



Event Sponsors:



Alcatel-Lucent



DeLaRue



Supporters:



**DIRECTORS' ROUND TABLE, 24 NOVEMBER 2008**

**NB: THIS EVENT IS NOW FULLY BOOKED**

Business risks being driven overseas by the cost of regulation that is not only irrelevant to good business practice but opens up more vulnerabilities than it addresses. Legislation mandating or forbidding the retention or disclosure of information that is no longer needed for business purposes is set to get worse at a time when confidence has collapsed in the ability of large organisations, including government and regulators, to keep it secure.

The recent crisis in the banking industry brings into sharp focus some of the critical challenges posed to companies to maintain an appropriate information governance regime. Such pressures suggest the increasingly vital importance of establishing information governance regimes across both public and private sectors which not only command professional and public support but also encourage and reinforce good (including efficient and profitable) business practice.

But how can and should good practice be identified, fostered and enforced? How much is about people processes rather than technology? Should the agenda be driven by industry, the professions, government or regulators - given that officials now appear less trusted than business, albeit more than politicians or journalists?

And who is willing to lead? Who is willing to follow them? Who is willing to contribute what to making it all happen?

The objective of this Directors Round Table event is to identify whether there is the WILL, on the part of large organisations and their legal advisors and auditors, to take a lead in rebuilding confidence that their information governance is fit for purpose in a world where data loss can destroy competitive advantage.

If so, we will organise a short order follow up meeting to launch a working group to bring the necessary players together and ensure action – professional, practical, political and regulatory.

Sir James Crosby will give the keynote speech which will be followed by four short introductory contributions from Professor Jim Norton (Institute of Directors); Dr Louise Bennett (Chair of The Security Forum Strategic Panel); John Suffolk (Government Chief Information Officer) and Carlos Solari (Vice-President for Security, Strategy and Solutions, Alcatel-Lucent).

Philip Dunne MP (Parliamentary Chair of EURIM's Information Governance Group) will then chair an off-the-record discussion. Stephen Darvill (Logica, Industry Chair of EURIM's Information Governance Group) will provide a concluding summary, and Margaret Moran (EURIM Chair) will close the event.

## KEY RECOMMENDATIONS FROM CONTRIBUTED PAPERS

### Leonard Anderson, SOCITM – Information Governance for Sharing Personal Data

In the context of multi-agency information sharing, much information governance guidance has already been documented. Guidelines produced in the FAME National Project have been used to prove the applicability of an all embracing set of processes involving practice outcomes, governance and technology. Information Governance is but a small part. Partnerships are the way forward; all stakeholders need to agree on a common language and roadmap. Public sector technology is accused of ignoring the impact of international standards. Kent Connects is taking a leadership role in using FAME to develop the business case for the KUDOS partnership.

### Louise Bennett, BCS – Responsibilities for personal data holdings

The main information governance requirements are:

- Clear responsibility accountability and authority for information management.
- Training of all staff in the information's purpose, handling and protection.
- A clear understanding and management of processes associated with the introduction and use of new databases.
- Appropriate security systems for the protection of the organisation's data and information, including business continuity planning.
- Simple clear documentation of the organization's use of and dependence on information that is followed throughout the organization.

### Colin Beveridge – Measures for preserving stakeholder confidence

This paper sets out a summary of straightforward, easily-adopted yet effective, measures to help organizations gain and preserve stakeholder confidence in information governance.

The author challenges the presumption that changes to the political or regulatory process will help to identify and encourage best practice because such [legal] changes could only realistically follow, rather than lead, suitably effective practice. Properly-considered legislation/regulation is therefore unlikely to provoke timely remediation of the already pressing problem of diminished stakeholder confidence.

The most plausible solution is a concerted, sustained and timely effort to prevent further high-profile incidents, through immediate and direct improvement to practice.

### Tim Boswell MP & others – Motion for a Resolution to the Council of Europe Parliamentary Assembly: Identity Documents & Databases

"Noting the right of member states to require their citizens and nationals to carry identity documents and recognising the importance of effective and co-ordinated measures to combat the growing threat of extremism and terrorism; noting that not all member states currently require citizens to carry identity cards and that some are planning to: We urge the Assembly to prepare a code of conduct for introducing identity documents based on the criteria.. [in this document]."

