

# Information Security Economics: Some Developments in HP Labs and the UK Cyber-security KTN

David Pym  
HP Labs, Bristol and  
University of Bath

## Information Security Economics: A Systems Perspective

## What is information security economics about for industry?

- Need for security because services interact with bad guys.
- Services are delivered by systems.
- But a system has many (types of) component.
- Systems exist in economic environments.
- The risk associated with a service is derived from the characteristics of the system and its environment.

## Systems

- Systems consist of more than just their technical 'core':
  - They connect to other systems;
  - They interact with people;
  - They interact with business processes.
- External to the technical core are:
  - The economic environment;
  - The threat environment.

# Security

- Some dimensions:
  - A definition (Wonham): ensuring that just the right people have access to just the right information at just the right times;
  - Protecting the system/service against threats to confidentiality, availability, and integrity (CIA).
- Different (types of) organization(s) have different priorities for their CIA profile. How to determine what are the acceptable trade-offs?
- Security policies are intended to promote/enforce an organizations priorities.

# Economics

- Many points of view here.
- But a few thoughts:
  - Not *just* about microeconomics: the incentives of the players in the 'security game' are an important part of the analysis;
  - Possible applications of macroeconomic and financial modelling methods (e.g., the central bank analogy);
  - Information security as a public good? Mechanism design?

## Risk

- Risk cannot be assessed in isolation. That is, significant problems with traditional accounting methods (NPV, RoI, ALE, say) in this space.
- Risk *for a system/service* can only be assessed in the context of the economic and threat environments (e.g., CIA priorities).

## Understanding it all

- Modelling for prediction:
  - Aim to build (mathematical) models of the complete system and its economic and threat environments;
  - Need to integrate user, system, and economic models;
  - Critical work at levels of abstraction that keep it real.
- Can then sensibly model/assess risk.
- This is the objective of ...

# Money

- How will we make some?
  - Make information security a core, enabling part of systems and service delivery.
  - May be necessary for national governments to take a lead (public good).
  - Potential discriminator for systems/services suppliers and for regional/national economies.
  - And some more I'm not able to talk about ... .

## The 'Trust Economics' project

- Funded by the UK's Technology Strategy Board (about £1.7M over 3 years, including industrial contributions).
- Partners: HP Labs, Merrill Lynch, University College London, University of Bath, University of Newcastle.

# A Case Study: Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security

## The USB Memory Stick Problem

- Context: Financial Services Industry.
- Staff use USB memory sticks for good reasons (availability, back-up, convenience, and more).
- Often the data being carried is confidential (to the bank, to the customer).
- Sticks used in many different locations (desk, home, transport, client).
- Different types and intensities of threat in different locations.

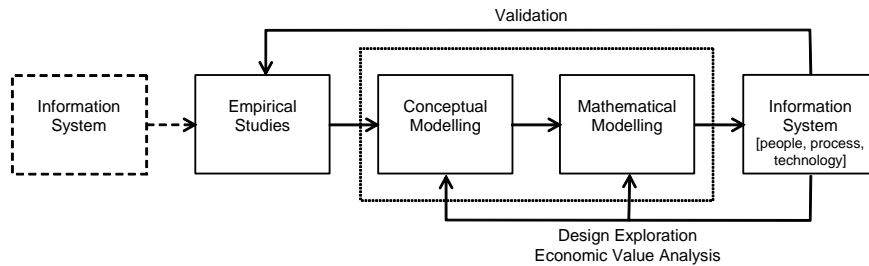
## An Example of What?

- A good example of the more general problem facing (information) security officers.
- How to design policies, and make appropriate supporting investments, to achieve the desired outcome for the business process and regulatory environment?

## The Study

- Understand what influences the use of encryption with USB sticks.
- Hypothesis: confidentiality (promoted by encryption) trades off against availability.
- Obtain empirical data by conducting semi-structured interviews.
- Construct a (mathematical, but executable) process model of behaviour based on this data.
- Consider the utility derived from results using an economic model inspired by the Central Bank Problem.

