

# The Importance of Standards

## EURIM Directors' Forum on Information Governance

### Summary

- 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 safe-guard sensitive information and educate data-handlers is standards-based.
- As poor organisational 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.

### Background

Information - we are told - is an asset. More recently, however, it would seem to be a toxic liability.

In Summer 2008, a plethora of Government-sponsored reports emerged, each covering differing aspects of what might be termed the 'information governance debate' but with broadly-aligned findings and recommendations. Typically, to cite the Thomas-Walport *Data Sharing Review*, there were calls for a "significant improvement in the personal and organizational culture of those who collect, manage and share personal data".

It is clear that organisations from all sectors are increasingly unsure of their ability to maintain and transfer data securely and lawfully, especially when so much of this activity may be entrusted to sub-contractors. Not wishing to impede business efficiency and unaware of the legal framework, the default setting seems to one of continued poor (or non-existent) processes and a misplaced trust in not being the next name to be shamed!

### A 'lighter-touch regulation'

It has long been recognised that formal standards are a robust means of codifying agreed good practice. Specifically, in this arena, standards development dates back to 1988 when the British Standards Institution, in its capacity as the UK's national standards body, was asked by the Department of Trade & Industry to co-ordinate a multi-stakeholder approach to publishing a common information security framework.

The value of standards as a form of 'lighter-touch regulation' is precisely in that consultative, consensus-driven and vendor-neutral approach. The work begun 20 years ago became a British Standard in 1995, and its significance was further given recognition as an international (ISO/IEC) Code of Practice five years later. The accompanying specification - ISO/IEC 27001 - has proven to be hugely successful in helping organisations implement their own information security management systems. Certifications worldwide currently stand at around 5,000 with such diverse bodies as the United Nations, China's Shenzhen Stock Exchange and lottery operator Camelot all benefitting from such independent audits of compliance. In an era of unprecedented service outsourcing and off-shoring, when organisations want reassurance that those with whom they do business operate to a common minimum security standard, ISO/IEC 27001 - with its risk-management approach - is the accepted 'lingua-franca'.

As importantly, according to the BERR PriceWaterhouse 2008 Information Security Breaches Survey, the globalisation of the standard is "helping raise awareness" at home with the number of UK companies having implemented the 27000 series up 60% compared to 2006.

## **Improving the 'organisational culture'**

In common with Thomas-Walport, the Cabinet Office's study of *Data Handling Procedures in Government* recognised that a "culture that properly values, protects and uses data" needed to be one of the central tenets of its own information assurance strategy. This included mandatory risk awareness e-training for all staff with access to personal data, and even extended to encouraging the roll-out of professional (externally-accredited) qualifications in information management.

Here again, existing standards-based solutions are already available that support this multi-tiered requirement. BSI operates an education programme that covers every aspect of 'information governance' (including information security, data protection and Freedom of Information) and is piloting the use of e-learning. Courses cater for all needs - from 'awareness' to 'implementation' - and include full ISEB (Information Systems Examining Board) qualifications.

Training is designed to help attendees understand and implement effective management systems, outlining the implications of third-party auditing (where appropriate) and possible penalties for non-compliance.

## **Beyond 'security'**

As indicated above, the concept of 'information governance' extends beyond the definition traditionally associated with information security. Consequently, as has been well-documented, responsibility for information governance needs to sit with an organisation's entire senior management team so that the IT director can largely concentrate on protecting data assets from *external* threats via maintenance of robust system security. In short, good information governance should be as weighty a board agenda item as sound corporate governance.

Similarly, standards have been developed in the fields of Business Continuity Management and Risk Management. Taken together with Information Security and the upcoming standard in Data Protection, these prove to be a powerful portfolio of solutions from which to build an organisational Information Governance strategy.

## **Adapting to new challenges**

Standards evolve to meet the changing requirements of industry, government and society largely because the consultative means by which they are produced ensures their development keeps pace with the very challenges affecting their relevance. Business needs to feel confident its management processes are up-to-date and relies increasingly upon standards makers to set the 'continuous improvement' agenda.

That said, information and communication technology (ICT) moves so fast that this traditionally wide-reaching process is not always appropriate. Instead, what may sometimes be required is a 'fast-track' route to guidance.

To address this, BSI can tailor standards solutions to better meet the needs of stakeholders. By limiting consultation, a document can be published in as little as 6 months, but because its development is managed by BSI throughout, the finished specification retains credibility in the market. BSI is especially skilled at framing policy requirements in a way that encourages compliance, and is grounded in pragmatism and ease-of-adoption. Increasingly, government and industry are seeing the benefits from coming together as partners under the auspices of BSI's long history of expert and impartial standards development.

Just as with that first DTI-backed Code of Practice for Information Security, standards-making continues to prove it is 'fit-for-purpose' and is needed now more than ever.