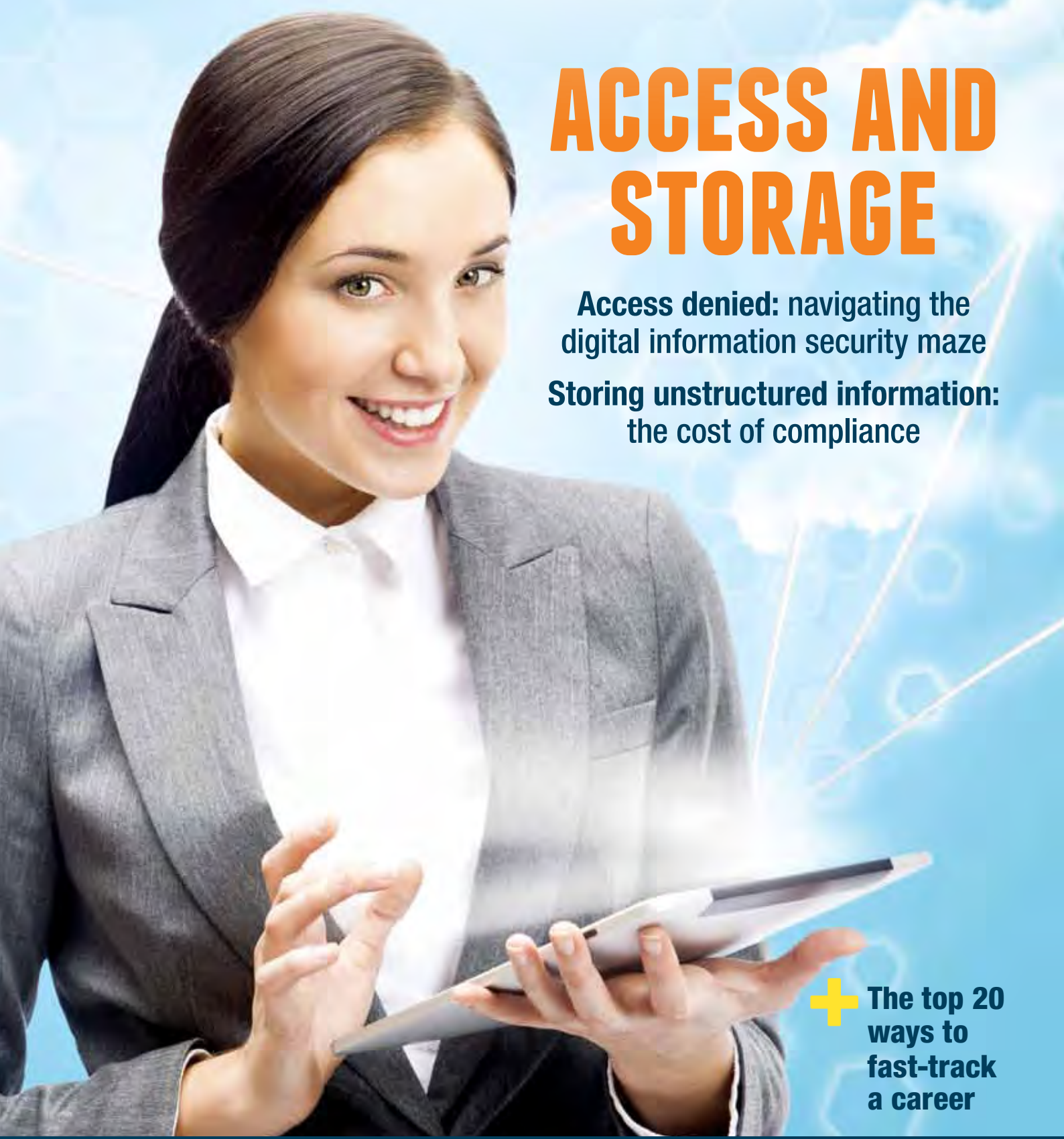
Vol 29 / Issue 1 / February 2013 / issn 0816-200x
AU $90.00 incl GST ($81.82 + GST) for four issues

iQ

THE R·I·M QUARTERLY

Professionals Australasia



ACCESS AND STORAGE

Access denied: navigating the digital information security maze

Storing unstructured information: the cost of compliance

+ The top 20 ways to fast-track a career

See more at www.rimpa.com.au

iQ THE R·I·M QUARTERLY
Professionals Australasia

VOLUME 29 / ISSUE 1 / FEBRUARY 2013

Official Journal of Records And Information Management Professionals Australasia

EDITOR: Heather Millar
Zest Communications
Professional writing and editing services
Web: www.zestcommunications.com.au
Email: editor.iq@rimpa.com.au
Post: Editor, *iQ* Magazine
PO Box 779, McLaren Vale SA 5171

ART DIRECTOR: Kerrie King
Kerrie King Design
Magazine and corporate design services
Email: king.design@iinet.net.au
Stock images: Shutterstock

EDITORIAL COMMITTEE
Kristen Keley (SA)
Michael Steemson (NZ)
Philip Taylor (QLD)

CONTRIBUTIONS & EDITORIAL ENQUIRIES
Articles, reports, reviews, news releases, Letters to the Editor, and content suggestions are welcomed by the Editor, whose contact details are above.

ADVERTISING
Wendy Morris
advertising@rimpa.com.au

ANNUAL SUBSCRIPTIONS
AU $90.00 incl GST ($81.82 + GST) per annum for 4 issues (including postage), from:
Subscriptions, Membership & Financial Services
RIM Professionals Australasia
PO Box 276, St Helens TAS 7216
P: 1800 242 611 F: 1800 333 802

***iQ* ONLINE ARCHIVE**
Copies of articles published in *iQ* since 1984 are available at the Members Only section of the RIM Professionals Australasia website, in the *iQ* Article Archive. Complete back issues from February 2005 are available electronically at the Members Only section of the RIM Professionals Australasia website.

The Members Only section of the website can be accessed with RIM Professionals Australasia membership, or, outside Australia and New Zealand, with the purchase of an *iQ* annual subscription.

RIM PROFESSIONALS AUSTRALASIA WEBSITE
http://www.rimpa.com.au

CONTENTS

David Pryde, Chairman of the Board, RIM Professionals Australasia

Looking forward to balance and adventure in 2013

I sincerely hope that you and your families celebrated a very Merry Christmas and a Happy New Year, by devoting your energy to 'quality family time'. During the year we can become so focused at doing our jobs well, 'fighting the hard fight', that we lose sight of the very people that are our main inspiration for working.

They love us and support us, pick us up when we are 'down' and celebrate our victories (with pride) in us. I am not trying to be an analyst or a counsellor in this column, but at this time of year when you are making resolutions and planning for the year ahead, include some strategies that give the family more time with you.

I have always been an advocate that we must give appropriate time and resources to the three biggest influences on our life: Our Employer, Our Family and Our God. You can add other influences like professional association, volunteer and charity work, sports and academic success – but these are not like the first three mentioned.

Get these out of kilter and the impact can only be distressing – *the true professional finds balance in planning to provide each with the correct amount of attention*.

Wherever you are on your RIM adventure I wish you every success along the way

Nothing revitalises or replenishes our flagging energy stocks faster than relaxing time with family and loved ones! Add sun, surf, a selection of delicious treats and a splash of our favourite beverage for the perfect mixture.

A WATERSHED YEAR FOR RIM

After years of being told to adapt and to be more innovative at conventions and forums across the planet, the RIM community responded in 2012 by reaching for the cloud!

To meet the growing needs of records and information managers, in solving the problems of managing social media, the security of data from mobile devices, the excessive costs of increasing storage, finding cheaper alternatives to legacy scanning projects, all eyes are keenly focused on MS SharePoint (SP) and other content management platforms.

While SP has been around since 2001, it has only gained a following over the last few years as its functionality and additional 'third party plug-in' solutions have gained credible successes.

I am not advocating one product over another, as all solutions must be unique to each organisation.

I am pleased that the technology is stimulating debate and discussion, that our 'white-knuckled' grip on long held virtuous recordkeeping principles is being challenged for the good of the profession. However, any innovative solution must still guarantee the authenticity, the accessibility, the irretrievability and the authority of the original record whatever the media, for the life of the record.

Enterprise Content Management solutions are not 'white knights' or 'silver bullet' solutions that are going to instantly solve all your problems and provide a myriad of new benefits. They require a deep understanding of your organisation, demand a great deal of time and effort in building the foundations correctly – and are more easily built if you have a good idea what you want them to do.

This year is going to be a 'watershed' as a number of large ECM projects are implemented and completed. 2013 will determine whether all the writing and talking in 2012 was worth the effort.

Wherever you are on your RIM adventure I wish you every success along the way knowing that RIM Professionals Australasia is there to support you along the way.

Let me take this opportunity to wish you and your families a happy 2013! Let it be full of peace, joy, good health and prosperity for all.

David Pryde
MRIM

Kate Walker, Chief Executive Officer, RIM Professionals Australasia

Access and storage options for better RIM

Access and storage is the theme for this edition of *iQ*… and what a can of worms those two little words create. A simple fact we all know – but one worth reinforcing – is that records and information management shouldn't just be a priority, it must be *mandatory*. Records and information management is the building block that connects business departments together. Businesses rely on technology and systems to run their business, yet most businesses are not organised around records and information. The result… information islands, an inability to manage information consistently, leading to duplication, inefficiency and the inability to use information for efficiency and competitive advantage.

The sheer volume of information and its continued growth is one of the main causes of these islands. So what are some of the 'options'?

Server virtualisation – this just makes the problem worse. All this does is result in an increased storage spending.

Cheaper storage – again, not the answer.

ASKING THE RIGHT QUESTIONS

Just as an aside, cloud conversations are rife today; from the boardroom to IT departments, the debate about moving some of your business process to the cloud is raging. Whilst moving to the cloud can offer many advantages, it also raises many questions including issues such as data sovereignty, security and risk management. There is also one big concern that most IT departments are familiar with in any type of selective sourcing arrangement, which is the dreaded lock-in situation.

Selecting a cloud platform that is built on proprietary formats means that businesses can face a lock-in situation which will make it much more difficult for them if they change service provider at some point in the future; either because they want to bring the processes back into their premises or they want to select another service provider.

We have seen a lot of news and solid adoption from the public, from providers as well as local players, and many of the stories surrounding cloud computing have not necessarily been focused on the security of a cloud, rather the availability of it – whether that be short-term due to network or system outages, or long-term viability due to a provider going out of business or substantially changing its terms of service.

Whether your cloud provider changes their terms of service or has interruptions to service that cause you to search for alternatives, many customers are asking themselves some important questions:

- Will my cloud provider change its terms of service, and what can I do about it?
- If I don't have control over cloud costs, does this diminish its value?
- How easily can I move my data to a different provider?
- How do I know which country the data is stored in and who has access to it?
- What do I do if the only copy of my data is in the cloud; how do I download it all and start all over with a new provider?
- If my cloud provider changes to a limited data service, how do I select which data remains protected and which data may be purged due to the size limit?

Better records and information management is the answer. Without it, storage costs will spiral, information becomes harder to find, risks of legal action and privacy breaches escalate and the ROI of storage is diminished.

So, what are some actions every business should take?

- Protect by backing up
- Deduplicate
- Delete confidently
- Discover efficiently

I've spoken on information governance previously, but it is a policy-based management of information designed to lower costs, reduce risk and ensure compliance with legal, regulatory standards and/or corporate governance. It includes policies and technologies to understand what information is at what point in its cycle and to apply appropriate policies (including retention and disposition).

Your organisation needs to know:

- *What* information is stored
- *Where* information is stored
- *Who* has access
- *How* long the information is retained and preserved

With sensitive information being the biggest 'concern' to sell a records and information management program, you need to focus on two factors:

- Guarding the locations where the information is stored and managed
- Guarding the perimeters across which information may be distributed

As a professional, you need to sell the value of records and information management and ensure that you are involved in the full picture, which includes access and storage.