# The Basic Methodology



## The Background Economic Model

- Inspired by the macro-economics ‘Central Bank Problem’:
  - Interest rate instrument;
  - Trade off unemployment ( $u$ ) against inflation ( $\pi$ );
  - (Asymmetric) utility function.
- Roughly,  $u = u^n - c (\pi - \pi^f) + d$ .
- *Utility*  $(u, \pi) = a (u - u_0)^2 + b \text{Linex} (\pi - \pi_0)^2$ , where *Linex* denotes a linear-exponential function as used by Varian, Zellner, and others, and  $u_0$  and  $\pi_0$  are target rates of unemployment and inflation.

## Analogy for Information Security

- Consider confidentiality, integrity, and availability.
- For our purposes, neglect integrity and trade off confidentiality against availability.
- The instrument is investment information security (alternatively, system complexity).
- For the results of this study, take the simplest conceivably useful set-up:
  - Confidentiality depends linearly and negatively on availability, with a stochastic threat term;
  - Availability depends linear on security investment;
  - Simplest conceivably useful utility:  
 $U(C,A) = \alpha(A - \beta C)$ , where  $\alpha$  and  $\beta$  are parameters derived from the system/process model. Not attempting optimization here — utility function too trivial.

## The Empirical Study

- 17 in-depth studies with employees, managers, and information security staff.
- The interviews were semi-structured, exploring
  - the tasks and responsibilities of interviewees,
  - their perception of the risks facing the company,
  - their attitudes to the company's security polices and security measures, and
  - the perceived impact of security measures on individuals' tasks and responsibilities, and company productivity.
- Then asked a range of questions about their USB stick usage; in particular, to understand the factors affecting the use of encryption.

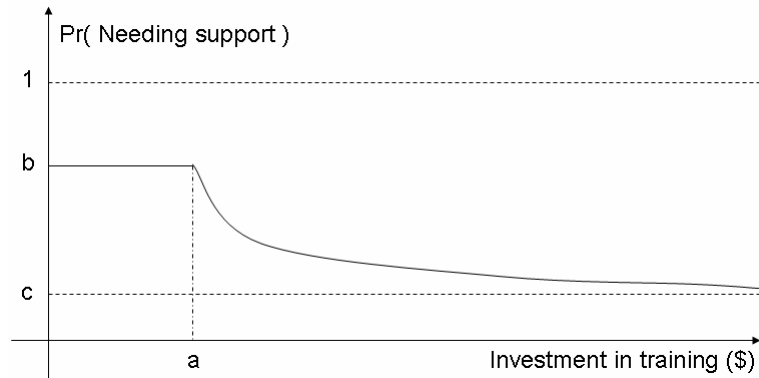
## Analysis of Interview Data

- The interviews were transcribed, and analyzed using techniques from Grounded Theory.
- Grounded Theory is a qualitative data analysis method widely used in social sciences, which allows identification of salient concepts and relationships between them.
- The method has been applied to modelling user perceptions and attitudes, including identifying factors that affect employees' perceptions of corporate security policies, and modelling employee decision-making on compliance with password security policies.

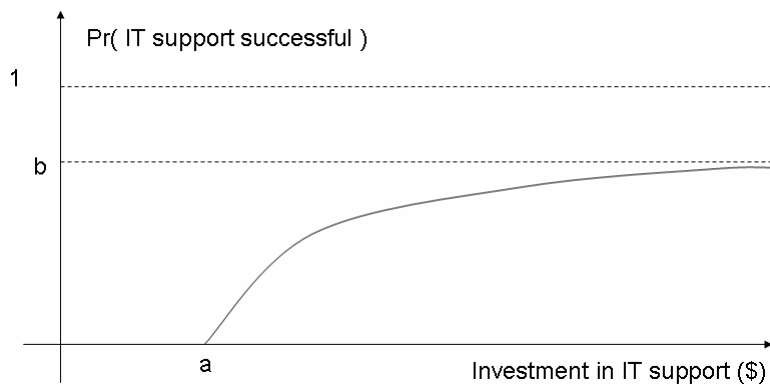
## The Process Model

- Conceptual: the intermediate step from the Grounded Theory to the executable mathematical model.
- Based around three types of investment:
  - *Training* — individuals are trained to understand and work within the organization's information security policies;
  - *IT Support* — the organization provides specialist IT personnel to help individuals resolve problems;
  - *Monitoring* — the organization monitors the behaviour of the individuals with respect to its information security policies.
- Associate with each of these a 'transfer function', understood from the empirical data, which expresses the contribution of each factor to the probability of the use of encryption.
- Probability also depends on some functions capturing an individual's scoring of various factors (see the paper).
- Capture the lifecycle of a USB stick (as employed by a typical individual).

