concepts related to human behaviour. To that end, we envisage several modelling technologies to be applied and extended, and conversions between these models to be established. In our case study we use TKS [8] to mediate between the results of non-formal empirical studies on human decision-making and the formal models we use to evaluate the systems and policies.

3. USB FEASIBILITY STUDY

Protection of data and information is of critical importance to many enterprises, and various IT security products and solutions are available to protect against accidental or malicious data leakage. However, introducing such information security technologies has considerable impact on the operation of the enterprise, since it may impact day-to-day work habits of individuals (e.g., it may introduce restrictions on the material employees may download or upload). For an enterprise to be resilient, we contend that it needs to introduce such new technologies using sophisticated analysis of the impact on employee productivity, costs, etc. In other words, applying the trust economics methodology would establish (or at least improve) enterprise resilience.

The feasibility study targets information security, which is a sensitive issue in many enterprises. In particular, we study how the use of USB memory sticks may put enterprises at risk, and we study the cost and benefits of protection software. A feasibility study is a restricted case study to demonstrate the viability of the proposed methodology. As a consequence, the results we show provide initial insights, but a much more in-depth case study is needed to address IT investment questions of security administrators related to USB protection software.

Employees within an organization may be given a USB storage device upon which to place company-managed data. It is the intention that this data can then be accessed at other locations, such as at an employee's home, in transit between work locations (e.g., on a train), during work presentations, or at a client's premises. As such the adoption of USB storage devices is reserved for those working environments where flexibility in working practices is a requirement. This then correlates with the concept of resilience, in that flexibility is knowingly introduced into the company network to allow employees greater freedom in where they use company data.

The company network may have to interact with USB storage devices that are in or have moved through a number of operational states. Devices can potentially be moved between secure and insecure environments. This may incorporate the modification, addition or removal of data within these environments. Devices may be handled by legitimate users, but also by malicious parties (potentially within or outside the organization). Devices may be encrypted or unencrypted and the data that a device holds may require measured treatment within the company's data management scheme. Devices are intended to be used to store legitimately obtained data (i.e., work files) that correspond to the access rights of the individual. However, one can easily imagine scenarios in which maliciously-oriented carriage of data (e.g., transfer of sensitive files outside of the network), or introduction of viruses or 'malware' into the company domain occur.

We will first review the various security solutions available to protect against USB stick misuse.

3.1 IT Solutions for Information Security

Within the feasibility study, we conducted an in-depth survey and study of the technologies to support the secure use of USB memory sticks [11, 12]. Various software solutions exist that provide control of data security within an enterprise environment. Different categories of products were visited in the survey, such as USB device protection, Digital Rights Management, at-rest disk encryption and operating system solutions (mostly related to the Microsoft Windows OS family).

To address the economic value analysis, [11] lists the cost models and actual prices of various products. This provides figures that can be used as a foundation for the subsequent modelling of the economic factors related to data security. Decisions pertaining to security infrastructure must consider the costs of a complete 'solution', including elements such as cost of IT personnel to run the system, cost of updates and patches, possible cost of tracing and monitoring for unprotected machines, the cost of teaching and informing users, and other hardware and software support. This takes us quite a long way in assessing the cost of a USB protection solution, but a true economic value analysis should also include a risk analysis of security breaches and of breaking regulations, as well as a financial impact analysis of productivity loss caused by the security solution. We finally note that in the marketing literature of the products surveyed, economic considerations are always discussed from the perspective of the enterprise, and incentives for users are difficult to identify and typically not discussed in product and technology documentation.

There are a number of issues regarding human vulnerabilities and productivity that must also be considered. All of the proposed technologies considered the human aspect in their design and product. Tools exist for online training during use of the software, some providing help messages and explanatory text associated with specific security-related activities. We found, again, that the perspective is almost exclusively that of imposing rules on users, with little innovation being put into identifying ways to provide incentives that change user behaviour. The empirical studies provided several examples of the effects of these rules. The intention of the policy, from an organisational view, was to provide confidentiality; the effect on the users was to reduce availability (e.g., one might not be able to show a presentation or prepared document). This impacts both the business (missed business opportunity in the short term, reduction in perceived competence in the long term) and the individual (missed opportunity, embarrassment, doubts about personal competence).