Kate Walker
FRIM MAICD AMIM, MBA, BSC (BAdm), AdvDipBus (Rkg), DipBus (Adm)

WORLDWIDE NEWS

Social media in Australian Government survey

A survey of social media use by Australian government agencies has revealed a strong but wary interest in the new functionality.

Victoria University of Wellington School of Information Management masters degree scholar, Rebecca Stoks, fielded returns from 63 agencies from her on-line survey seeking news of how government agencies in Australia are capturing records created on social media websites.

She launched the survey with the revelation that "over 470 Twitter accounts have been created by government departments across Australia.[1]

Two-thirds of the responding agencies acknowledged they had been using media for a year or more, and almost five out of six had social media policy in place or were developing one.

Rebecca Stoks reported: "When it came to deciding what to capture, respondents were divided, with some capturing everything and others capturing selected records."

On the downside, most of the agencies using the medium doubted they were meeting legal obligations to keep the records and only half of these thought their methods were sustainable.

Ms Stoks said: "Most respondents had consulted their local public records offices on social media recordkeeping and found their advice useful. However, when asked what gaps existed in the current guidance on social media records, several respondents expressed a desire for practical and sustainable solutions for what to capture and how to capture."

1 See http://egovau.blogspot.co.nz/p/australian-government-twitter-accounts.html

Vale Marian Hoy


Marian Hoy

RIM Professionals Australasia would like to recognise the passing of Marian Hoy, who was a tireless volunteer for the association for many years as well as working for the association as our education and professional development officer for the past 3 ½ years. As many of you will know, Marian was battling cancer. She suffered a pulmonary embolism on 23 October 2012 and went downhill rapidly from then, passing away on 28 October 2012. RIM Professionals Australasia extends its heartfelt condolences to her family.


Heather Millar and Adam Rickard

Congratulations

Congratulations to *iQ* editor Heather Millar, who was married in McLaren Vale, South Australia in December 2012. Heather and husband Adam Rickard then honeymooned in North Queensland. We wish them well in their married life together.

NSW State Records launches new OpenGov website

State Records has just launched a new website dedicated to making NSW government information more accessible. OpenGov NSW (www.opengov.nsw.gov.au) is a searchable online repository for information published by NSW Government agencies, including annual reports and open access information released under the *Government Information (Public Access) Act* 2009.

OpenGov will provide a simple and easily accessible path for the public seeking information on government services, commitments and programs, both contemporary and historical. By uploading annual reports, other publications, and 'GIPA' open access documents to OpenGov, public offices will have less content on their own websites to worry about over time. All content in the OpenGov site will be preserved permanently by State Records' digital archives team, using state of the art digital preservation technologies.

OpenGov is available for any NSW public sector organisation to post their published information to, including universities, local government and state-owned corporations. Government agencies can publish their annual reports solely at OpenGov and link to these from their own website, as permitted under the *Annual Reports (Departments) Regulation 2010*, Clause 13. A downloadable widget is available in OpenGov that provides a link from an agency's website to its content on OpenGov NSW.

➲ For more information, email opengov@records.nsw.gov.au

Little NZ Crown agency shows way to The Cloud

A new, small NZ Crown Agency, the precisely-named Walking Access Commission, has made its mark as the first government entity adopting a locally-hosted cloud solution to support compliance with the Public Records Act, the legislation at the heart of Kiwi public sector recordkeeping.

With seven Wellington-based staff and eight advisors located around the country, the organisation needed an IT solution that would allow better collaboration between team members, improved security and a more organised information management system compliant with the Public Records Act (PRA).

Using iWorkPlace, a Microsoft SharePoint application developed by Christchurch knowledge management consultancy, Information Leadership, the Walking Access Commission (NZWAC) added key functionality ... and cloud storage.

Commission Corporate Services Manager, Helen Barker, told *iQ*: "Information Leadership put a whole lot of things together to make life easier in-house and for our regional advisors. We had SharePoint, but we didn't have all of the smart features that they applied to it."

"We needed better information management for public enquiries. We now have automated recording of our enquiries and the ability to sort and display them, which has made our management much easier and saved us a lot of time – it's a great feature."

The commission was set up in 2008 to enhance access to New Zealand's many beautiful public walkways, beaches,

mountains, rivers and lakes. It outsourced IT requirements and took on Microsoft SharePoint for managing data from regional advisors. As the organisation developed, so did its need for more specialised tools and customisation, particularly for managing public enquiries.

Information Leadership was engaged to apply solutions supporting PRA compliance and catering to the commission's unique set of requirements.

Working in tandem with Auckland-based IT infrastructure company Appserv that supplied the infrastructure and hosting capabilities, Information Leadership provided recordkeeping and productivity enhancements on a SharePoint base.

Information Leadership Director Sarah Heal reported: "We're excited by this development because it shows that Government agencies can operate in the cloud and still meet public records requirements.

"A key focus of ours is to take a pragmatic approach to individual clients' needs. In this case, we took SharePoint and used our proven extension products to provide a strong fit." Sarah Heal added: "This solution shows how small organisations can meet high risk or compliance needs quickly and cost-effectively, without having to invest in the purchase, design and maintenance of complex IT systems."

Some of the features improving the commission's day-to-day information processing include the Colligo email product, simplifying email filing and search, display enhancement and better information navigation.

Collaboration among commission's team members was another challenge. Previously, regional advisors could not access files and resources held in the Wellington office requiring some files saved in two places. By applying user profile access levels to data, Information Leadership facilitated access to relevant corporate information.

NZWAC Corporate Services Manager, Helen Barker agrees: "We're very happy with the result because it ticks a lot of boxes for us. We now have a smarter system that meets our IT needs."


Sarah Heal

'Cool' NZ Web harvest of 150m URLs

New Zealand is this month carrying out its third NZ domain Web Harvest to "take a snapshot of New Zealand as it exists on the web and recognise the Internet's importance in all areas of its society and culture".


Mark Crookston

NZ National Library's Alexander Turnbull collection Digital Collection Strategy Leader, Mark Crookston, announced: "We estimate we will capture approximately 150 million URLs, resulting in 12-15 terabytes of uncompressed data. That's quite a lot of cool stuff."

The harvest will run from around February 4 to 22. Previous New Zealand web harvests were held in October 2008 (105 million URLs and four terabytes of uncompressed data) and in April 2010 (130 million URLs of roughly eight terabytes).

Mark Crookston told *iQ*: "The technical parameters of the harvest are the same as for the successful 2010 harvest. These were developed after consultation with the public and Internet stakeholder groups. We will attempt to acquire:

- websites with the .nz country code;
- websites in .com, .net and .org domains that can be programmatically determined to be physically hosted in New Zealand; and
- selected websites based overseas that are covered by the provisions of the National Library of New Zealand Act (2003)."

The harvest is required by the National Library of New Zealand Act and the Minister's National Library Requirement (Electronic Documents) Notice 2006. The Library has commissioned the Internet Archive, an American-based not-for-profit organisation, to do the work. ❖

➲ More information: http://natlib.govt.nz/publishers-and-authors/web-harvesting/2013-nz-web-harvest

CONTACT US ✉ If you have any news stories for *iQ*, please contact editor.iq@rimpa.com.au

New Australian standards – management systems for records

In June 2012 Standards Australia published *AS/NZ ISO 30300 Information and documentation – Management systems for recordkeeping – Fundamentals and vocabulary,* and *AS/NZ ISO 30301 Information and documentation – Management systems for recordkeeping – Requirements*. Apart from minor changes to some terms, these standards are a direct adoption of the International Standards ISO 30300 and ISO 30301. So what does this mean for Australia? **Judith Ellis** responds.

It means we have the first of a series of standards that organisations of any size or type can use to design and implement a management system for recordkeeping (MSR). An MSR is a 'management system to direct and control an organization with regard to recordkeeping'. (AS/NZ ISO 30300, 3.4.2)

All organisations have a management system of some sort, that is, a framework of policies and procedures and associated resources to achieve the objectives of the organisation. The management system comprises a set of interacting elements such as the governing policies and objectives, definition of organisational structures, roles and responsibilities, organisational plans, and operational processes. The management system may be formal or informal, depending on the size and nature of the organisation.

Within an overarching management system an MSR directs and controls an organisation by establishing a policy and objectives specifically in relation to recordkeeping. This is to 'ensure that authoritative and reliable information about, and evidence of, business activities is created, managed and made accessible to those who need it for as long as required' (AS/NZ ISO 30300, Introduction).

The MSR standards are a set of tools *aimed specifically at management* as a governance framework for recordkeeping. They provide for the implementation of a systematic and verifiable approach to the creation and control of records, linked to issues of governance, business effectiveness, risk and security.

The MSR focuses on managing the organisation, whereas our foundation standard *AS ISO 15489 Information and documentation – Records management* focuses on managing records and records systems. AS ISO 15489 and other ISO and Australian standards are related products to the MSR series, and are used to design and implement recordkeeping operations.

In our first two products, AS/NZ ISO 30300 defines the fundamentals of an MSR and contains the vocabulary used in MSR standards. AS/NZ ISO 30301 establishes the requirements for designing, implementing and continually improving an MSR. It includes defining the policy and objectives for recordkeeping, defining roles and responsibilities, designing

and implementing systematic processes, measuring and evaluating the performance of the MSR to ensure it is meeting the objectives, and reviewing and improving the MSR.

A further International Standard is being developed – *ISO 30302 Management systems for records - Guidance for implementation*. This will help organisations implement an MSR in accordance with the requirements in ISO 30301 (or AS/NZ ISO 30301).

In time a national certification scheme will be established in Australia, whereby organisations can seek certification against AS/NZ ISO 30301.

So why would an organisation choose to implement an MSR, and potentially obtain certification? At a strategic level it creates an infrastructure that supports legal compliance, good corporate governance, risk management, and the building of trusted environments for conducting business between entities. It also enables integration of recordkeeping into the processes of other commonly used management systems standards such as quality and information security. At an operational level it enables the integration of recordkeeping into business processes, eliminates redundancy, establishes consistency, optimizes processes and resources, and improves decision-making. It enables the use and reuse of information as a business and commercial asset. ❖

➲ More Information

- For further information about these developments, see the ISO website for MSR: http://isotc.iso.org/livelink/livelink?func=ll&objId=11600905&objAction=browse&viewType=1
- Or join the LinkedIn MSR Group: http://www.linkedin.com/groups/ISO-30300-Management-systems-records-4175551?trk=myg_ugrp_ovr
- The Standards can be purchased online at: http://www.saiglobal.com

• ISO material quoted in this paper are extracts from the relevant cited standard, or based on it, and is reproduced with permission from SAI Global Ltd under Licence 1208-c030.

ABOUT THE AUTHOR

Judith Ellis BA (Hons), MA, MRIM, AIMM, MACS is Managing Director, Enterprise Knowledge and Chair of the Standards Australia IT 21 sub-committee on MSR. She is also Convenor, ISO/TC 46/SC11 Working Group 8 on MSR.

First NZ Public Records audit report disappoints professionals

A Government report on the first New Zealand public recordkeeping audits has been published, without fanfare or advance notice, 18 months after the surveys and just before the Christmas/New Year holiday shut down. **Mike Steemson** reports

The report on 38 agency audits undertaken between July 2010 and June 2011 appeared unannounced on the Archives New Zealand website on 17 December, nine days after its unnoticed and publicly unreported tabling in the Wellington Parliament. Offices surveyed ranged from the little NZ Blood Service to the major entities such as the Department of Conservation and State Services Commission, the public service management agency.

Kiwi recordkeeping professionals reacted strongly to the delayed report. A senior public sector records manager told *iQ*: "It is a matter of concern if subsequent reports also take this amount of time to see the light of day. The audits become less and less valuable with the passing of time. If they show bad procedures, after delays as long as this, there's less comeback. Executives will know that it doesn't really matter."

Public recordkeeping observers say the report, the *Chief Archivist's Report to the Minister: Public Records Act 2005 Audits 2010/2011*[1], was completed months before, but no explanation for the delay had been offered by the Government agency responsible, the Department of Internal Affairs.