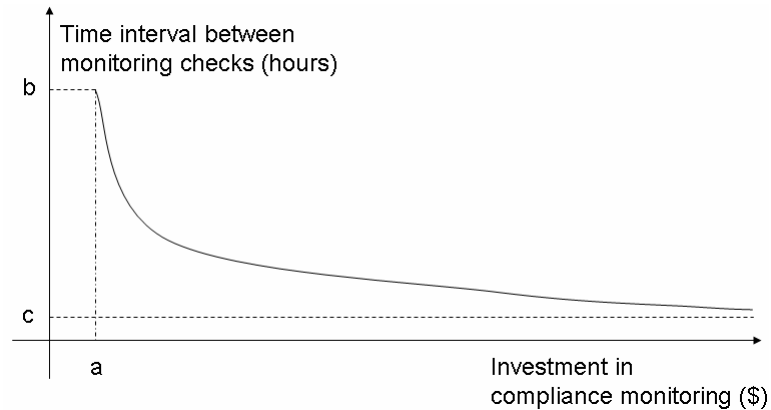
## 'Training' Transfer Function



## 'IT Support' Transfer Function



# 'Compliance Monitoring' Transfer Function



## The Process Model

- Executable: written in the 'Demos2k' language ([www.demos2k.org](http://www.demos2k.org)).
- Executable models based on (i) mathematical models of resource and process, and (ii) probability distributions and queues.
- Development and reimplemention under way — better modelling structures, better semantics, better system structure.

## Some Results

- Results
  - Investments have a binary effect on compliance (likelihood to encrypt); i.e., at a certain point we switch from 10% to 90%.
  - Asymmetry between confidentiality and availability (i.e., can get much more confidentiality without much loss of availability).
  - This suggests a sweet spot for investment!
- Surprising (Scientific) Conclusion
  - It is possible to integrate inputs from the different disciplines!

## Directions

- Explore the (family of) economic models suggested by this framework more fully. In particular, seek solutions, look at shocks, and more.
- Improve the process modelling framework better to capture distributed system structure (i.e., location).
- Employ richer cognitive/behavioural models.
- More studies in the similar style.

## Cyber-security KTN: Economics of Information Security SIG

### What's it about?

- What is the value of information security?
- How should organizations invest in system security — in people, process, and technology — to support their security policies and business objectives?
- How can organizations understand their information security profiles (CIA, etc) in their business contexts?
- What is the appropriate supporting economic theory?

## Possible activities

- Community building — an ongoing forum.
- Data sharing protocol — no data, no economics, except at a conceptual level.
- Education: e.g., influence MBA and PhD programmes? Undergraduate programmes?
- Workshops on, for example, the economics of corporate citizenship or individual privacy.
- Where can economic theory help?
- Working party to produce a report on the state of the cost-effectiveness of UK individual, institutional, and corporate information security.

## Stakeholders?

- Research councils (ESRC, EPSRC), TSB.
- Government Departments: Cabinet Office, DIUS, BERR, Home Office, Health, etc.
- Business leaders
- Universities/academics
- Industry bodies, CPNI (UK's Centre for the Protection of National Infrastructure), consumer groups

# Contact

- Prof. David J. Pym
- Systems Security Lab, HP Labs,  
Bristol BS34 8QZ
- Email:
  - [david.pym@hp.com](mailto:david.pym@hp.com)
  - [d.j.pym@bath.ac.uk](mailto:d.j.pym@bath.ac.uk)
- Web:
  - [www.hpl.hp.com/personal/David\\_Pym/](http://www.hpl.hp.com/personal/David_Pym/)
  - [www.cs.bath.ac.uk/~pym](http://www.cs.bath.ac.uk/~pym)