### John Bullard, IdenTrust – Avoid re-inventing wheels

The world's regulated financial institutions have centuries of experience in vouching for their customers' authenticity, their standing, their credit, and their due performance. In a world of ubiquitous electronic networks, where data/information and money are synonymous, these qualities and requirements are no less important than in the paper world, and these same institutions are ideally equipped to perform the same role. We may not always like them but we trust them. Being the most highly regulated sector of any nation-state economy, the combination of local control and yet global contractual reach represents the way to ensure resilient Information Governance standards. The foundation stones exist today in the UK, and worldwide.

### **Andrew Cooke, Atkins – Would you rather lose your business from too little or too much Information Governance?**

Now is not the time to introduce draconian security processes. Now, more than ever, good professional balance is needed to identify risks realistically and to apply countermeasures that will reduce risks in practice. Now is a time for everyone to find ways to ensure that disclosure of personal data cannot lead to serious consequences for individuals – by requiring strong authorisation before financial commitments are agreed, and by acting together to ensure that individuals who live their lives under physical threat should have their whereabouts comprehensively protected across Government and other major institutions.

### **CSC – Secure Data - A Government Challenge**

Over recent months a number of high profile data losses from Government departments have been reported. These concerns are being raised at a time when there is a drive to have a more 'joined up' Government by reducing duplication and optimising collaboration across Government departments through the use of technology. More legislation is unlikely to assist in ensuring data safety as the reported incidents were all in breach of existing legislation. This paper looks at how Government might go about rebuilding confidence, what best practice looks like and the solutions that should be put in place and by whom.

### **Bob Darby & Pat Ellison, Barnardo's – Information Governance : Barnardo's Perspective**

The paper sets out the challenges for Information Governance which are posed by the current agenda for multi-agency working as experienced by a large voluntary organisation working with children and families. It links those challenges to the Transformation programme, through which local authorities have been funded by central government to modernise the back office systems and processes which support the delivery and monitoring of services to citizens. It argues that an unenlightened approach to the information requirements of multi agency working can threaten the independence, effectiveness and sometimes the continuing existence of partner organizations in the voluntary sector.

### **David Fatscher, BSI – The Importance of Standards**

The wheel does not need re-inventing! Standards are the universal language for supply chain management.

The most effective method of building internal systems to safeguard sensitive information and educate data-handlers is standards-based.

As poor organizational culture is commonly-acknowledged as the single biggest barrier to effective Information Governance, centring a staff education programme around agreed best practice clearly makes sense.

Laws seldom prevent what they seek to forbid. Standards are a form of 'lighter-touch' regulation, and can be a swift-but-considered response to developments in technology.

### **Global Trust Center/Metanoya (UK) – A Proposal for - Rights and Responsibilities for Citizens in the Digital World**

In every environment where mankind exists, we need to understand our roles, rights and responsibilities. This is certainly the case in the digital world which has existed for less than two decades but has become omnipresent. There has been no time for roles, rights and responsibilities to be established as they have in the real world. A clear set of rules needs to be developed to define structure and acceptable behaviour so that it does not descend into anarchy, thus destroying all of the positive impact of the digital world. Protecting the citizen is only one side of the coin, we must also understand the responsibilities that go hand in glove with these rights.

### **Andrew Hardie – Information Governance - Just Say No!**

Government data losses have brought Information Management centre-stage. Political alarm risks hasty legislation and more bureaucracy. The recommendations of numerous reports bring new risks including more complexity in areas criticised as too complex. Proposals for greater system integration ignore research indicating negative outcomes because of unexpected side effects. Management fears risk unworkable procedures and ill-judged technology-based solutions which achieve 'compliance', but ignore the human dimension of the issues. Complexity and people are the core problems and are reflexively inter-linked. Seeking to manage information securely by personal liability and punishment without clear, simple solutions is unlikely to succeed. New thinking is badly needed.