From the operational perspective, a bottleneck and potential vulnerability lies in the role of the IT administrator. Most systems are centrally managed, and any deviation from the defined rules needs approval by the IT administrator. As a consequence, the system's inflexibility may result in productivity loss for employees or at the least a reduction in the capacity of a company to accommodate atypical, unpredictable working practices (see also [12]).

3.2 Examination of Human Behaviour

To obtain an empirical basis for our model, we conducted a study to elicit factors that contribute to corporate and individual security cost. We conducted 17 in-depth interviews with security staff, employees and managers in the two companies who are partners in this research project. The interviews remained anonymous, and were semi-structured, exploring aspects such as the tasks and responsibilities of the interviewees, their perception of the risks facing the company, their attitudes and perceived impact of security metrics, etc. All interviewees were asked about one specific security problem: USB sticks, and we suggested the company was considering making the use of encrypted USB sticks mandatory. We refer to [3] for details, here we sketch the methodology used and highlight some results.

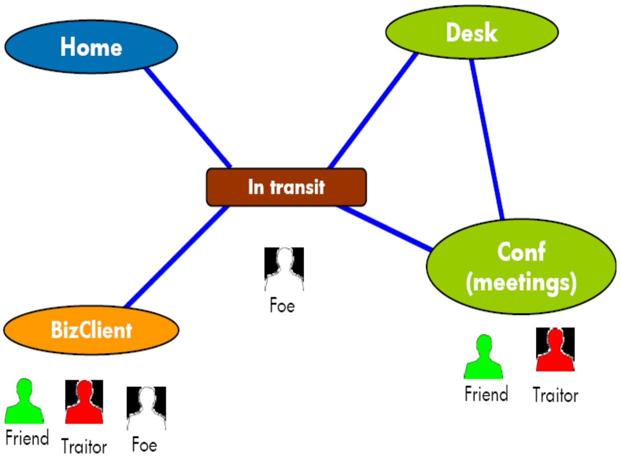

Figure 2: Working locations and their associated threats.

The interviews were transcribed, and analyzed using techniques from Grounded Theory [17], a qualitative data analysis method widely used in social sciences, allowing identification of salient concepts and relationships between them. Over the past 10 years, the method has been successfully applied to model user perceptions and attitudes in human-computer interaction in general [1, 19].

From the interviews we were able to identify two main USB stick usage scenarios. These scenarios broadly corresponded to the type of organization the subject worked for. Here we discuss one scenario in a little more detail. In this scenario, the USB stick is primarily used for temporary storage for transit between locations such as an employee visiting a client company to deliver a presentation. The data required to deliver the presentation would be copied from the companys computer system onto the USB stick and taken to the clients location. Any data which must be brought back to the home company can be copied from the clients system onto the USB stick and brought back by the employee.

The main concern for the security manager in this scenario is the potential confidentiality issues resulting from company data being transported through unsecure locations while in transit to and from the client. If the USB stick was lost or stolen at this time while containing unencrypted data, then the cost in terms of reputation and lost business would be to the company itself rather than the individual. While the company can punish the individual internally, it cannot recoup its losses by doing so. As a consequence, this scenario encourages the security manager to take a confidentiality first approach when designing the USB control policy. The risk model we develop in Section 3.3 which quantifies breaches of confidentiality, uses the above scenario. We refer to [3] for a detailed analysis.

	fraction encrypted	exposures	confidentiality loss	mean time between exposures
no traitors	80%	4.18	9.68	755.5
with traitors	80%	7.72	98.46	357.7
no traitors	100%	3.90	0	948.0
with traitors	100%	8.06	125.67	356.8

Table 1: Confidentiality Loss, depending on the encryption level and the existence of traitors.