Greg Goulding

Reaction from Archives New Zealand Chief Archivist, Greg Goulding, early in the new year gave little explanation other than to say: "While we understand the concern about the delay in presenting this report, it should be noted that each agency that was audited received an individual report on the findings in that agency immediately on completion of the audit. We are on track to have the second report (on the 2011/12 year) tabled before the middle of 2013."

DISMAY AT BROMIDE RESULTS

Information professionals in public and private sectors were also dismayed at the bromide phraseology in the 25-page document. The report is notable for its frequent use of phrases like "the audit found no evidence of significant failure to meet the requirements", "evidence of work being done in the records management areas," and "overall the awareness of requirements is good".

It is illuminated by a decorative, diagrammatic display of audit results aggregated to "best fit across the body of audited public offices".

A district health board records manager protested: "The audits found no evidence of significant failure to meet the requirements of the Act yet the diagrammatic display reveals that five percent of those audited had 'no awareness of the need for and basic implementation of recordkeeping requirements'. How does that work?"

The officer continued: "Almost a quarter of the audited agencies also showed no 'awareness of the need for and basic implementation of systems and/or controls for the creation and capture of records'. How do the findings match these results?

ABOUT THE AUTHOR

Former London newspaperman Michael Steemson, ARMA, is the principal of the Calderson Consultancy in Wellington New Zealand and a member of the editorial board of *iQ*.

✉ He can be contacted at mike.steemson@xtra.co.nz

REPORT "DOESN'T REGISTER"

"What I find worrying is that there is no indication of what has happened to these public offices. Have they been offered guidance to improve recordkeeping, been given deadlines to implement recommendations? In comparison with the results of the recent information security audit this report just doesn't register. I know where we will be focussing our efforts from here on."

A private sector information manager complained: "Personally I want to see the detail that sits underneath this report. I do not trust the figures that are shown here. I have worked with a number of these organisations and the facts simply don't support what is documented here."

A records officer who has worked with two of the audited agencies reported: "From my experience, I very much doubt the reported 'commitment to recordkeeping capability improvement' is actually happening especially now the razor gang in Parliament is slashing public sector jobs left right and centre. What did the independent auditors do to confirm what they were told?"

A district council records department leader was equally dismissive, commenting: "While the key findings speak of a high level of commitment, the numbers shown in the statistical summary do not convincingly support that claim. "

But the officer was more positive about the report overall, saying: "The report is interesting enough, largely because it's a first. The content is rather disappointing. It may advance the cause of good recordkeeping but only imperceptibly." ❖

Bibliography

1 *Chief Archivist's Report to the Minister: Public Records Act 2005 Audits 2010/2011*, see http://archives.govt.nz/advice/public-records-act-2005/chief-archivist-s-report-minister-public-records-act-2005-audits-2010.

The future of records management: a personal view

When the author became a records manager, the PC had just been invented. In that time she has seen considerable change in the profession. Here, she outlines where she believes the profession needs to move as the change from records to data management takes place.

By **Deborah Talbot**

When I started working as a records manager, recordkeeping was based around paper records – with very little interest in the electronic record. Since that time businesses have embraced technology and electronic records have become prolific. We went through the discussions on the *paperless office* – but this has never eventuated and never will as so many people still print their electronic documents. Even today's Y generation – who don't know what life is like without the computer, internet and electronic devices – print just as much as other generations because they absorb information differently depending on the media they are using to view it.

In recent years the move from PCs to mobile personal devices could be considered the same level of quantum leap for recordkeeping as the invention of the PC in the 1980s.

Many schools have introduced Mac technology in order for students to gain computer literacy as well as to enhance the learning experience. This means that businesses which are currently using Microsoft functionality may need to look at the skills that new starters are bringing with them. The new starters will be used to one interface and the market share of Apple over Android / Google smartphones will also influence how people want to interface with the electronic world.

Schools and businesses are now bringing in the Bring Your Own Device (BYOD) strategy so that users can interface with the network and cloud computing on whatever device they are comfortable with. With a move to cloud computing the need for records management will probably become less obvious to the business world. However, it will still need to be undertaken. An example of where this could lead is with the UK Web Archive at the British Library planned adoption of a crowd-sourcing approach to their appraisal decisions.

I have found over the years with managing paper records that many managers choose to reschedule a box of records rather than make the decision to actually destroy something "in case it is needed in the future". This is especially the case when the records are inherited from a previous manager. This issue will only be exacerbated in the electronic world where the cost of storage is decreasing, and everything can be found by a global search facility "if it's needed".

Many people nowadays rely on the ability of free text search engines to find everything on a particular topic and have lost the concept of using quality metadata to enhance the search results. This is something I have found when migrating from a records management system to something like SharePoint with a full text engine indexing the full document and the IT project manager not understanding the value of the metadata fields already established for the existing system. Will this matter in the future? Classification schemes are no longer apparently necessary as they were used for managing the physical location of a record. However, an understanding of classification and taxonomy is still required as it assists in managing views of records.

IN 10 YEARS' TIME...

As for the future of records management, I see a move away from embedded PC-based technologies to cloud computing using mobile devices and mobile apps. More people are telecommuting to work; the use of Telepresence and shared desktop applications will create more potential for remote working situations requiring access via mobile device applications.

In 10 years' time we will not recognise the applications and devices available. Records management will have moved from being a custodial role to that of value enhancement of the knowledge held in records systems. As Xiaolin Zhang mentioned in his plenary address at the VALA2012 conference, the information management space needs "new generations of knowledge access capabilities".

Publishers are currently experimenting with semantic publishing and records management appears to be going

down the same path when it comes to semantic searching rather than the classification and keyword/thesaurus based systems of the past.

Records are becoming intelligent and computable so that the value adding of that intelligent content is an opportunity that will need to be considered. I agree with Zhang's statement "with e-society everything is within easy reach" whereas in the past the different information management islands were separated, technology is now bridging those islands together with a blurring of the roles for records management, librarianship, archives management, IT etc.

I see a role for the information specialist that crosses those boundaries, not in the distant future but already starting. Over the past 30 years, my experience and qualifications in librarianship, records management, archives, information and knowledge management has placed me in an ideal position to bring these information streams together to the advantage of the organisations for which I have worked. There are many synergies between these related disciplines and the new mobile technologies provide an opportunity for these synergies to be realised.

For me the future is a merging of the information disciplines to value-add the knowledge products they manage. For many people the use of cloud technologies gives them freedom from perceived constraints placed on them by systems administrators, records managers etc to the managing of what they see as 'their' information. The role of the records manager (information professional) will be to make the management of the cloud-based systems more effective for the user in a seamless way that they are unaware of the 'work behind the cloud'. The user just wants to know they have records stored somewhere; they don't want to be bothered with the management of that storehouse. The information professional will be concerned with taxonomies and information management so the cloud will work effectively.

Ambient sensors are also coming into the forefront of data sourcing and there is a need to be able to manage the data from such sources. Therefore, I see a move from records to data management as an integral part of the records manager's role.

Above all, however, is a need for a clear understanding of information architecture, user requirements, where users source information, how they use it and what information they generate. An ability for records manager to undertake user needs analysis, information audits and develop strategies to meet these needs will be integral to the success of the profession. They must move away from rigid classification schemes to app-based systems that users feel comfortable with in order to prepare for the BYO device strategies that are developing now. ❖

ABOUT THE AUTHOR

Deborah Talbot has been employed in Information Management in the corporate sector for over 30 years. She works at Rio Tinto Exploration as Information Specialist, and is the J Eddis Linton Student of the Year for 2012.

THE PSYCHOLOGY OF RECORDS MANAGEMENT

How do we change the thinking of the rest of the company to see the importance of RIM as a corporate asset? **Craig Grimestad** asks

Records and Information Management (RIM) is a fascinating occupation, the only one that I can think of that is essential to a company's wellbeing – yet has no priority. Except for a small program team that has the word 'Records' in their job description, RIM has no priority for any other individual. Can anyone say, "I didn't meet the deadline because I was working on RIM"? (Maybe you can if they don't know what RIM stands for, but that's not good either.) Or, "I missed the meeting because I was too busy organising my records." Finally, how about, "We're too busy deleting our courtesy copies to answer our customer's question." **When put side by side with any other business activity for resource priority, RIM always loses. Yet, at the end of the day, it must be done.** It must be done to ensure the business has, and can find, the information it needs to operate in the present as well as the future. It must be done – even without any priority.

Imagine papers lying on the floor, in hallways, in bathrooms, and literally flying in the breeze

I digress, but can you imagine a work environment without any RIM? Imagine papers lying on the floor, in hallways, in bathrooms, and literally flying in the breeze. Records may be in folders, but the folders have no identification and the contents have no known association. Everyone is free to pick up any paper they find, to read, to relocate, to keep, or to destroy – anytime they choose. Take some home and let your children use the back sides for their homework assignments. Grab a bunch and see if they will sell on eBay. If papers are in boxes, with the disarray of the papers in the box, it is hard to tell if they are garbage or storage. The thought is ludicrous. So it turns out we all have some inborn desire and instinctive nature to manage records. It's natural to manage records!

So with an innate desire to manage records, but no priority to do so, how does a company establish and manage an effective RIM program? The answer quite simply is psychology. *Psychology? Are you nuts?* Well maybe a little bit, but it is still the right answer. The corporate records manger, the departmental records coordinators and the rest of us in the industry know the rightful place of RIM. How do we change the thinking of the rest of the company to see it?

There are many components of RIM psychology from the boardroom to the workstation – too many to cover in one writing. But let's start at the top. **Records are a corporate asset**.

When the leadership team gets it, I mean really gets it – it is a game changer. You see they understand that assets represent value, and that assets require protection and maintenance. Buildings are insured, secured and maintained. Companies cut the grass, wash the windows, paint the walls, change light bulbs, maintain, repair, and replace heating, cooling, lighting, electrical and plumbing systems. It's just a building! But they value the asset. Records are also corporate assets. ❖

ABOUT THE AUTHOR

Craig Grimestad is a senior consultant with Iron Mountain Consulting. His specialty is designing RIM core components with a sub-specialty for RIM auditing. Craig holds a Masters of Science degree in Engineering and was the records manager for the Electro-Motive Division of General Motors where he participated in the development of the GM Corporate RIM program, and implemented and managed Electro-Motive Division's RIM program. He joined Iron Mountain in 2008.

• This is a foundation article for a series of articles the author is writing on the psychology of RIM. You can read more at http://blog.ironmountain.com/author/cgrimestad/

Access denied – navigating the digital information security maze

Out there, in the corridors of power, the compactuses of restriction and assorted business systems, there's a war going on. It's the 'War of Access'.

By **Kevin Dwyer** and **Michelle Linton**

In the 'War of Access', the fight is over who can, who should and who will see 'my' records. The two armies slogging it out in this cold war are the people of the business defending their right to individually and inconsistently determine who will see their records and the stewards of information, records management.

Prevarication rules as organisations avoid the proactive conversations necessary to make the hard decisions to develop a mature organisation-wide approach to accessing records – hard decisions that not everyone will like. The factions continue to reactively squabble with each other over the rules of operation and how to apply them and very little progress is made towards a better world.

When managing only paper records, business easily wins the fight. The Records and Information Management (RIM) team receive paper records when the business deems them to be important information needing protection. If the business doesn't want RIM or others to see the information then they simply don't tell them about it. It is squirrelled away in locked filing cabinets, personal drives or restricted access Windows folders. And of course only emailed to people that are trusted!

The business has a myopic view that their information is incredibly secure. They see some exceptions of course,

such as when their 'trusted' friend shares the email – innocently or otherwise, or those few other people who know their password use it or when the building burns down/is flooded. They see the likelihood of these incidents as so rare that it is not worth the complications of thinking about the security decisions to protect the organisation from the consequences.

The 'that won't happen to me' mentality fails to note that these 'rare' incidents have happened in almost every known organisation with disastrous consequences to reputation, finances and operations.