### **Andrew Hardie – Sharing is dead! Long live sharing! - What can we learn from the post-9/11 US Intelligence Community experience?**

Sometimes, examining problems from the opposite direction helps. In the UK and Europe, Information Governance focuses on data protection to limit sharing. In the US, following 9/11, information sharing in the US Intelligence Community is being revolutionized, emphasising the "responsibility to provide", but securely. Although arising from very different environments and needs, their work may be valuable in the European context as the same security principles can both meet data protection concerns and ensure systems integrity. Tightly controlled sharing is the counterpart to tightly controlled access. This summary of recent reports hopes to inform the current UK Information Governance debate.

### **IAAC IdA recommendations**

IAAC's report strongly recommends that the UK Government develops an Identity Governance Action Plan and, within that, should work swiftly to develop, agree and deploy an Identity Governance Framework for the UK.

The report also recommends that the UK Government should ensure that proposed governance arrangements are widely debated and agreed; the UK should move quickly to put the governance arrangements in place as soon as possible, not just "in due course" as was indicated in "Transformational Government".

### **Kalypton – Briefing Note: Effective supervision before more regulation; Briefing Note: Record retention and information governance**

The current banking crisis has inevitably led to calls for more regulation to improve the internal and external supervision of the industry, yet the current legal and regulatory regimes already provide for the very supervision that is being called for. Not only do they provide senior management with the guidance necessary to carry out their supervisory obligations, they also provide the tools necessary to enable regulators to enforce those obligations and to perform their oversight duties. There is no need for additional legislation or regulation. What is needed is the political will and courage to enforce what exists already.

### **Metanoya and Information Assurance**

The document encompasses the following points:

- The key reasons for IA failure.
- The increased need for corporate governance within Information Assurance.
- Why IA responsibility should be in the boardroom and not the IT department.
- The benefits of classifying data at the point of creation.
- How to drive IA up the corporate and government agenda to drive education and positive action.

### [Adrian Norman – Goldfish come round again](#)

Cybernetics shows that successful regulation of a single national identity system is impossible. Thirty years ago, when the author described the concept of a Global Data File in an Information Systems Haven, GOLDFISH, as an identity service provider, computers were 30,000 times less powerful and more than 1,000 times rarer.

Knives and fools can quickly tap the increasing power of IT to find weaknesses in ID systems to steal and lose data. If one succeeds, the monopolist loses the trust of its clients and so does the regulator; at present both are government. Government should regulate the market for trusted ID services offered from the UK to the world market.

### [SAS – Information Governance White Paper](#)

To signal that data should be as protected and leveraged as much as people, pounds and property, the Public sector should provide a lead by taking a series of actions including:

- creating a public protection commissioner to champion the cause of information exploitation and sharing;
- setting up a pan government 'Business Intelligence Competency Centre' to proactively support public sector bodies in this area and spread best practice; plus
- widen and standardise information management audits across the public sector and beyond to include information management maturity and strategy assessments.

### [Carlos Solari, Alcatel Lucent – The Will to Regain the Confidence - Trust of Our Customers and Citizens](#)

We don't have much time – we cannot afford to wait a few years to begin embedding security in the systems of convergence technologies and Web 2.0. We don't need more bureaucratic policy overhead, but we do need models that allow us to measure security – in the design stage, in deployment and in the operational stages that can transform cyber-security from art to the science of metrics, baselines, and business-rational based remediation. The X.805 standard is proposed to serve as the model available in the present time to help us make this transformation. Information communications technology is in everything including the national infrastructures as we automate to improve operational efficiency and compete in the global markets. Loiter too long and it will be too late, the systems will be deployed and operational making it too expensive to redesign these systems.

### [Paul Wilson, De La Rue – The Information Agenda](#)

- Corporate Information Governance policies are complicated by the retention and disclosure policies of foreign jurisdictions.
- Increases in information sharing in both the private and public sectors are likely to lead to more data losses and breaches of privacy laws.
- Technology has been, if anything, a negative factor in better information governance to date.
- Standard operating practices in Information Governance for public sector organizations and for private sector contractors to Government are long overdue and where private citizens' data are concerned, must be mandatory.
- A code of best practice in Information Governance for commercial organizations is preferable to further legislation

**Full texts of these papers are available at:**

<http://www.eurim.org.uk/activities/ig/drt081124.php#papersreceived>

## PARTICIPANTS

**Dr Louise Bennett** is Chairman of the British Computer Society Security Forum Specialist Panel and leads their "Building Trust in e-government" initiative. She has worked at Board level as a Director in both the public and private sectors for the last twenty years and specialises in building resilient organisations through sound corporate governance and risk management.