3.3 Mathematical Systems Modelling

The mathematical model that is the core of the trust economics methodology (see Section 2.3 and the box 'Quantitative Modelling' in Figure 1) needs to account for the following: (i) the environment (economics, threats, human factors, etc.) within which the system exists; (ii) the (distributed) location structure of the system; (iii) the resource elements that are scattered around that structure (including people); (iv) the processes that execute on top of all of (i)-(iii) (including human behaviours). Our approach is that of classical applied mathematics. We use techniques from algebra, logic, probability theory, queuing theory, and theoretical computer science [13, 14], and we make use of the Demos2k tool kit [5] that provides a realization of some of the above modelling methods.

We have already mentioned in Section 3.2 the various ways people told us they use USB sticks. Although there were several different usage scenarios described, it was possible to abstract common ways in which USB data sticks were used, e.g., transfer of data between colleagues and business partners. Figure 2 depicts the different players in these scenarios. For details of the Demos2k model, we refer to [3].

Based on the interviews, our model exhibits a player called 'Friend' to represent legitimate recipients. At first sight, it may seem surprising that business data could be taken into a home environment. Many modern businesses recognise, however, the practicality of employees working on projects at home. In changing location, the holder would often need to use transport such as car, train and plane, or use a hotel. These transient locations represent places at which the USB could be lost, and potentially be recovered by an adversary (i.e., 'Foe'). The other main places at which data could be captured by adversaries are clients (i.e., external business situations, conferences and such like), and in dealing with people masquerading as Friends (i.e., 'Traitors').

There are also risks associated with data capture, namely exposure of a USB containing confidential information by an adversary in a context where they can freely extract the information. This is potentially very serious and can lead to severe reputation damage to the organisation and individuals concerned, especially if the information is subsequently used in a publicly damaging manner (i.e., business advantage, press leaks). The cost of these breaches could be very high. In our model, we assume that, once the USB is under an adversary's control, there is some probability that the information will be exposed. We handle this probabilistically to reflect the fact that exposure is not a perfect operation. Accidental archiving of USB-held material (either encrypted or unencrypted) onto someone else's PC is considered a milder form of exposure that can lead to personal embarrassment of the employee, but generally does not have direct external consequences. The cost of these breaches to the corporation is much less.

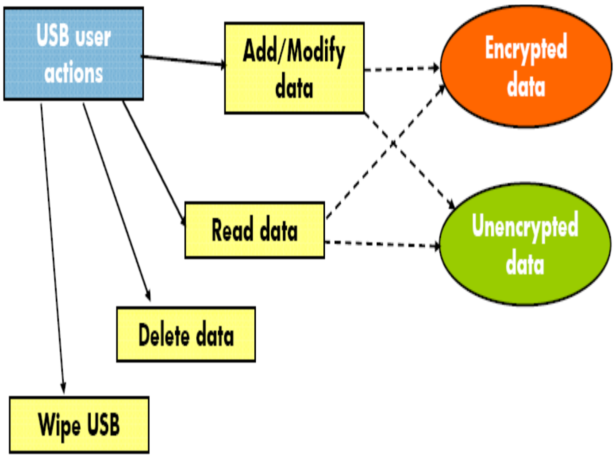

Figure 3: Common USB user actions.

To incorporate all the above, the model represents 'a day in the life' of a USB memory stick. The common tasks undertaken by the user (shown in Figure 3), such as manipulating data on the memory stick, exchanging data with a colleague or replacing a lost memory stick, are represented explicitly in the model. In turn, these entities are built from the fundamental operations of adding, reading, and deleting encrypted and unencrypted data from the memory stick. Concurrently, a movement entity changes the location of the memory stick and its user according to Figure 2, between different types of work location, home, and 'in transit', with the relative frequency of the different tasks and events changing at each location.

Some initial results are given in Table 1, for one year of USB use. Confidentiality loss is the product of number of exposures and the amount of data that can be seen (a Traitor can see all data, including encrypted data, while a Foe can only see unencrypted data). The main result obtained from the simple initial model is that encryption can provide a perfect solution, but only if there are no traitors in the organisation. If traitors are present, encryption can only be a partial solution. The main message is to reduce the possibility of traitors, and manage their presence through a holistic, policy-driven approach to vetting and information security management.