RIM has ploughed on, despite the resistance and the apparent desire of the business to fall on its own sword, to fight to protect their organisation's physical information assets. Then along came digital records in an electronic document and records management system (EDRMS). What a bonus! Now it's possible to register all records as they are created, apply appropriate security from the outset, control and audit who viewed, edited, shared, etc. the record, and reduce the risk of information loss for the organisation. RIM is now in a position to truly meet their responsibilities.

However, many businesses continue to thwart the best efforts of RIM through a somewhat tedious and erroneous list of excuses for not adopting organisation-wide access and security practices:

- *"I can never find records once they are in the EDRMS."*
- *"All it does is stop my team from accessing records they created."*
- *"Why should the RIM team have access to my sensitive records?"*
- *"People should come to me and ask my permission to see my records each time they want access so it might as well be in my shared drive."*

story snapshot

When a project is run to increase EDRMS adoption rates, there are inevitable fears about access to records.

Reluctance to embrace the EDRMS with good recordkeeping practices leads to higher risk to the organisation.

Information assets are managed by an information security approach that seeks to protect confidentiality, integrity and availability.

Configuring the EDRMS to meet an organisation's security policies and procedures is often tricky.

When a RIM team runs a project aimed at increasing EDRMS adoption rates amongst users they inevitably run up against fears about access to records either from the viewpoint that "Everyone will be able to see my files", to the other extreme of "I'll never find them again".

To win the battle, RIM needs the business to have faith that the records necessary to do their job can be accessed easily. At the same time, they need to have confidence that truly sensitive information is not viewable by unauthorised people. These are the cornerstones in gaining the trust of managers and users to move to or increase the use of digital recordkeeping.

It's not simple to create this environment of trust. The business has its own ideas of what security and access means and how to apply it. It's challenging to create the security protocols and environment that can be correctly interpreted and willingly applied by the business across multiple recordkeeping systems that keep records in digital, paper and other physical formats.

A lack of knowledge of information security as a topic and the role of recordkeeping and the use of EDRMS functionality helps create and perpetuate myths and stories that reduce that faith considerably and perpetuate the reactive war. Sadly, the result of this reluctance to embrace the EDRMS with good recordkeeping practices is higher risks to the organisation and reduced productivity.

UNBUNDLING INFORMATION SECURITY

It is important when trying to navigate the word of digital information security as applied by an EDRMS to understand the context in which it sits.

The starting point of managing information security is for an organisation to understand what its information assets are.

An information asset is information that has value to the organisation. An information asset may not be a record. A record, being evidence of a business decision, is most likely to be, however, an information asset. In most organisations, information assets are managed by an information security approach that seeks to protect:

- confidentiality, by ensuring that information is only accessed by authorised individuals
- integrity, by ensuring the accuracy and completeness of information
- availability, by ensuring access to information, systems, networks and applications.

A range of approaches including physical security (locks, codes etc.), password protection, intrusion detection and prevention, security classification labelling, encryption, secure shredding and plain simple security awareness protect information assets as part of an information security management system (ISMS).

Recordkeeping practices utilising the functionality of an EDRMS have a large part to play in supporting an ISMS. The EDRMS also creates an auditable security trail throughout the life of the record enabling breaches of security to be managed at their source. Also, in the event of a disaster, there is immediate availability to digital records, increasing customer confidence and reducing loss of business.

SECURITY & ACCESS IN AN EDRMS

Digital information assets deemed to be records and stored in an EDRMS generally have their access described by three attributes: security classification, caveats and access control.

Security classifications

Security classifications may apply to records (documents and folders). The security classifications in the EDRMS should mirror those of the information security policy. The classifications used depend on which standard the organisation wishes to follow. An example is the Australian Government Security Classification (Table 1).

SECURITY CLASSIFICATION	TO BE USED WHEN
UNCLASSIFIED	Information is released within the organisation on the basis of 'need to know' but is not restricted. Information is not released outside the organisation without the permission of the owner of the information.
UNCLASSIFIED with Dissemination Limiting Markers Eg: For Official Use Only (FOUO) Sensitive: Personal Sensitive: Legal	Information can only be released to organisations and individuals with a demonstrated need to know and information is to be stored and processed away from public access.
PROTECTED	Used when the compromise of the information could cause damage to the Australian Government, commercial entities or members of the public – eg, tender documents.
CONFIDENTIAL	Used when the compromise of the information it relates to must be considered as possibly causing damage to national security – eg, damage diplomatic relations.
SECRET	Used when the compromise of information could cause serious damage to national security, the Australian Government, nationally important economic and commercial interests, or threaten life – eg, raise international tension.
TOP SECRET	Used when the compromise of information could cause exceptionally grave damage to national security – eg, lead directly to widespread loss of life.

Table 1: Australian Government Security Classification

The first level of classification is UNCLASSIFIED, which should be the default. UNCLASSIFIED can be strengthened by use of a dissemination limiting marker (DLM). Their purpose is to restrict release of information to a group of people for a purpose. For example, a record classified UNCLASSIFIED: Sensitive: Legal is likely to be restricted to people in the legal department.

The levels of classification impose increasing restrictions on their storage, distribution, copying and destruction.

Most organisations will have well over 95 per cent of their records classified as UNCLASSIFIED or PROTECTED (or equivalent eg, in-confidence).

Caveats

A caveat is a warning that the information has special requirements in addition to those indicated by the security classification. It is generally used to limit specific types of records to specific roles across an organisation, such as HR records types to HR roles. When it is used those people who need to know about its use need be involved and educated. Others in the organisation do not need to know about the use of caveats.

Access control

Access controls are the most specific level of security applied to records in an EDRMS. Access control is an individual

security control and is applied to individual records. Access controls restrict access across a range of properties such as: View Document, View Metadata, Update Document, Update Record Metadata, Modify Record Access,

Access controls when thought through well, combined with security classifications usually provide sufficient security control through an EDRMS.

EDRMS OBJECT CONFIGURATION

Configuring the EDRMS to meet an organisation's security policies and procedures is often tricky. At a minimum there are three objects to be configured: record types, profiles/locations and classifications.

The goal is to determine how to apply a combination of security attributes to each of the objects in a complementary manner. When an EDRMS was a new digital records system the simplistic approach was to provide each business group with their own record type and security configuration. It was not unusual (and is still prevalent) to see 25 folder types, one for each branch, and 25 document types as well. Specialist record types were in addition to this. Not only was this a nightmare for RIM to maintain, it supported information silos rather than information access, and users complained.

As EDRMS configuration has matured RIM has become aware of complex combinations of object configuration that minimise maintenance and promote improved sharing of information. Using the previous example, a folder record type with default full access to the owner of the record, and view-only access to all other groups, combined with inherited security for document record types, reduces 50 records types to two.

NAVIGATING THE CHALLENGES

Security and access and object configuration is not new. It exists in physical records management. The difference is it's enforced in an EDRMS. That can make it difficult for even the best recordkeepers in an organisation to adapt to the change.

Imagine this scenario. You're an executive assistant in Branch 1. The director of Branch 2 requests a record that is classified as confidential to Branch 1. You know this record has been discussed with the director and they have had input into it. In a paper-based world it was easy to decide the information could be shared with this person and to take a copy and send it around. Rightly or wrongly it happened. In a Windows folder world it is printed and provided. In an EDRMS, any action on that record is audited and the breach of security recorded. The answer to the director must be no. The executive assistant is not happy, the director is not happy, and the EDRMS is seen as restrictive rather than upholding the policy of the organisation.

To avoid this unhappy circumstance being the norm in an organisation, there are several simple things which need addressing.

Overuse of security and access controls

The most common issue plaguing the application of security policy to an EDRMS is the over-classification of records and the over-use of access controls.

People who have come from an environment of personally designed file structures on a shared drive have a sense of 'ownership' of information that goes well beyond any requirements of information security. They are loath to share their information with colleagues in their section let alone the whole organisation. The consequence of extending this approach to an EDRMS is to make records unavailable to staff who have a need to share the information.

The result is frustration and unproductive work by the RIM unit and the end-users as permission is sought and gained to open up access to the records. Over-classification results in unnecessary, administrative arrangements that remain in force for the life of the record. The volume of security classified information becomes too large for an organisation to protect adequately. Over-classification brings security classification and associated security procedures into disrepute. This often leads to security classifications being devalued or ignored by organisation employees.

The default security level should be UNCLASSIFIED. The default access control for all records should preferably be the whole organisation. The vast majority of records should be viewable by anyone in the organisation. This is rarely the case. Higher classifications should be used sparingly and only when the record meets the requirement of the classification. Most organisations, for example, will have very few, if any, CONFIDENTIAL records as defined in the Australian Government Classification system.

Policy & procedure

Security is not a popular topic in most organisations. Spend time and effort to make people aware of the policy for applying additional security and the need to abide by the policy and to follow the procedures. Ensure emphasis is given to the procedure for applying for permission for others to have access if necessary.

Continuing education

Make sure people are aware of how security works and what is happening when they apply it. Telling people how to apply security is insufficient. Educate people in the difficulties that result when incorrect security and access options are applied. Have people experience the difficulty in finding a record if view metadata access has been denied, or a caveat is applied.

Be proactive about managing the situation, rather than reactively adjusting access record by record as requests come in. And expect that education is ongoing. Managing the security of information is a priority and the majority of organisations are many years from achieving full EDRMS security maturity.

ABOUT THE AUTHORS

Michelle Linton, Managing Director, Linked Training
Michelle is a Learning & Development professional with 24 years' experience in the planning, design and delivery of training programs. Michelle has developed and delivered innovative, outcome focused EDRMS training for over 30 government and private organisations since 2005. Michelle's pragmatic approach to learning strategies leading to application adoption has been enthusiastically welcomed by the industry, and she is a regular speaker at RIM events and contributor to industry magazines. Linked Training is the training partner in the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.
✉ She can be contacted at Michelle@LinkedTraining.com.au

Kevin Dwyer, Director, Change Factory
Kevin is a Change Management professional with more than 30 years' experience in the planning, design and delivery of change management programs. Since 2001, and the establishment of Change Factory, he has been involved in many Change Management projects ranging from re-engineering of customs processes to reduce risk to creating and revising performance management systems to improve customer service outcomes at five-star resorts. His first EDRMS project was as the Change Management partner for the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.
✉ He can be contacted at Kevin.Dwyer@changefactory.com.au

Wants versus needs

Individuals within the business will provide RIM with a description of what they 'want' in security configuration, which is often overly cautious for the majority of records. RIM must discover the business goal, which will inform the actual 'need'. This is frequently not what was asked for, so demonstration is then required to provide all stakeholders with confidence in the solution.

RIM sense and sensibility

Sense: the ability to think or reason soundly. Sensibility: an acute perception of, or responsiveness toward something.

Sometimes RIM are their own worst enemy by taking a conservative view of security themselves and being very fixed in their approach to applying the security policy to the EDRMS. Take the situation where a manager had been acting up for six months and has written a record that was the responsibility of the higher position. The following year, now seated in the lower position, his manager asks him to update the record. After fruitlessly searching for it, he contacts RIM and is informed access is restricted to the higher level position and above. After explaining the situation and requesting access the answer is a resounding NO.

Technically the RIM staff member was correct, but the person wasn't even provided with the protocol for having the access adjusted. There will always be valid exceptions to a rule, and RIM staff need to be educated on how to manage them and keep people onside.

The reverse situation has been seen also, where the business pleaded for a single unclassified folder type to facilitate cross-functional sharing and enable the executive team to access information. The change required, in both approach and restructuring, was outside the comfort zone of the records unit, and was stubbornly blocked. The business, in return, was equally stubborn in refusing to use the EDRMS. ❖

Compliance cost associated with the storage of unstructured information

The purpose of this study, sponsored by Novell, is to better understand compliance costs associated with the storage of unstructured information within business organisations.[1]

By **Ponemon Institute** and **Tripwire**

Our definition of compliance costs goes beyond efforts dedicated to privacy and data protection. It includes the management storage systems (a.k.a. configuration management), access governance and e-discovery operations. Safeguarding an organisation's unstructured information from unauthorised access or misuse has become a daunting task for those responsible for its security, especially when the storage system does not directly reveal the creator, owner or primary users of stored information at the file level.