**Jeremy Boss** is the Chief Information Officer for the Audit Commission and has a background in information risk management and information systems management. In addition, Jeremy is the Senior Information Risk Owner responsible for information governance within the Commission, has a professional leadership role for information and IT auditors and inspectors and is a member of the Cabinet Office led CIO and Knowledge Councils.

**Nick Coleman** is a leading authority on business and technology. He was commissioned in 2006 as the Independent Reviewer of Government Information Security and he authored the 'The Coleman Report' published by the Cabinet Office in June 2008. He is a Board member and founding Chief Executive of the Institute of Information Security Professionals. He was formerly Head of Security Services at IBM across Europe, Middle East and Africa. He serves on the IT Sector Panel of the Institute of Engineering and Technology and on the Security Strategic Panel at the British Computer Society as well as the European Network and Information Security Agency (ENISA) Permanent Stakeholders Group.

**Andrew Cooke** joined Atkins in 2002 and is the Director with responsibility for the Security Sector. He has recently completed a long-term engagement with one of our confidential clients in this sector and retains the role of Senior Responsible Industry Executive for this and Atkins other major assignments in the sector.

**Sir James Crosby.** Running until 2006, his Executive career consisted of 25 years in fund management, insurance and banking. He is now a non-executive director at the FSA, Compass Group plc and ITV plc, a trustee of Cancer Research UK, and an advisor to Bridgepoint Capital and Oxford University Press. In March, HMT published his report on identity management and this autumn published his report on mortgage finance.

**Bob Darby** is Director of Information Services of Barnardo's, the largest UK Children's Charity delivering a range of services to over 110,000 children and their families across the four nations of the UK. Bob has specific interest in the governance and leadership of IT within the third sector and the opportunities and challenges presented through organisational and technological transformation.

**Stephen Darvill** has worked since 1969 in the ICT services industry supporting both private and public sector customers in UK and overseas. He is Government Relations Director for Logica UK, Chair of Intellect's Professionalism Workstream, Industry Chair of the EURIM Information Governance Group, Council member of PITCOM and a member of the BCS External Relations Board, the BCS Professionalism Board and the IET IT Sector Panel.

**Philip Dunne MP** is Parliamentary Chair of EURIM's Information Governance Group, MP for Ludlow since 2005. Chair of All-Party Parliamentary Group on Corporate Governance, member of Treasury Select Committee and Public Accounts Committee. Before entering Parliament he had a 20 year career in banking and co-founder of quoted book retailer.

**Louise Fluker** is General Counsel and Company Secretary, De La Rue plc 1999-present; chairman of De La Rue's Risk Committee and Health & Safety Steering Group; Trustee of Farnham Castle; former chairman of the Employed Barristers' Committee of the Bar Council and former vice chairman of the Education and Training Committee of the Bar Council. She was educated at Cambridge University and Gray's Inn.

**David Griffiths**, Partner at Clifford Chance, is head of the Communications, Media and Technology group in London and also leads Clifford Chance's global outsourcing team. He has over 25 years experience in negotiating contracts and advising on regulatory issues for the IT industry and its customers. He specialises in helping clients with complex, cross border and strategic outsourcing projects for IT and other business processes.

**Dr Gordon Head** is an Executive within the National Security Group in HP. He is currently in the early stages of a post-doctoral thesis in radicalisation and its effectiveness in counter terrorism at the Karolinska Institute in Stockholm. Gordon has a deep understanding of the use and adoption of technology in areas of counter terrorism and radicalisation.

**John Higgins** is Director General of Intellect, the trade association for the high tech industry in the UK. John is also Vice Chair of RISC - an alliance of trade associations and think tanks working in the area of homeland security and resilience; Chair of the Audit Committee at the University of Warwick and Chair of the CBI's trade association council from January 2009.

