

Risk Assessment & Benefits Model – Report of Progress

Key Action(s) from Previous Meeting

A point of leverage would be the banks, who understood risk assessment; several individuals might be approached on the issue of security. The group should make the approaches to plan what areas to focus on and to scope the nature of the risk assessment study as part of the forward progress for the group. **It was agreed to contact key personnel on this issue.**

Outcome: Contacts provided in the Banking sector were unable to provide opportunities for the discussion of issues to enable a focus on variables as a baseline for the risk assessment model. Companies appear understandably sensitive, for reasons noted in Jim Lound's presentation during the last meeting (28th Oct 2004).

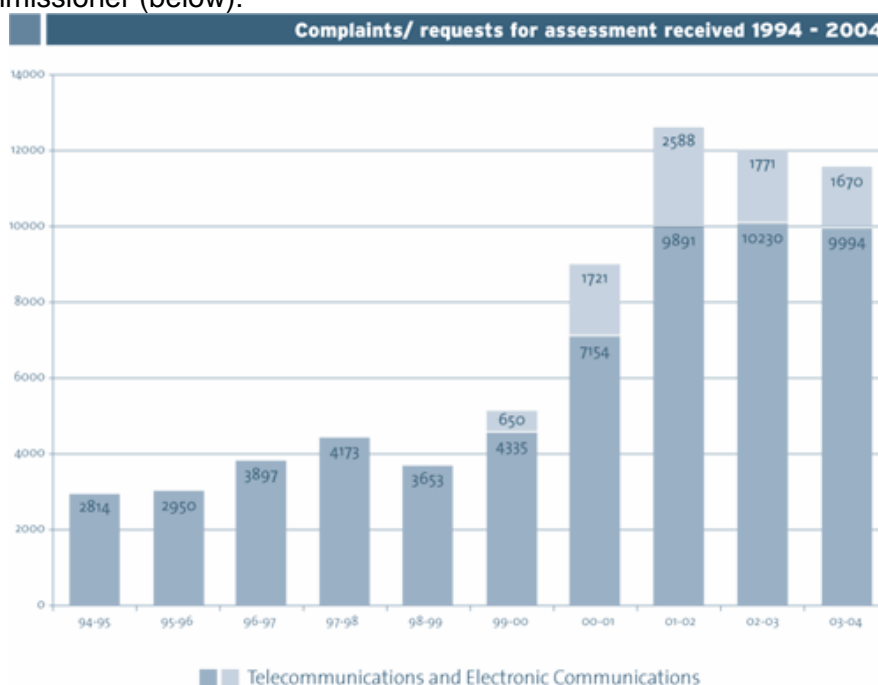
Proposed Remedial Actions:

1. Reduce the Complexity & Scope of Risk Assessment Model
2. Build simple straw man for public and private sector data controllers in Circle of Trust Model.

2a: Public Sector - FOI Act may allow the provision of some data from the public sector on statistics we may use as a baseline for the risk model for data sharing.

2b: Private Sector – It may be unreasonable to expect industry to share with us numbers on the false positives and false negatives created during data sharing transactions as they will always consider these commercially sensitive.

We need not be so pessimistic, however. One end of the continuum could be the relatively positive view suggested by the statistics reported by the Information Commissioner (below):



A broad brush approach suggests that if the 9,994 figure (i.e. excluding the telecoms and electronic communications stats) for 2004 is taken and compared with the UK's population (estimated 60 million total, not adult only – to retain a

deliberately optimistic approach), then we have a broad risk profile of 0.02% nationally.

Research using APACs data suggests a UK industry risk baseline of about 0.2% by value. Ideally we should use the volume of transactions (data to be obtained), but for the sake of illustration we could use between 0.2% and 0.02% (APACS figures and Information Commissioner's figures respectively) as a broad brush baseline for the risk model.

What we could do next, perhaps, is apply one or other figure within this range to the data controller categories referred to in the Data Sharing Grid distributed at the 28th Oct 2004 meeting. This could be done at a specially convened workshop as Dave suggested, where we (i) apply risk numbers as baselines (treated as probabilities of data sharing security lapses that lead to costs to one of the stakeholders) and then (ii) add, for each category of data controller, the number of transactions that they conduct annually. These two figures multiplied will create the projected risk profile of data loss per type of data controller.

Then we can apply a "cost" to the stakeholders concerned and we have an assessment that can be put up for scrutiny.

To aid our thinking in applying the different risk profile numbers to the model, we might use the data below (again from the Information Commissioner) which shows mismatches between the awareness of rights at data controller and data subject (individual) level:

Public Awareness and Awareness of Rights

Data Protection	Actuals	Ests/Targets	Actuals	Ests/Targets	Ests/Targets	Ests/Targets
	2002/2003	2003/2004	2003/2004	2004/2005	2005/2006	2006/2007
% Total data controllers aware of subjects rights	92%	94%	89%	92%	94%	96%
% individuals aware of own rights	74%	78%	74%	75%	75%	76%
Freedom of Information						
Freedom of Information	Actuals	Ests/Targets	Actuals	Ests/Targets	Ests/Targets	Ests/Targets
	2002/2003	2003/2004	2003/2004	2004/2005	2005/2006	2006/2007
% individuals aware of own rights of their obligations	49%	50%	56%	60%	63%	65%
% of public authorities aware	53%	60%	84%	95%	98%	98%

The figures are based on annual tracking research in the spring of each year.

We might also take the assumption that "More data-sharing has the potential in principle to be detrimental to data quality. For example:

- with wider access and use, external - i.e. users outside the department which originally collected the information - or inexperienced users may create errors;
- with increased external use, there is greater potential to spread errors; and,
- the existence of multiple users may blur 'ownership' of the database and with it the loss of responsibility to supervise database practices and maintain quality."

<http://www.number-10.gov.uk/su/privacy/07.htm>

It is acknowledged that all of the above data can be refined and tweaked, and no doubt will. Nevertheless, this document aims at building a "Straw Man" to enable refinement and use of a risk and benefits analysis model for decision support.