In an earlier study of more than 800 IT practitioners in US organisations, we determined that a significant amount of an organisation's sensitive or critical information is stored in an unstructured form.[2] Such data might include information about customers, employees, sales results, research, legal and compliance, finance and executive or board meetings. We also found that much of this information may not be well protected, thus increasing the risk of data loss or theft. Finally, our research shows that the storage of unstructured files are

increasing rapidly, thus exacerbating the need for greater efficiency, control and compliance.

Drawing upon our proprietary database of 94 larger-sized benchmarked companies located in the US, we present re-analysed cost results on the compliance activities associated with the storage of unstructured information. Our re-analysis of these benchmarked companies focus on the preventive and corrective controls implemented by them to secure a broad range of stored information, including documents, presentations, spreadsheets and other intellectual properties.

Using an activity-based costing framework, our re-analysis captures both the direct and indirect costs associated with unstructured information contained on permanent storage devices (not including portable data-bearing devices). In this context, we define costs to include all cash expenditures and internal costs including labor and overhead. Our analysis does not include soft costs such as opportunity losses, reputation damages and other intangible consequences of noncompliance.

SUMMARY OF KEY FINDINGS

Please note that the illustration on page 18 reports the activity-based costing framework used in this re-analysis.

This framework consists of nine discernible cost activity centres that define compliance costs associated with the storage of unstructured information for a one-year period. Following are the most salient findings of this research.

- The cost of compliance associated with the storage of unstructured information is expensive. On an annual basis, we estimate $2.1 million as the average cost for 94 benchmarked organisations. The minimum cost is nearly $400k and the maximum cost is over $7.1 million.
- Approximately 61 per cent of compliance costs are considered direct cost and 39 per cent indirect costs. The spilt between direct and indirect cost varies considerably among the nine activity cost centres examined.
- The most frequently cited compliance activities include backup and disaster recovery operations, and access governance activities. The least frequent include policy management and monitoring or scanning activities.
- Overall, the most expensive compliance activities include e-discovery ($768k), assessment and audit ($637k), and access governance ($594k).
- With respect to direct costs, the most expensive compliance activities include access governance ($400k) and e-discovery ($390k).
- Compliance costs increase with organisational size (headcount), but the rate of increase seems to be relatively flat. This suggests that smaller organisations incur a relatively higher cost burden than larger companies. The average cost for organisations with less than 5,000 employees is $1.23 million, while the average cost for organisations with more than 75,000 is $2.71 million.
- Among 11 industries, we found that industrial ($2.81 million), pharmaceuticals ($2.73 million), communications ($2.52 million) and financial services ($2.52 million) experience the highest average cost of compliance with respect to the storage of unstructured information.

COST FRAMEWORK

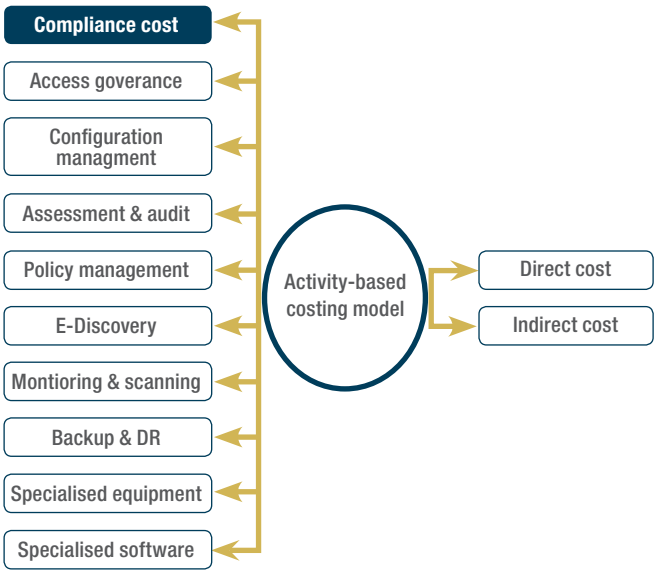
Our primary method for determining the cost compliance associated with data storage relies on the objective collection of cost data. Using a well-known cost accounting method, we were able to allocate detailed cost data into discernible activity centres that explain the entire data protection and compliance mandate within benchmarked companies.[3]

We determined that the following nine cost activity centres explain the economic impact of compliance costs associated with the storage of unstructured information. Within each centre, we compile the direct and indirect costs associated with each activity.

Following are nine cost categories included in our activity-based cost analysis.

- **Access governance** – consists of all compliance activities associated with identity, authentication, provisioning and access rights to data stored on different platforms or configurations.
- **Configuration management** – consists of all compliance activities associated with establishing and maintaining data storage requirements at the rack, volume and file level. This category also includes storage allocation and re-allocation decisions according to data centre management policies.
- **Assessment and audit** – consists of activities associated with the review, evaluation and verification of data storage according to the organisation's policies and security requirements. This category also includes information governance assessment, including the review of storage providers in cloud or virtual environments.
- **Policy management** – consists of all activities that are associated with the development, implementation and enforcement of company storage requirements (including those requirements specified by laws and regulations. This category includes the deployment of automated policy engines or tagging applications. It also includes data partitioning or classification schemes associated with different volumes or file storage systems. Finally, this cost category includes the maintenance of data archiving rules.
- **E-Discovery** – these costs are associated with the discovery of electronic documents contained on the organisation's storage devices typically required in litigation. It also includes other legal defence and compliance costs associated with the e-discovery process.
- **Monitoring and scanning** – consists of all activities associated with monitoring storage policies and related compliance requirements as established by the company. While much of this cost is incurred in the organisation's data centre, it also includes remote monitoring efforts that may occur in outsourced or cloud storage environments. Scanning activities include the review of storage devices according to physical (environmental) and virtual metrics.
- **Backup and disaster recovery** – includes all compliance costs associated with routine data backup efforts as well as all methods deployed to fend off various disasters including weather, cyber attacks, flooding, fire and so forth. This category also includes all costs incurred to recover data from damaged storage devices.
- **Specialised equipment cost** – includes all expenditures, implementation and operating costs associated with equipment that facilitates the organisation's data storage compliance efforts. Such equipment includes environmental control systems at the storage device or rack level. It also includes hardware maintenance and upgrade costs.
- **Specialised software cost** – includes all expenditures, implementation and operating costs associated with software programs (applications) that facilitate the organisation's data storage compliance efforts. It also includes software maintenance and upgrade costs.

This illustration (this page, top) presents the activity-based costing framework used in this research to define the compliance cost associated with unstructured information storage. As can be seen, it consists of nine discernible cost centre activities. Each one of these activities generates both direct and indirect costs (in different proportions).

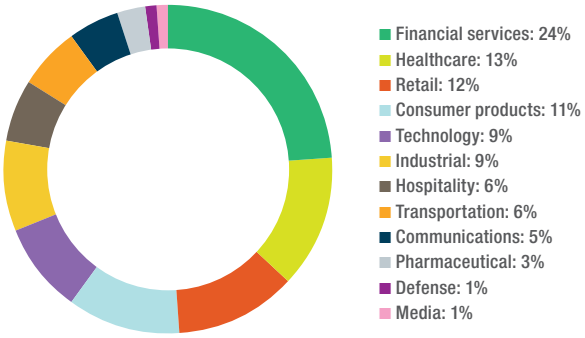


Compliance cost framework for the storage of unstructured information

CARVE-OUT SAMPLE

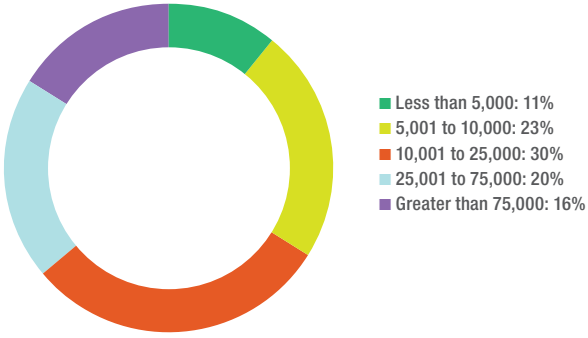
The pie chart directly below reports the percentage of companies by industry included in our benchmark analysis.

Our final carve-out sample includes 94 organisations. Each organisation serves as the unit of analysis. A total of 313 benchmarked organisations (a.k.a. case studies) were initially evaluated for inclusion in our analysis. However, 219 were rejected because they lacked robust information relating to data storage systems and specific compliance effort. Financial service companies represent the largest segment (24 per cent), following by healthcare (13 per cent) and retail (12 per cent).



Industry classification of the benchmark sample
For 94 benchmarked companies

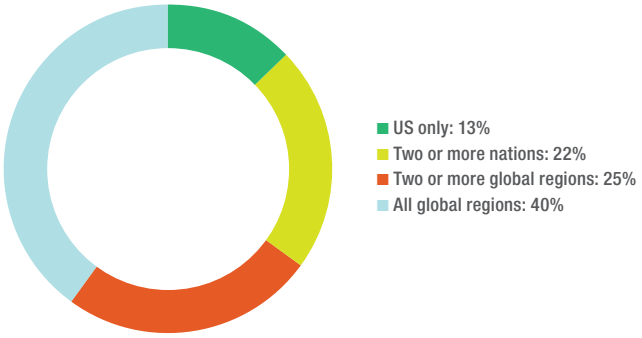
The pie chart below reports the headcount of organisations included in this benchmark sample. As can be seen, two-thirds (66 per cent) are organisations with more than 10,000 full-time employees.



Benchmark sample by global headcount (size)
For 94 benchmarked companies

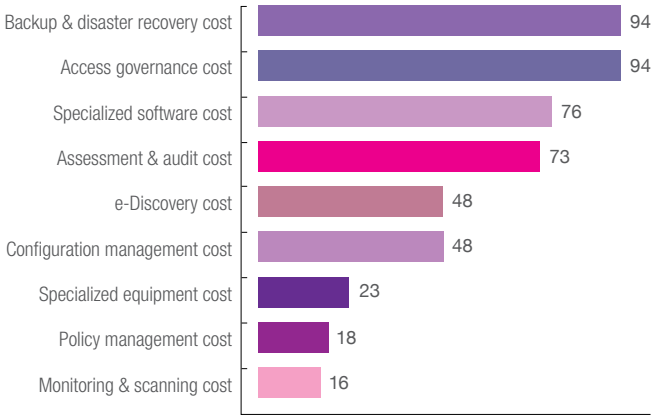
To maintain complete confidentiality, the benchmark database does not contain company-specific information of any kind.

The pie chart below reports the global footprint included in this benchmark sample. As shown, 40 per cent of companies operate in all global regions. Another 25 per cent operate in two or more global regions. Only 13 per cent operate solely in the United States.



Benchmark sample by global footprint
For 94 benchmarked companies

The bar chart below reports the frequency of cost activity centres examined in this research. As can be seen, two cost activity centres – backup and disaster recover and access governance – are present in all 94 companies. The remaining seven activity centres are present in only a subset of benchmarked companies.



Frequency of nine cost activity centres
For 94 benchmarked companies

BENCHMARK METHODS

To obtain information about each organisation's compliance and related management costs associated with unstructured information, the researchers utilised an activity-based costing method and a proprietary diagnostic interviewing technique. Ponemon Institute's benchmark database contains descriptive costs for literally hundreds of cost activities relating to data protection, compliance (with applicable laws and regulations globally), and infrastructure. Within each cost centre, we estimated both the direct and indirect compliance cost defined as follows:

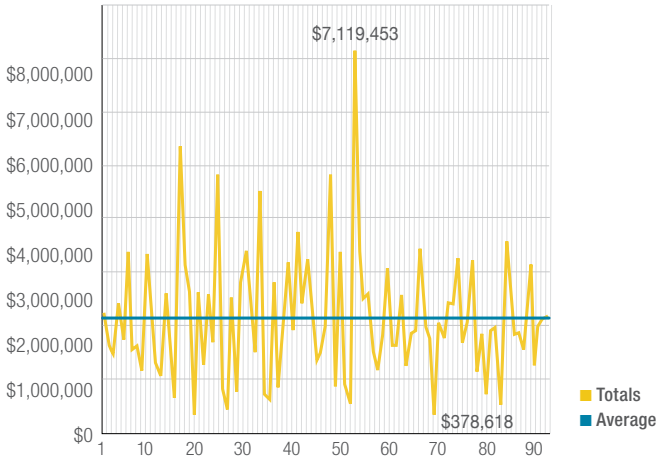
- Direct cost – the direct expense outlay to accomplish a given activity.
- Indirect cost – the amount of other organisational resources spent, but not as a direct cash outlay.