4. CONCLUSION

This paper introduces the trust economic methodology to improve decision-making about IT security. The trust economics methodology bases investment decisions on analytic models of the behaviour of information systems in the context of the environmental threats they face. It consists of a mathematical framework, together with a modelling philosophy, integrating mathematical modelling of the technological aspects of a system, with user models and economic models, as a means to evaluate a system. The methodology improves enterprise resilience by providing tools that allow the enterprise to better react to or introduce change.

The presented USB feasibility case study demonstrates the application of the methodology to enterprise information security decisions. Considerable research challenges have been uncovered during the feasibility study. These include establishing and quantifying economic and business impact of IT decisions, capturing human decision-making, developing realistic attack and vulnerability models, and enhancing the modelling techniques. To leverage the established trust economics methodology it is important to create intuitive tool support for IT staff, and where appropriate achieve automation of the trust economics based decision making process.

5. REFERENCES

[1] A. L. Adams and M. A. Sasse. Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12):40–46, 1999.

[2] R. Anderson, R. Böhme, R. Clayton, and T. Moore. Security economics and the internal market, 2007. European Network and Information Security Agency.

[3] A. Beautement, R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, A. Sasse, and M. Wonham. Modelling the human and technological costs and benefits of USB memory stick security, 2008. submitted for publication; available upon request.

[4] G. Clark, T. Courtney, D. Daly, D. Deavours, S. Derisavi, J. M.Doyle, W. H. Sanders, and P. Webster. The Möbius modeling tool. In *Proceedings of the 9th International Workshop on Petri Nets and Performance Models*, pages 241–250, 2001.

[5] Hewlett-Packard Company. Demos 2000, 1994-2008. `www.demos2k.org` (and papers mentioned therein).

[6] J. Fiksel. Designing resilient, sustainable systems. *Environmental Science and Technology*, 2003.

[7] Y Ho. Dynamics of discrete event systems. *Proceedings of the IEEE*, 77(1):3–6, 1989.

[8] H. Johnson and J.K. Hyde. Towards modelling individual and collaborative construction of jigsaws using task knowledge structures (TKS). *Transactions on Computer Human Interaction*, 10(4):339–387, 2003.

[9] H. Lacohe, S. Crane, and A. Phippen. Trustguide: Final report. *Hewlett-Packard*, 2006.

[10] Office of Science and Technology. Foresight: Cyber trust and crime prevention project: Executive summary. *UK Department of Trade and Industry*, 2004.

[11] S. Parkin and A. van Moorsel. A trust-economic perspective on information security technologies. Technical Report CS-TR 1053, Newcastle University, School of Computing, 2007.

[12] S. Parkin, R. Yassin Kassab, and A. van Moorsel. The impact of unavailability on the effectiveness of enterprise information security technologies, 2008. accepted for Int. Symp. on Service Availability.

[13] D. Pym and C. Tofts. A calculus and logic of resources and processes. *Formal Aspects of Computing*, 18(4):495517, 2006. Erratum (with Collinson, M.): Formal Aspects of Computing (2007) 19: 551-554.

[14] D. Pym and C. Tofts. Systems modelling via resources and processes: Philosophy, calculus, semantics, and logic. *ENTCS*, 172:545–587, 2007. Erratum (with Collinson, M.) Formal Aspects of Computing (2007) 19: 551-554.

[15] A. R. Sahner, S. K. Trivedi, and A. Puliafito. *Performance and Reliability Analysis of Computer Systems*. Kluwer, Norwell, MA, USA, 1996.

[16] C. Smith and A. van Moorsel. Mitigating provider uncertainty in service provision contracts, 2007. Workshop on Economic Models and Algorithms for Grid Systems.

[17] A. L. Strauss and J. M. Corbine. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage, Newbury Park, CA, USA, 1990.

[18] R. Telang and S. Wattal. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Trans. Software Eng.*, 33(8):544–557, 2007.

[19] D. Weirich and M. A. Sasse. Pretty good persuasion: A first step towards effective password security for the real world. In *Proceedings of the New Security Paradigms Workshop*, pages 137–143. ACM Press, 2001.