

The Pursuit of Trustworthy Information Systems in the New Millennium

Today and for the foreseeable future, new public policy issues are brought up by advances in communication and information technology. The Internet is much more than an apparatus for moving bits of information around the world – it generates whole new patterns of behaviour and whole new possibilities for everyone. ‘Everyone’ means what it says – the terrorist as well as the educator, the law abider as well as the criminal. Presented with a kaleidoscope of good and bad, our governmental, legal and regulatory infrastructures have to decide what to do.

In a democracy, such decisions should be made on the basis of informed debate between those responsible for these infrastructures and the public. Unfortunately, a number of the issues are quite technical. Actions that look obviously desirable may prove to be technically very difficult or expensive, or may turn out to inhibit conduct that is valued or enhance conduct that is deplored. There is no common currency in the weighing of enhanced law enforcement against loss of personal privacy. Legislation that was perfectly sensible in a former environment can turn out to be unsuitable now. New procedures for electronic commerce, for example, while aiming to make transactions quicker and easier, can produce an

undesired and unmentioned redistribution of risk between participants.

Recent events, both creative, such as the successful cloning of higher species and the near completion of the human genome project, and destructive, such as the BSE crisis or attacks of 11 September, have put a great deal of information stress on the population. When experiencing such ‘future shocks’, it is common to react as if there are no relevant expertise or skills to bear and to make up policy ‘on the fly’.

In information systems, there is in fact a large body of expertise and a collection of skilled individuals and organisations who are able to draw upon previous situations and make sense of alternative reactions in a calm and considered way.

The way that government agencies, businesses, private organisations and individuals interact through information systems is evolving very quickly. The rapid introduction of databases describing us and our property, our history and our future (e.g. insurance and online transaction systems between organisations and individuals) has been faster than any rate of uptake of technology in the past. Compare the rate of change of the Internet and the Web with the timescales for the migration from early printing press to paperback books, or the millennia

associated with the transition from the use of banknotes to the introduction of debit cards. Compare the time it took from its first use for the PC to become all-pervasive with the rate of transition from the use of papyrus to paper.

Modern manufacturing and communication systems not only enhance the pace of change, but also the complexity of organisational relationships. It is expected that cultural and business relationships will now be global. Many global companies now do no manufacturing themselves, but outsource the process in a number of places. Because of cultural, political, economic and legal differences, this leads to exponential growth in the complexity of the information associated with such relationships. There are no longer any real simple hierarchical chains of government and trust.

Privacy is a major issue. Correlation of different sets of personal data can seriously erode personal privacy. All too often we fail to define the use of data accurately. The Data Protection Act goes some way towards requiring the keeper of personal data to define use. However, there are exceptions and, even when not, there is little attempt to ask users to think about risk, cost, conflicts and roles of information users.

We do not ask people for a clear exposition of their expectations, for example, for reliability of information

and change control. We do not have adequate tools to describe the behaviour of information users, nor for the managing the acceptance of information use amongst subjects. Neither message secrecy nor de-identification of records is sufficient for privacy. Ill-informed people often see encryption as a panacea in this area, which it emphatically is not.

The public understanding of risk in security systems must include the notion also that there are no 'zero defect' approaches. The policy must

make clear what are the priorities (privacy, safety, etc.) and the engineering of the systems must make transparent that the policy has been captured in the operational system.

'The price of freedom is eternal vigilance'. The price of information systems security (privacy, integrity, reliability, trustworthiness, affordability, usability, etc.) lies in the education and proper resourcing of the overall system. It is not simply a naïve combination of hardware with underpaid, undertrained, overloaded staff.

Most studies show that the vast majority of security system failures are caused by people – either accidentally, deliberately, or in complex combinations of unintentional and intentional actions. ■

[The authors are members of the Foundation for Information Policy Research. FIPR (www.fipr.org) seeks to enhance the quality of debate by producing clear statements on the issues at stake and reasoned proposals for policy improvements].

Lecture Programme



ROYAL
ACADEMY
of
ENGINEERING

The 2002 Hinton Lecture

Delivering the National Rail Infrastructure

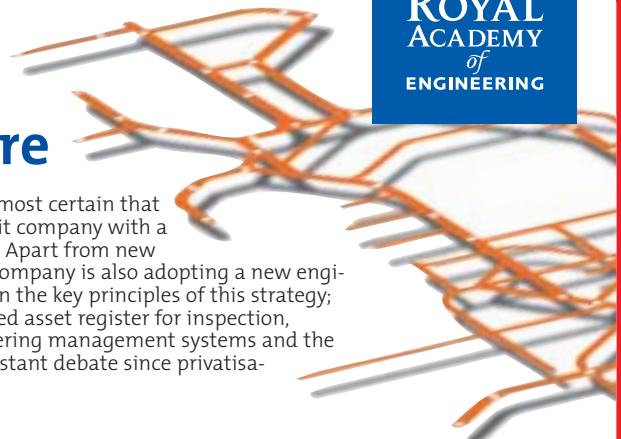
Speaker:

John Armitt CBE FREng
Chief Executive, Railtrack PLC

Venue:

7 Carlton House Terrace
London SW1

By the time of the Hinton Lecture, it is almost certain that Railtrack will have become a not-for-profit company with a new broadly based 'ownership' structure. Apart from new ownership and business objectives, the company is also adopting a new engineering strategy. This lecture will focus on the key principles of this strategy; the development of a new condition based asset register for inspection, repair and renewal technologies, engineering management systems and the contractual relationship, a subject of constant debate since privatisation, which will deliver the new strategy.



THE 3Rs: LESSONS LEARNED FROM SEPTEMBER 11TH

Speaker:

Robert Prieto
Co-chair, New York City Partnership
Infrastructure Task Force

Venue:

7 Carlton House Terrace
London SW1

An analysis of the events of September 11th and the immediate recovery effort provides valuable lessons for engineers who must determine how buildings and infrastructure should be designed and built to provide a reasonable degree of security while at the same time remaining accessible, accommodating and an integral part of the urban fabric. The built environment of the 21st century must be able to resist, respond and recover from unforeseen and unimaginable acts of nature and of man.



Sponsored by



To reserve a seat please contact:

The Royal Academy of Engineering
29 Great Peter Street, Westminster, London SW1P 3LW
Telephone: 020 7222 2688 Facsimile: 020 7233 0054
Website: www.raeng.org.uk
Registered Charity No. 293074

All welcome, admission free