Our benchmark database was designed to collect descriptive information from companies' compliance efforts. Our research design relies upon a shadow costing method used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of individuals within participating organisations. Hence, we extrapolated the costs incurred by each organisation either directly or indirectly to achieve compliance with a plethora of different requirements.

Within each category, cost estimation is a two-stage process. First, the survey requires benchmarked companies to provide direct cost estimates for each cost category by checking a range variable. A range variable is used rather than a point estimate to preserve confidentiality (in order to ensure a higher response rate). Second, the survey requires companies to provide a second estimate for indirect cost. These estimates are calculated based on the relative magnitude of indirect cost in comparison to a direct cost within a given category.

The size and scope of benchmarked activities are limited to known cost categories that cut across different industry sectors. To maintain complete confidentiality, the benchmark database does not contain company-specific information of any kind. Research materials do not contain tracking codes or other methods that could link responses to participating companies.

The present benchmarking process started with the re-analysis of 313 separate organisations with specific focus on all activities associated with the compliance of unstructured information retained in permanent storage systems. As mentioned, a total of 94 organisations had sufficient detailed results for our re-analysis. The benchmark data used in this report is not older than 24 months. The following graph reports the total activity cost distribution of our carve-out sample.



Distribution of total activity costs
For 94 benchmarked companies

RESULTS

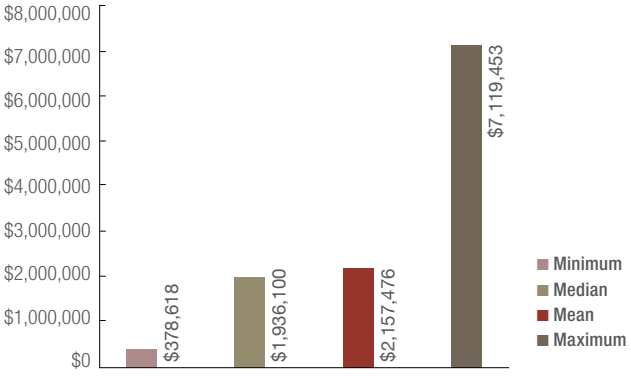
The following table summarises the benchmark results on compliance cost associated with the storage of unstructured information. Please note that additional details will be provided in the final report.

COST ACTIVITIES	AVERAGE	MEDIAN	MINIMUM	MAXIMUM
Access governance	593,939	360,984	68,324	4,341,378
Configuration management	314,217	244,590	15,508	1,678,507
Assessment & audit	636,873	607,008	52,607	1,973,607
Policy management	173,216	137,039	7,607	876,500
E-Discovery	768,977	684,344	198,100	1,588,369
Monitoring & scanning	94,349	67,336	33,576	500,100
Backup & disaster recovery	126,604	110,419	26,564	326,934
Specialized equipment cost	222,707	137,784	10,866	889,037
Specialized software cost	353,117	272,882	3,914	856,485
Totals	$2,157,476	$1,936,100	$378,618	$7,119,453

The cost of compliance associated with the storage of unstructured information is expensive. As shown in the bar chart below, we estimate $2,157,476 as the average annual cost for 94 benchmarked organisations. The minimum cost is $378,618 and the maximum cost is $7,119,453.

Overall, the most expensive compliance activities include e-discovery ($768,977), assessment and audit ($636,873), and access governance ($593,939).

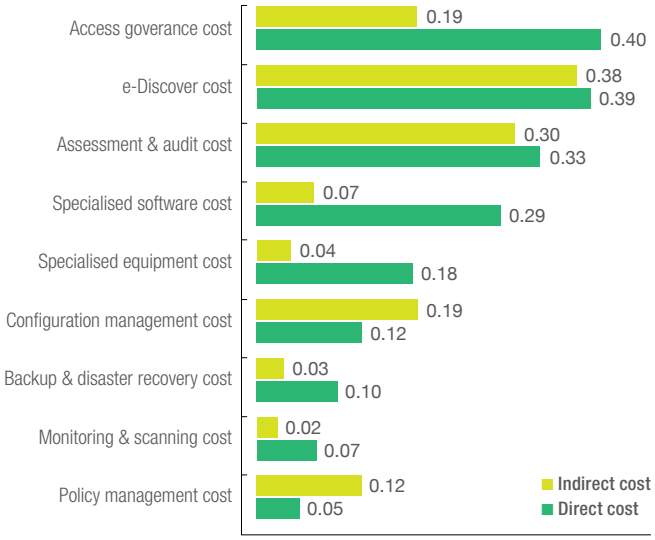
A majority of costs are classified as direct. Approximately 61 per cent of compliance costs are direct ($1,326,141) and 39 per cent indirect ($831,334). As previously noted, direct costs include all cash expenses and outlay to accomplish a given activity such as consultants, legal experts, external audits and so forth. Indirect costs are the labour, overhead and other organisational resources spent, but not a direct cash outlay.



Overall activity cost statistics
For 94 benchmarked companies

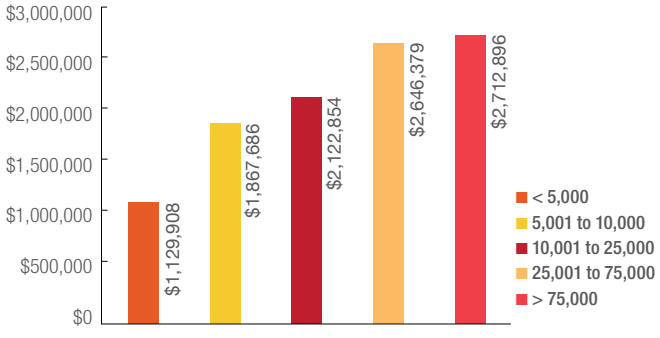
The chart suggests smaller-sized organisations incur a relatively higher cost burden than larger companies

As shown in the bar chart directly below, the spilt between direct and indirect cost varies considerably among the nine activity cost centres examined. With respect to direct costs, the most expensive compliance activities include access governance and e-discovery. With respect to indirect costs, the most expensive are e-discovery and assessment and audit activities.



Direct and indirect cost of compliance by activity center
For 94 benchmarked companies, $1,000,000 omitted

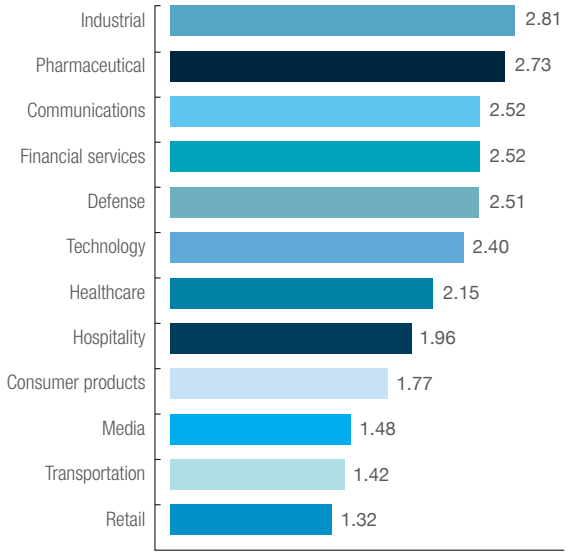
As noted in the bar chart below, compliance costs increase with organisational headcount. However, the rate of increase seems to be relatively flat. The average cost for organisations with fewer than 5,000 employees is $1,129,908, while the average cost for organisations with more than 75,000 is $2,712,896.



Activity cost by organisational headcount (size)
For 94 benchmarked companies

The above chart suggests smaller-sized organisations incur a relatively higher cost burden than larger companies.

In terms of industry differences, we found that industrial, pharmaceuticals, communications, and financial services experience a higher average compliance activity cost with respect to storage of unstructured information. Please note some industry sectors are too small to draw inferences about industry differences – see bar chart above right.



Activity cost industry classification
For 94 benchmarked companies, $1,000,000 omitted

CAVEATS

This study utilises a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing definitive conclusions from findings.

- **Non-statistical results:** The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of data centres. Statistical inferences, margins of error and confidence intervals cannot be applied to these data by virtue of non-scientific sampling methods.
- **Non-response:** The current findings are based on a small representative sample of 94 completed case studies selected from 313 separate organisations. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the underlying costs involved in safeguarding unstructured information on various storage systems.
- **Sampling-frame bias:** Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature compliance programs.
- **Company-specific information:** The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- **Unmeasured factors:** To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organisational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- **Estimated cost results:** The quality of survey research is based on the integrity of confidential responses received from benchmarked organisations. While certain checks and balances can be incorporated into the data capture process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results. ❖

• A full copy of the report can be found at: http://www.novell.com/docrep/2011/07/ponemon_true_cost_of_compliance.pdf

ABOUT THE AUTHOR
Ponemon Institute and Tripwire.
✉ Ponemon Institute can be contacted at research@ponemon.org

Bibliography

1 Unstructured information refers to electronic information on file servers and Network Attached Storage (NAS) devices that is not stored in a database or in a document/content management system. Examples may include electronic spreadsheets, PowerPoint and Word documents, audio files, video, blueprints, software source code, instant messages, Web pages and so forth. A large per centage of unstructured data is, or contains, sensitive or confidential business information. A typical business or government organisation stores many thousands of files containing sensitive data in documents and files in shared folders on SAN, NAS and DAS storage systems.
2 See: Survey on the Governance of Unstructured Data, Ponemon Institute May 2008
3 Ponemon Institute's Cost of Data Breach studies conducted over the past six years utilises activity-based cost to define the total economic impact of data loss or theft that requires notification. See, for example, 2010 Cost of Data Breach, Ponemon Institute January 2011.

Life in the fast lane

Be the speedster in the career-change velodrome. **Deborah Tarrant** details the top 20 ways to fast-track a career

1 TAKE A LEAP

Fast-tracking a career requires more than a fresh mindset, says John Rawlinson, Group CEO of global recruitment firm Talent2. Those who feel stuck in an area of technical expertise should remember that competencies are not job-specific. "In a job search, highlight exactly what you can do, not just what you have done," advises Rawlinson, who is a living example of what he preaches. Years ago he leapt from being a PE teacher to become a sales rep for a pharmaceutical company. "I had an outgoing personality and was used to communicating with a variety of people. I also had knowledge of how the human body worked which relates to the medical field." The 'people skills' also came in handy for his later shift to the recruitment industry where he has interviewed thousands of candidates for jobs.

Self-awareness is critical, according to Rawlinson. "An important simple question that bamboozles many in job interviews is: 'What do you like doing?' It's amazing how many people can't answer."

For relatively instantaneous career 'pop', Rawlinson suggests "take on a big project and deliver on it successfully".

2 USE THE TALENT PIPELINE

Major employers have streams of smart individuals – popularly known as HIPOs (high potentials) – who not only are anointed for rapid progression through the corporate ranks, but also receive special opportunities. HIPO selection, therefore, can be a self-fulfilling prophesy.

The chosen ones have performed well across a range of roles rather than sat in one spot, tips Andrew Hagger, Group Executive, People Marketing Communication at NAB, where 600 of the Big Four bank's 28,000 Australian employees are currently in the Group Talent Pool.

These high achievers enjoy targeted development and support through mentoring from senior executives, networking, masterclasses and secondments, says Hagger. "Typically, they push up against the organisation driving their own acceleration. We want our people to be ambitious about their careers. Their hands are on the steering wheel."