**Anne Joseph** is Director of EU Governmental Affairs at Reed Elsevier, a leading provider of professional information and workflow solutions to the Science, Medical, Legal, Risk Management and Business sectors. In this role, Anne's field of interest includes Intellectual Property, Privacy and Public Sector Information policy.

**Michael Keegan** is Business Unit Director, National Identity Scheme, at Fujitsu Services. He is a member of the Strategic Supplier Group of the Identity and Passport Service. Prior to joining Fujitsu, Michael served in a variety of Executive Management roles across the financial services, IT and private equity sectors.

**Jill Kirby** is Director of the Centre for Policy Studies. A writer and policy analyst, her 2008 CPS report *Who do they think we are?* reviews the impact of government data-sharing on privacy, personal identity and the balance of the relationship between the individual and the state.

**Mike Maddison** leads the UK Security & Privacy practice for Deloitte. He has over 20 years experience in the field of technology risk, audit, information and physical security. Prior to joining Deloitte he held a number of senior user security management roles and most recently was Director of IS Security & Business Continuity for a FTSE top 20 company.

**Ian Manocha** is Managing Director of SAS UK. SAS is the global leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Ian is a trusted advisor to senior executives across a broad spectrum of industries, and is respected for his work on the concept of 'Enterprise Intelligence' to drive innovation and performance.

**Jeremy Monroe** has been involved in large IT and transformational projects for over 20 years, originally starting as a consultant, now in delivery. Once a partner in Coopers and Lybrand, he now works in IBM, magically without ever changing his job.

**Peter Montagnon** is Director of Investment Affairs at ABI. He has been appointed by the European Commission to serve on the new European Corporate Governance Forum and is Chairman of the Board of the International Corporate Governance Network.

**Professor Jim Norton** is an independent director and policy adviser. On a part-time basis, Jim is the Senior Policy Advisor - e-Business and e-Government, for the UK Institute of Directors (IoD). He is also an external member of the Board of the UK Parliament's Office of Science & Technology (POST) and a council member of the UK Parliamentary IT Committee (PITCOM).

**Richard Reeves** is Director of Demos. He is a former Director of Futures at The Work Foundation, Society Editor of *The Observer*, principle policy adviser to the Minister for Welfare Reform, Economics Correspondent and Washington Correspondent of *The Guardian* and research fellow at the Institute for Public Policy Research.

**Carlos Solari** is VP for Security Strategy and Solutions, Alcatel-Lucent. His background is a mix of industry and senior US government roles with the Army, FBI, and CIO for the White House.

**Malcolm Stirling** is a Director with CSC specialising in Public Sector services. In 1983 Malcolm joined AGB Impact to become Technical Director for application management services and in 1985 was appointed Managing Director. In 1987 Malcolm joined KPMG and later became a partner in the consulting practice. In 2002 KPMG Consulting was transferred to Atos Origin where Malcolm was a managing director.

**John Suffolk** was appointed Her Majesty's Government Chief Information Office in June 2006. He has a background of over 25 years' experience in IT and major transformation programmes. John will lead the work of the CIO Council in delivering the Government's strategy for the transformation of public services enabled by technology and provide leadership to the IT profession across the wider public sector and enable public service transformation through the strategic deployment of technology which includes driving the use of shared services.

**Clare Wardle's** experiences at Royal Mail Group have included speaking to OECD on encryption and digital signatures, acting as a non-executive director for a subsidiary, attending G8 in Japan to discuss e-crime, and £1bn+ outsourcing and PFI projects. Clare currently co-ordinates a broad portfolio of legal work including telecoms, financial services and retail, competition and compliance, litigation, employment and pensions, managing internal and external teams and budgets.

**Attendance will also include over 80 observers from Parliament, Government, Industry and the Third Sector**

**The event will be followed by a reception co-hosted by The Conservative Technology Forum and Labour E-Futures**

**We are grateful to our sponsors for their generous support.**

Event Sponsors:



Alcatel-Lucent



DeLaRue



Supporters:

