Information Management –– Headache or Opportunity?: The Challenges that the Recent Focus on Information Management is Presenting to Senior Leaders in the Public Sector

Natalie Ceeney

Public Policy and Administration 2009 24: 339
DOI: 10.1177/0952076709103815

0952-0767
200907 24(3) 339–347

Information Management – Headache or Opportunity?

The Challenges that the Recent Focus on Information Management is Presenting to Senior Leaders in the Public Sector

Natalie Ceeney

Chief Executive, The National Archives, and Government Head of Profession for Knowledge & Information Management, UK

Abstract There has been significant recent focus on information and data handling in the public sector prompted, in part, by the loss of two discs from HMRC in late 2007 containing the details of 25 million citizens. This article explores the issues behind this new focus, and examines how many of the underlying issues are either new, or really different from the issues that Boards explore every day in relation to other business challenges. Drawing on recent publications as well as from the author's experience as Government Head of Profession in this arena, this article argues that information assets are as much opportunities as risks, and that the opportunities are still poorly understood, and information assets underexploited. It also proposes that Boards need to treat information management as a core business challenge, and use existing techniques, particularly that of risk management and cultural change, to ensure that they address the critical challenges that digital information presents.

Keywords data handling, governance, information management, leadership, risk management

Introduction

It seems we cannot read a newspaper today without reading about a data breach, concerns about how our information is used, or a scandal as a result of information

DOI: 10.1177/0952076709103815
Natalie Ceeney, The National Archives, Ruskin Avenue Kew, Richmond, Surrey, TW9 4DU, UK.
[email: natalie.ceeney@nationalarchives.gov.uk]

not being shared between key public bodies. There appear to be high levels of public concern about how public services are managing citizens' data, which are damaging the reputations and effectiveness of public institutions. And the level of actual losses of data, in the public as well as private sectors, internationally as well as nationally, are widely recognized to be unacceptably high.[1] As public servants, we have in the last 18 months received the Hannigan review into handling of personal data,[2] the Walport/Thomas review into data sharing,[3] and the Poynter review into HMRC's data loss.[4] Large numbers are quoted whenever data breaches are mentioned – whether in terms of the fines imposed on private sector companies who breach basic data management rules,[5] or the number of laptops lost from the Ministry of Defence.[6] And yet Boards and senior leaders across the public sector are struggling to know how to engage with this new, and different issue. Why? And how should they engage? And are we really looking at just a threat or also an opportunity in the advent of digital information?

What *is* clear is that today's digital society is radically different from the world in which most senior leaders grew up. Today's British children spend more time on the Internet than playing with each other or watching TV.[7] HR Departments debate their policies on staff use of Facebook, and how they will deal with people posting derogatory comments about line managers in public. The civil service has announced guidelines to enable civil servants to blog,[8] and the Power of Information review,[9] and subsequent task forces are exploring the ways of reusing government information to create citizen-focused services and transform citizen engagement with government.[10] Mobile phone usage is over 100 per cent per head of population, and the most highly used government website is that of JobCentre Plus, which 78 per cent of its users view weekly.[11] This is not the paper-based society that the current CEOs and Boards of today's public sector institutions were raised in.

And that might explain the way that most public sector bodies have reacted to this new information revolution, and the challenges that it is brought. As Keiran Poynter, the HMRC review lead, and former PWC Chairman, said in July 2008 'I have spent the past few months looking at the issue and talking to leaders from the public and private sectors about data security issues. What has emerged is that there is a decided lack of ownership when it comes to data security . . . [and] there is a widespread perception that information security is an information technology issue and that produces a tendency to focus on security safeguards such as encrypting data on laptops . . . '.[12] But let's challenge this approach. If there was a fraud, where financial data was lost because someone had allowed a bankers draft to be intercepted, would we tackle the financial culture in the organization, and capability of the finance team, or would we focus on the postroom? We understand financial issues, and so know how to respond – and hopefully most Boards would put their focus on the underlying cultural and capability issues, as well as reminding the postroom of the rules. But our understanding of information issues is weaker, and so are our responses. Of course we need to encrypt laptops containing sensi-

tive information, just as we would have needed to stop postrooms sending out bankers' drafts in unprotected post in the example given. But in the information context, we seem scarily content with the technical solution, and risk missing the fundamentals. In both of these cases, we need to tackle the root cause issue, which requires us to understand where our risks lie, and focus on building our capability to manage our assets. This means that Boards need to get engaged in a different way than they are currently doing.

So What Has Changed? Is the World Really that Different?

It's easy to say that 'digital information has changed everything', and in some ways it has. An obvious change is the sheer volume of content. There is far more digital information than ever before – with estimates of growth of volumes at 60 per cent per annum.[13] Individuals send hundreds of emails in a day when 10 years ago they might have generated 10 memos. The Department for Culture, Media and Sport, one of Government's smallest departments, have estimated that 10 years ago, they added a volume of information equivalent to the Complete Works of Shakespeare to their computer systems every day. Five years ago, they were adding the same volume every hour. Now they are doing so every minute, and it is estimated that by 2010, they will be doing so every second.[14]

But digital has also changed how we work. There is no doubt that communication methods are radically different now from 10, or 20 years ago. We can communicate wherever we are, 24/7, using Blackberries and PDAs. Digital information has also enabled unprecedented public access. In the research field, the web has allowed literally tens of millions of people to search for their family history easily, from the comfort of their own homes. This used to be a niche and rather specialist research hobby requiring long visits to archives working through paper records, and some comfort with traditional research methods. Digital has changed the face of customer service delivery, allowing people to renew tax discs online, including the 4494 people who renewed their tax online last Christmas Day. In itself, this has led to huge changes in customer expectations of public service delivery – we expect to interact with public services 24/7, and on our terms, from wherever we are. And, as consumers, we do not assume that this comes with a higher risk profile than it used to.

But there is a lot that has not changed. In the case of Victoria Climbié's death, back in February 2000, Lord Laming's subsequent enquiry found that poor record keeping was a major contributory factor to her death at the hands of family members. Lord Laming's report stated that, 'in Brent, Victoria's case was given no less than 5 "unique" reference numbers. Retrieving files was, I was told, like the National Lottery, with similar odds'. More lightheartedly, government Second World War public communication posters now held in the UK National Archives stress the need to 'keep your secrets safe', one illustrating a business man appearing to leave a key document on a train. We are aware that the risk of similar

incidents recurring has not disappeared – yet these were about the management of paper, not digital, files. Technology has not changed the underlying principles. And, worse, as Keiran Poynter says, 'technological measures risk creating a false sense of security. Most breaches are the result of quite mundane physical factors, and are essentially caused by process failures and/or people simply not knowing what to do. Organizations can have all of the policies and processes they like, but if their culture and values, management systems and scrutiny are not joined up in a clear governance framework, this lack of integration lends itself to data security issues'.[15] Poynter is referring specifically to the risk of data loss, but the same can be said of information management more generally. The issue is not primarily a technology issue. It is a cultural and governance issue. And that is not new.

So What is 'Information Management' and Why are Boards not 'Getting it'?

So what do we mean by 'information'? It is, surprisingly, a question I am asked very frequently. Information is the currency of what we do. It is the data that flows through our customer databases, it is the write up of key meetings and submissions or discussion papers analysing new policies. It is the reference documents we hold, our FOI requests, our internal 'wikis' sharing knowledge, and our key conversations. But it is often wrongly assumed to be synonymous with IT. IT systems are often the conduit for information – but the systems can only manage what is put on them – we do not assume that Finance is the same as IT just because we put financial data on IT systems.

Boards are struggling in part because we have made the issues far too technical and specialist, which professionals all love to do. Today's public sector CEOs did not grow up in a digital world, and we have experts around us; data protection experts, FOI teams, records managers and information architects; who all want to prove their value and make things complicated and specialist. Yet, is this an excuse? Is finance that different? Few non-accountants can claim to completely understand the technical terms of public sector accounting rules, and yet most Boards can understand the principles and manage their money pretty effectively. A major challenge, perhaps the most significant challenge that we have in this field, is convincing Boards that managing information is conceptually no different from managing finance, or HR. And in this lies the key to taking this issue forward; namely putting the information management agenda into standard business language, and applying the same principles as we apply to other areas of our enterprise.

But there are other reasons we are struggling. The change to a digital environment requires new skills. Clerks who managed paper files do not have the same skills as those required to manage customer databases or the sharing of datasets between organizations. The sheer volume of content means that old paradigms cannot work, so new strategic thinking is needed. There is no doubt that many

traditional information management specialists are struggling. But again, this is akin to Finance and HR. It was relatively recently that we all woke up to the fact that we no longer wanted personnel departments processing transactions, but that we wanted HR and OD departments telling us how we could increase employee engagement. We employed new people to do this, with new skills. And in central government at least, it is only within the last three years that we have seen a major influx of qualified accountants professionalizing and commercializing our approach to money. Boards coped with these changes, and can do so for managing their information.

So, is Information Management a Risk or an Opportunity?

The data handling focus has highlighted the negative consequences of managing information badly, and has focused Boards on how to minimize data loss. But there are just as many risks of *not* sharing information, and huge opportunities that we are only starting to understand in terms of exploiting information as an asset.

A recent compelling report that illustrates the potential opportunities of managing information well is the 'information opportunities' analysis published by Cap Gemini in March 2008. This revealed that nearly two-thirds of managers believed poor information management was hurting productivity and that this was currently costing the UK public sector £21bn in lost effectiveness. And it is easy to see how this can be true. Many of our own organizations hold multiple versions of customer data, do not share information between teams, or lose opportunities because information is not shared. Cap Gemini also argued that we need to see information as the next big under-exploited asset after our finances and our people. Again, parallels to functions that Boards understand well.

And the other area of opportunity is that of creating new economic models, and new citizen engagement through using and reusing existing public sector information. The Power of Information review, written by Ed Mayo of the Consumer Council, and by Tom Steinberg of My Society, captured visibly some of these opportunities, which are illustrated through Tom's own private work (see http://www.theyworkforyou.com as an example of how existing data can be used to make the workings of parliament accessible and engaging to all citizens). The power of the web now allows online debate about policy issues, it allows us to harness the views of citizens experiencing services today. It allows interest groups to take the output of government, whether mapping data, school results or house prices and create, very cheaply, services for local users which government could not have foreseen. And other reviews, most notably the OFT review into Commercial Use of Public Information,[16] quantified the potential economic value of allowing wider reuse of our public sector information assets as around £500m to the UK economy.

How Should Public Sector Approach this Issue?

The steps we need to take are actually not that challenging conceptually, and they come down to applying standard, business principles that we apply to Finance and HR to the management of information. The starting point should be risk management. All businesses, in all sectors, need to understand where their business risks are, and failure to exploit assets is a risk, just as breaching data security is. This does require organizations to understand where their information assets are held, just as they need to understand where their money lives, but it provides a sensible structure to do so. Government guidance on this, issued by Sir Gus O'Donnell in March 2008, 'Managing Information Risk' even lays out categories of risks and questions for boards to ask.[17] Kieran Poynter similarly highlights this: 'a failure adequately to manage information security risks is often symptomatic of broader risk issues or a fragmented governance framework'.[18]

In most organizations, this turns the spotlight on a number of gaps in areas that are well understood by organizations: governance and clear accountabilities; cultural issues and staff training; capability of supporting professionals; clarity and appropriateness of processes and procedures and supporting (supporting, not leading) technical infrastructure. The specifics will depend on the specifics of each organization. Customer data-rich organizations will have a particular risk profile that prioritizes action in the area of data security, while policy environments are more likely to focus on harnessing opportunities to share knowledge and exploit the assets they have more effectively. None of this approach, or the issues or solutions are new to Boards, to CEOs and to Audit Committees. Perhaps the biggest challenge that this presents is to the professionals supporting the process, who need to reframe the language in which they present, and expose their approaches to senior business scrutiny, perhaps for the first time.

What is really clear, though, is that Boards have no choice but to embrace this agenda. In the civil service, all Accounting Officers are now explicitly accountable for the management of their information, with full disclosure of breaches required in annual reports, and increased powers for the Information Commissioner as regulator. But it is not just the rules that have tightened. The damage that recent data breaches have caused to trust in government is clear, and there is no excuse for us failing to manage the assets that our customers trust us with. We spend taxpayers' money, and require our customers to give us their data to deliver our services. We have a responsibility to manage that data well, and to use it to deliver better services. And we owe them that we manage our information well so as to manage down the wastage that poor information management generates.

Conclusion

Information management is going to be a major issue on Board agendas for years to come. And it needs to be. We have a responsibility to ensure that customer data is managed effectively, and to manage the information we hold as effectively as we do other assets. If we see information as an asset, we can see huge opportunities in managing it well, in addition to the more obvious risks of managing it poorly. These opportunities are not just financial (although the financials are non-trivial, and particularly within the current economic climate, any opportunities for financial gains have become even more relevant and important); they are also about creating wider citizen engagement and new services beyond traditional public sector boundaries.

But Boards need to change their approach if they are going to do so. They need to move away from the notion that IT will solve their problems. IT neither makes the finances balance, nor the people work harder; it just helps operationalize solutions and make life work more effectively. The real challenge is for Boards to add information management to their agenda, and think of it in the way they think of HR or Finance. The business rules, and tools that are used for these disciplines work on the management of information, and will effectively expose the underlying challenges of capability, processes and culture, which Boards know how to tackle. We need to demystify information management and make it mainstream. And we need to do it now.

Notes

1. 'It is alarming that despite high profile data losses, the threat of enforcement action, a plethora of reports on data handling, and clear ICO guidance, the flow of data breaches and sloppy information handling continues'. (Richard Thomas, the Information Commissioner's speech to the RSA Conference Europe on data breaches, 29 October 2008, http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf). In October 2008, the Information Commissioner's Office (ICO) revealed there were 176 data breaches in the public sector in the last year, twice as many data losses than the private sector, which clocked up just 80 reported cases. A breakdown of the public sector cases revealed that 75 were in the health sector, 28 by central government and 26 by local authorities (http://www.ico.gov.uk/upload/documents/pressreleases/2008/data_breaches_29_october_2008.pdf)
2. *Data Handling Procedures in Government: Final Report*, June 2008, http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf
3. *Data Sharing Review*, Richard Thomas and Mark Walport, July 2008, http://www.justice.gov.uk/docs/data-sharing-review-report.pdf
4. *Review of Information Security at HM Revenue and Customs*, Kieran Poynter, June 2008, http://www.hm-treasury.gov.uk/d/poynter_review250608.pdf
5. Fines imposed on companies for data management breaches include: (i) In December 2007, The Financial Services Authority (FSA) fined Norwich Union £1.26m for failing to have adequate checks and systems in place to prevent a £3.3m

fraud that took place in its life assurance division in 2005. The fraudsters managed to successfully cash in the life policies of 74 customers worth a total of £3.3m simply by using a selection of publicly available information, such as their dates of birth, names and addresses. In some cases, they also managed to get the call centre operative to change personal information, such as bank account details, on their systems. The FSA said that it believed Norwich Union had failed to adequately assess the risks posed to its business by financial crime, claiming it had left its customers at greater risk of falling victim to identity theft and other financial fraud (http://www.norwichunion.com/media-centre/story/3763/statement-from-norwich-union-life-fsa-fine/); (ii) The United States Sarbanes-Oxley Act (SOX) of 2002 requires directors of publicly traded companies to provide internal control and governance mechanisms. SOX also empowers the US Securities and Exchange Commission with wide-sweeping mandates to ensure that SOX is adhered-to. In 2006, The Securities and Exchange Commission (SEC) fined Morgan Stanley $15m for failing to retain emails. The fine is the largest SEC has imposed on a company for failing to preserve electronic records.

6. Number of laptops lost/stolen from MoD: In a written parliamentary answer dated 17 July 2008, Defence Secretary Des Browne said 747 laptops had been stolen or lost from the MoD in the last 4 years, 400 more than originally reported (http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080717/text/80717w0034.htm).
7. Amount of time children spend using the Internet versus watching TV: A survey by Google's DoubleClick Performics looking at the behaviour of 10–14 year olds revealed 83 per cent spend at least an hour per day online, 68 per cent spend at least an hour per day watching TV. Radio, magazines and newspapers came in much lower with 29 per cent, 10 per cent and 5 per cent respectively. Nearly half of respondents go online many times per day (more than three), and 87 per cent usually spend at least a half hour each time (http://chiefmarketer.com/Channels/online/tween_shopping_habits_0729/index.html).
8. Guidance on Civil Service Blogging, http://www.civilservice.gov.uk/iam/codes/cscode/index.asp
9. Power of Information Review (POI) 2007, http://www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/power_information.pdf
10. Power of Information Task Force, http://powerofinformation.wordpress.com/
11. http://www.alexa.com/site/ds/top_sites?cc=GB&ts_mode=country&lang=none
12. Kieran Poynter, *Financial Times*, 16 July 2008 (http://www.ft.com/cms/s/0/525bc6ec-526d-11dd-9ba7-000077b07658.html?nclick_check=1).
13. Increase in volume of digital information: *The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011,* published by IDC (Interactive Data Corporation) in March 2008 (http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf) reveals a number of key findings, namely:
    - At 281billion gigabytes (281 exabytes), the digital universe in 2007 was 10 per cent bigger than originally estimated.
    - With a compound annual growth rate of almost 60%, the digital universe is growing faster and is projected to be nearly 1.8 zettabytes (1800 exabytes) in 2011, a 10-fold increase over the next 5 years.

- Your 'Digital Shadow' – that is, all the digital information generated about the average person on a daily basis – now surpasses the amount of digital information individuals actively create themselves.

14. Source: Mark O'Neil, Chief Information Officer (CIO), Department of Culture, Media & Sport (DCMS).
15. Kieran Poynter, *Financial Times*, 16 July 2008 (http://www.ft.com/cms/s/0/525bc6ec-526d-11dd-9ba7-000077b07658.html?nclick_check=1).
16. Commercial Use of Public Information 2006 (CUPI), http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft861.pdf
17. 'Managing Information Risk: A Guide for Accounting Officers, Board members and Senior Information Risk Owners', March 2008 (http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf).
18. Kieran Poynter, *Financial Times*, 16 July 2008.

Natalie Ceeney has been Chief Executive of The National Archives since October 2005, where she is responsible for leading the organization across all of its activities, from its increasingly proactive information management role across government through to the delivery of world-class customer services. Her previous career spans the public and private sector, including roles at McKinsey & Company, the NHS and The British Library. She is also Government's Head of Profession in Information & Knowledge Management, a visiting professor at the school of Library and Archive Science at UCL and sits on the Government's Power of Information Task Force.