It's not an elite tribe, he says. Everyone in the bank is offered development. Membership of the Group Talent Pool lasts only for 12 months. Besides, these days seniority is not necessarily a precursor for who gets ahead and whose voice is heard in one Australia's biggest financial institutions. The bank's recent high profile 'Break Up' ad campaign, launched initially on Twitter in 2011, had significant input from relatively new hirings whose expertise in social media far outstripped that of their bosses.

3 THINK LATERALLY

Career mobility and agility are vital attributes for fast-trackers. However, reinvention requires the right attitude and hard work. "It may be a grind, but it also brings great rewards," says Leo Grogan, career development manager of Melbourne Business School.

Grogan sees sometimes amazing transformations. From the current cohort of 100 students in the school's MBA program, he mentions a choir manager who has just finished an internship working on strategy for a major supermarket group and is now considering an offer to develop market penetration for an IT consulting firm, and a marketer of mobile phone devices who interned in a veterinary hospital and is about to join an international consulting firm.

"People look for shortcuts in a career change," Grogan says. But the 2012 version of offline networking – pulling on Lycra to cycle with the decision-makers – only goes so far.

In the 'discovery' ("What should I do?") phase of a career switch, some 'retooling' is required. An MBA course not only offers new skills and insights into different industries, but also delivers introductions to ambitious fellow students, influential alumni and major employers intent on cherry-picking the smartest.

For those who think an MBA is too much of a commitment, MBS now concentrates its fulltime program into 12 months as opposed to 16.

But, cautions Grogan, no higher education program guarantees success in a new industry or organisation. Speedsters in the career-change velodrome tend to be "futurists who communicate insights on new technologies, products and trends and have the ability to see over the horizon".

story snapshot

The up-and-coming company star knows how to identify a growth sector, hoard skills, target an internship, reverse mentor, blog to win and be an intrapreneur into the bargain.

4 CASH IN ON GROWTH SECTORS

Smooth operators set their sights on growth sectors. Phil Ruthven of international research house IBISWorld tips the services sector as a safe bet. Hot fields include eHealth, aged care and – boosted by the new carbon tax – environmental sustainability. Digital media marketing is also sizzling.

Instant gratification in dollar terms comes from the headline talent shortage fields, though. The average weekly wage in Australia's mining industry last year was more than $2018, with utilities – electricity, gas and water – a distant second with $1407, according to the IBISWorld Business Environment Report. Don't want to get your hands dirty? Delivering professional services to these industries also adds up, says Ruthven.

5 SPEAK UP

Surveys seeking information on greatest fears invariably come up with public speaking. Innate genius only goes so far when required to impress the executive team with a presentation or, perhaps, address a crowd of doubters about a company merger.

Thousands of businesspeople and professionals have learned to silence their fears with public speaking and presentation skills courses at the National Institute of Dramatic Art (NIDA) in Sydney. Core acting skills – vocal technique, physical presence and the ability to 'move' an audience – are also useful in business, according to Sean Hall, NIDA's corporate course manager.

Everyone has some natural ability for being calm and collected. Breathing – in particular the deep diaphragmatic kind – slows the heart rate and gives just that momentary pause that allows a nervous speaker to collect his or her thoughts, Hall says.

6 GET THE EXECUTIVE EDUCATION EDGE

"The post-GFC business world is more complex than ever. People think being busy is a good sign, but it may mean they're overwhelmed and not being effective," says Rosemary Howard, head of AGSM Executive Education. "Take time out. Get out of the workplace and get some new ideas!"

Short courses are one solution. The trend is for one-week programs with a residential component so people can immerse themselves in learning new approaches. The 'evergreen' pick at AGSM is the General Manager's Program where participants live in for five-and-a-half days to learn behavioural leadership – "to know themselves better and how to manage others".

The less-experienced can sign up for a Foundations of Management course, while those on the way to big boss status undertake the Advanced Leadership program (five days, plus three residential). All work on real-time projects for their organisations along the way.

The most time-constrained business people are often women who are juggling family commitments while trying to keep – or put – their careers on an upward trajectory. "While the number of women on boards is increasing, just 10 to 15 per cent of senior executives and less than three per cent of CEOs are women," says Howard. The Women in Leadership Program has been put in place to help women with gender-specific issues, such as unconscious bias and transitioning back to work or fast-tracking a career while also on the mummy track. The high-fliers at Chief Executive Women consider this so important, they're funding scholarships for talented women as they return to work after career breaks.

7 HOARD SKILLS

An emerging trend is the four-year career (the average time an American spends in a job). Human resource managers these days admit they're looking for growth on a CV rather than lineal progression.

One way of tackling this is to become a 'skills hoarder' by adopting a ceaseless, wide-ranging approach to learning new tricks. Lifelong learning is not a new concept, says AGSM's Executive Education chief Rosemary Howard, but there is a need for greater breadth today. "Knowing what's going on in different disciplines is very important. You want to be good at everything. The upside is that you can start anywhere."

8 THINK GLOBAL

Overseas' experience – exotic or high-flying – adds allure to CVs. Working for an organisation that offers the option is just one way to go. Big consulting firms – think McKinsey & Co or PricewaterhouseCoopers – satisfy an employee's wanderlust with offshore placements that are part of a continuous organisational diaspora. Postgraduates can apply for international exchange to study or conduct research. The Federal Government has funded collaboration between Australian and European universities on hot issues such as sustainable water management (www.icewarm.com.au).

Or, take the direct approach. Anna Shepherd, CEO of the Sydney-based home nursing service, Regal Health Services, says her business perspective shifted significantly after she enrolled in Harvard Business School's Owner/President program that brings together entrepreneurs from across the world for one month annually over three years.

TWITTER IMAGE: MR PICS / SHUTTERSTOCK.COM

9 INTERN

The best way to check out career possibilities without over-committing is through an internship. In Australia, most are available through organised corporate programs that take on students in the final years of tertiary programs.

Interning opportunities abound in fields such as engineering and accounting, says Dave Jenkins, one of the co-founders of Grad Connection, Australia's most frequently visited graduate site that provides links to positions in more than 140 companies. Be warned, though, so do those ready to leap into them.

Each July – the peak month for applications from soon-to-be graduates – about 100,000 hopefuls apply, Jenkins says. The good news is that in Australia all internships and summer placements offered through Grad Connection are paid positions.

So what happens to career switchers who want to try a new direction but are not studying? Insider advice from Jenkins is to apply directly to a prospective employer and think laterally. "Human resources departments tend to have strict rules about how they hire and they have plenty of choice." On the other hand, line managers in operational roles are constantly being asked to do more with less and may be delighted to share the ropes with a hardworking intern.

10 UNDERSTAND 'ME' MARKETING

There's a paradigm shift in marketing, says Natalie Lovett who has spent three years at its cutting edge as a client manager at Facebook Australia. She helps big brands such as the Commonwealth Bank, Pepsico, Diageo, Arnott's and Vodafone build their social media presences. But the marketing shift is not confined to the big end of town, it is made for personal brands, too, says Lovett, a guest lecturer in the School of Marketing at the University of NSW.

Recruiters are forever trawling for talent on social media sites – Facebook, LinkedIn, Twitter – but be warned that employers and their agencies also screen avidly via those digital spaces, Lovett advises, so keep online profiles presentable. How did she become a leader of the new marketing revolution? When she heard the world's most popular social media site was setting up in Australia, Lovett 'Facebooked' the company's vice president.

11 REVERSE MENTOR

Previously, the young sought business wisdom and advice from older colleagues, but increasingly now it's vice versa. Reverse mentoring is helpful for understanding what young customers think, from digital to behavioural. Canny business veterans have long been on to it. Just as the legendary Jack Welch – chairman of General Electric for 20 years from 1981– ordered his top 600 managers to reach down into the ranks to find internet junkies and become their students, today's big companies, such as IBM, actively promote communicating between ranks. On his blog, self-confessed 'noob' Mark Willson, the technology behemoth's director of marketing and communications, details how Jana Fielke, from the company's graduate program, guided him through his first tentative social media steps.

12 BECOME AN INTRAPRENEUR

Entrepreneurs start standalone enterprises, but 'intrapreneurs' stand out by starting new lines of business within organisations. Dan Godamunne is an example. He kicked off Fuji Xerox's eco-manufacturing initiative (and is now its general manager) after joining the tech company in 1993. Rather than churning out new products, Godamunne used his background in research and development to devise a way to remanufacture faulty components – an initiative that has proved highly profitable for the company. His impressively prescient sustainability focus is now part of a permanent exhibition at Sydney's Powerhouse Museum.

Other companies also value 'intrapreneurialism'. Vodafone employees can bid for innovation funds internally. Google gives employees a day a week to work on their own projects. The Commonwealth Bank runs IdeasBank, where bright sparks can float fresh concepts. IT company Atlassian offers employees the latitude to do their own thing at work via FedEx Days (24 hours in which developers can work on whatever they want) and 20% Time, which allows engineers to devote a fifth of their work to their own innovations. It's 'dedicated slack time' from which Atlassian bosses Mike Cannon-Brookes and Scott Farquhar hope employees' creativity will permeate their company's core products. So everyone's a winner.

13 VOLUNTEER

Pro bono work and volunteering is another way to acquire new skills or flex previously untested work muscles. Research by online professional network LinkedIn shows one out of every five hiring managers in Australia has employed a candidate because of their volunteer work experience. In the survey of 1000 Australian professionals, 77 per cent of respondents had volunteered, but only 46 per cent included the experience on their resumés.

14 MIND THE CULTURAL FIT

In the increasingly borderless world of business, 'global literacy' is in high demand, and cross-cultural trainers are proliferating. Culturally enlightened employees help things run smoothly in Australia's multicultural workplaces – and provide strategic advantage in transnational operations. What's more, they're nice folks to have around. "Cross-culturally trained people don't use stereotypes and are not judgmental – they're more tolerant and curious when they look at different behaviour because they seek to understand it better," says Dr Dan Caprar, a lecturer in cross-cultural management at the Australian School of Business.

With so much talk about 'the Asian century', zooming in for a regional fine focus makes sense. The University of Melbourne's nine-month Asialink program delivers cultural intelligence skills to more than 50 business and social leaders annually. Apply at www.asialink.unimelb.edu.au

15 BE A BLOG STAR

Spruiking expertise in a blog is a great idea, but remember the number-one blogosphere rule: don't be boring. The deadliest sin of bloggers is just talking about themselves, says Steven Lewis, who teaches Blogging for Business at Sydney Writers Centre. "Think about what people want to know rather than boasting about your achievements, and forget about rehashing news or other general information. Don't be afraid to have an opinion."

Many bloggers work on the principle: if I write it they will come, says Lewis. But the pressing question is: Will they return or be able to find that blog they casually encountered in a search last week? Clever bloggers capture email addresses and regularly update readers on new posts. Lewis practises what he teaches (blog.talist.com) and for online guidance about better blogging, recommends www.copyblogger.com

16 BE INFORMED

In the age of relentless 'ego casting', truly mind-boggling information sources are invaluable. By the end of 2012, one billion people are predicted to have experienced what Chris Anderson, founder of the TED phenomenon, calls "crowd-accelerated learning". TED began as a technology, education and design conference devoted to "ideas worth spreading" in the US in 1984, and is a regular hangout for Google founders Larry Page and Sergey Brin, Al Gore, etc. There's also hectic round of global events and salons, with local TED communities worldwide. Insights from TED are most accessible and affordable on the web (www.ted.com) where experts in their fields deliver 18-minute dissertations on everything from neuroscience to creativity.

17 WIN AN AWARD

Obviously, winning an award is a major profile-raising exercise. The sideline benefits that awards program entrants gain from participating are less blatant. Professional navel-gazing and the discipline of documenting and explaining achievements often astounds the judges and others – and the entrants themselves. Catherine Burn, Deputy Commissioner for Corporate Services in the NSW Police Force, who collected the top gong at last year's Telstra Business Women's Award says, apart from interesting introductions, winning the award has also boosted her self-confidence and made her more effective on the job. She's also hoping it encourages more women to take up policing.

18 LOSE THE ROUGH EDGES

Employers complain that even the best graduates emerge 'raw', minus basic social and people skills, such as how to dress for business, meeting behaviour, time management and understanding how to work in a team – "even how to shake hands and greet someone", says Sacha Koffman. That's why he set up Upskill (upskillonline.com.au) courses for his employer, talent2. Rough edges can be quickly smoothed, while other frequently missing skills – the fundamentals of spreadsheets, text documents, creating presentations and communicating electronically – can easily be added.

19 TAKE RISKS

Anyone who has never made a mistake has never tried anything new, said Einstein. Today's innovators can learn from other's mistakes from the comfort of home. A recent offering from the University of Adelaide is the online Master of Applied Innovation and Entrepreneurship which is drawing students from Australia and offshore with disparate interests. "Everything from food production to biofuels and apps," says course director Allan O'Connor.

Entrepreneurial spirit in the 21st century is boundless, according to O'Connor who says enrolments encompass start-up aspirants, those who may have already made a mistake or two and want to improve, people who just want to add some extra skills, and others who are funding or consulting to ventures. It's a course whose time seems to have come, as O'Connor notes a distinct trend towards independence among "millennials" keen to be "their own bosses rather than work for a firm".

Anyone who has never made a mistake has never tried anything new, said Einstein

20 NEED TO KNOW MORE?

Those who want to impress the board of directors – or anyone else – with knowledge on a specific topic might look to the teachings of former US hedge fund manager Sal Khan on YouTube. Khan – whose operation is now funded by Microsoft founder and philanthropist Bill Gates, and search giant Google – set up the not-for-profit initiative after posting a video explaining algebra for his niece in 2008. It's often easier to learn by video than traditional teaching methods, says Khan, who says the "pause" button proves handy. The MIT graduate, who also has a Harvard MBA, has developed a global following, creating 3200 videos and delivering more than 155 million lessons to date on topics from arbitraging futures contracts to the likely questions in a GMAT test – the entrance exam used for the world's top MBA programs – understanding yield curves and the pros and cons of debt vs. equity. Browse the Khan Academy's entire 'library' at www.khanacademy.org

• This article was first published in *Qantas: The Australian Way* in August 2012.

‘Always-on’ compliance: the value proposition for information governance

Why CEOs need records management and IT departments need a change of culture.

By **Rory Staunton**

A fundamental change of mindset is needed to address the needs of ever-demanding regulators in all government and commercial organisations. Every employee must ‘get ahead of the compliance curve’ by making compliance an everyday routine, ‘always-on’ part of the culture and infrastructure. This is the key to information governance which defines the set of integrated techniques, practices, policies, standards and systems that directs the purchase, design, implementation and usage of all information systems, so that they are ‘fit for purpose’ in meeting compliance regulations and at the lowest available cost. The systems and services that will emerge require organisations to assess the value and risk of their information from cradle to grave, not just when archiving. This requirement will massively increase the value of records managers that embrace the discipline needed to record boxes of paper and extend it to manage cloud systems that span every regulatory reporting requirement that CEOs need, to keep them out of prison.

OUT WITH 99% BOREDOM, 1% BLIND PANIC

At the old ICI chemical factory in Huddersfield there sits a one-legged stool in a glass case, in reception. It is a reminder of the industrial revolution when the safety of the factory relied on a worker whose job was to look at the temperature gauge on a pressure vessel. His role was to turn the steam heating down if it got too high, to avoid the pressure vessel exploding. If he fell asleep, he fell off the stool and woke up, and could continue to monitor the temperature. In the 19th century compliance with regulations relied on the stool to monitor the worker (who could not be relied upon to stay awake).

When Orville Wright started to fly his plane on 1911, his brother initially laid on top of the plane’s wing to control the moving wingtips. Many pioneer aviators died until the invention of flapper nozzle controller and hydraulic mechanisms that control the wingtips automatically.

These are early examples of the reality that we cannot rely on people to meet regulations, especially if the consequences of failure are life-threatening or business-critical. Automatic monitoring, controlling and reporting mechanisms are needed to detect breaches and correct them when a non-compliance event occurs. In the case of explosions in factories and plane crashes, prevention is obviously better than cure.

In information systems, most organisations are playing catch-up because they have experienced breaches of information compliance, illustrated daily by fines for Data Protection and Freedom of Information requirements, stemming from lost documents that cabinet ministers place in waste bins in public parks; laptops from the Ministry of Defence left in taxis; emails that reveal who knew what about LIBOR fixing; and mislaid pen drives full of personal account details lost by building societies.

Few IT systems in use today are designed to prevent such breaches, because the IT department that put them in did so with scant recognition of their fitness for regulatory compliance. A massive regulatory disaster recovery exercise is taking place in most IT departments, as they scramble to prevent hactivist threats, cyber-attacks, data loss, and identity theft from systems that should never have been acquired without them.

‘Big data’ is a term used by technology-pushing vendors to persuade naïve IT departments to spend even more money fixing a problem that they created – the purchase of so much IT that they do not even know what they have or where they have put it. They have little chance of meeting ever-increasing regulatory reporting requirements.

It will take a massive cultural change to persuade IT departments to think about compliance before they act, illustrated by the current fashion to implement cloud and SharePoint systems, without any requirement to include records management or information governance principles, and even less clear financial or operational justification. The vendors were able to exclude such functionality (because they do not know what regulations they must meet) and it helps them prevent substitution. IT departments let them do it. Such systems have strong cultural value but few can directly answer the question: “If it was your own money, would you spend it on that?”

Their silence is deafening…

WHY NOW: THE PERFECT STORM

In the film *The Perfect Storm*, small waves that are normally manageable combine in unusual circumstances to produce a massive wave which overwhelmed all the boats and harbours, and it takes George Clooney to save the day.

In today’s business and IT environments, we are faced with similar coincidences and convergence. Individually we can manage small disruptions. When they occur at once, they are overwhelming for most organisations, so a different approach is needed. The disruptions are:

story snapshot

A massive regulatory disaster recovery exercise is taking place in most IT departments.

It will take a huge cultural change to persuade IT departments to think about compliance before they act.

All organisations can build a successful information governance framework and get the regulators off their backs.

◆ **An un-forecast, deep, long-lasting recession.** Three months before the current recession started in 2008, the Head of the Bank of England was forecasting the opposite (and he is still in a job…!). The recession in the early eighties lasted two years. Here we are in 2012 with no end in sight…

◆ **New technologies.** The availability of high bandwidth internet everywhere, cloud computing and mobile phones with more powerful processors than desktop computers – and which are a lot easier to use – have all disrupted IT departments. There is a gulf between consumers that want Apps like the ones on their iPhones, and corporate IT that looks stupid, is difficult to use unless you are a geek or an expert, and threatens the careers of most IT staff. New technology has already emasculated Microsoft's brand, and escalated the value of Apple and Google, to ridiculous 'bubble' levels. There is no going back…

◆ **Globalisation and price-cutting competitors.** Manufacturing companies in Europe have struggled to survive when faced with China and other BRIC countries whose workers are paid a fraction of our wages and can ignore environmental concerns, freedom of speech and labour laws with impunity. Containerisation of shipping means that cheap cloned products can be in a European market faster than Primark can copy the dresses on the Milan catwalks.

◆ **Ever-increasing regulations.** We all want to be on both sides of every argument. On one hand: if the local council, some anonymous non-elected Government agency, the RSPCA and the Scottish Parliament do not get you, do not worry. Some EU bureaucrat will. Yes, they are coming to get you…

On the other hand, ask the owners of any small business whether regulations help or hinder. Ask GlaxoSmithKline how their shareholders responded to the latest $3-billion fine from the FDA for mis-selling drugs. This now may prevent more research on cancer, Alzheimer's and diabetes. Then ask patients whether they value this ethical company that has prevented more stomach ulcers, breast cancer and heart attacks than anyone else...

There are two sides to every regulatory argument and some people do not like jokes. The challenge records managers face is to get the balance right for the information in their own organisations. Let us try a few tests to see how far you have got….

CHARITY BEGINS AT HOME

To show the scope and depth of the challenge in making all your information systems fit for compliance (ie, part of an up-to-date information governance framework) try these little trifles. (Answers at www.strategy-partners.com)

- What is the difference between backup and archiving?
- How much does a file plan cost?
- What emails from the human resources department and accounts department should the IT department delete? Who set the policy?
- How can you prevent users of their own tablets and phones from capturing files and relocating information from corporate systems?
- What happens to the integrity of documents that were originally generated in old Microsoft office formats (.rft, .doc) when they are viewed in current versions of Microsoft Office that use .docx.? Or is it .docy or .docz?
- How do you know that documents viewed as .pdf are accurate and future-proofed by the ISO PDF/A standard, and not corrupted by a cheap and nasty 'free' PDF converter?
- How do you know if a document printed from a mobile phone is rendered accurately?
- How can you ensure that a record created and stored in an SAP system can be managed, without it leaving the SAP system?
- How do you transfer all the documents in the shared drive into SharePoint, whilst completing the appropriate metadata and without losing any information on the way? At low cost? In hours, not months?
- How do you extract records that are created in a SharePoint system into a non-Microsoft application, and ensure they are kept up to date?
- What percentage of space occupied by data and documents on most disk storage systems is either duplicated or redundant?
- When someone leaves the company, what happens to the information on their own/ home PC?
- How do local authorities hold a single view and record of citizens across their housing, benefits, planning, environmental, parking education and social care systems which were never designed to be integrated? The three largest IT vendors have made damn sure over the past ten years that they cannot be easily substituted.

- How do retail financial groups hold a single view of their customers' personal details across their current account, savings, pension, credit card, life insurance and mortgage systems that were designed in different acquired companies and contain records never designed to be federated or integrated?
- How do life insurance companies maintain the integrity of records when their IT platforms change every five years? Actuaries expect today's children to live to 115 – that is about 21 changes! Of course, the IT department never loses data when they transfer to new systems…
- How do life insurance companies answer questions about their records under the new Solvency II regulations put in place by the Financial Services Authority on behalf of the European Union insurance industry regulator, when they keep changing what Solvency II requires, and when it has to be complied with?
- How much is a pint of milk?

BUILDING AN INFORMATION GOVERNANCE VISION

Having identified the problems, all organisations can build a successful information governance framework, lower costs and get the regulators off their backs, if they firstly adopt a realistic approach. They need to:

- Articulate what successful information governance looks like (see www.dlmforum.eu)

Develop realistic tests for telling what are and what are not mere fads

- Recognise that records managers possess the skills all organisations need to value information when it is created, not just in the archives (as the ones who bayonet the wounded after the IT battle is over…)
- Stop spending limited resources on fashionable IT. Develop realistic tests for telling what are and what are not mere fads.
- 'Get ahead of the compliance curve' by only purchasing IT that can be easily substituted and has been designed to be 'fit for purpose' when it comes to meeting regulatory requirements. Elegant branded IT architectures are a luxury, but regulators are real.
- Start saying: "You cannot buy any more proprietary silo IT software components until you can show how it will help us meet our increasing regulatory requirements at a lower cost and without a nine-month IT project."
- Start evaluating how many email, website, business intelligence and document management systems you can throw away or switch off. For example, most UK local authorities have seven different document management/content management/website/EDRMS systems on 'evergreen' maintenance contracts.

ABOUT THE AUTHOR

Rory Staunton heads Strategy Partners' research team of content management market specialists. He has provided extensive IT advisory services to major organisations in the governmental, pharmaceutical, finance and utility sectors.

Strategy Partners – www.strategy-partners.com
Tel: +44 845 0941570 ✉ info@strategy-partners.com

- Get help from independent sources that can show you how to overcome vendor hype and help you sort out the essential from the fashionable. Beware consultants bearing gifts, especially those whose projects are marked with fiascos and who cyber-squat on regulators' website URLs.

AS A FAMOUS GENERAL ONCE SAID…

"When I hear people speak of culture, I reach for my revolver".

When you hear the regulator coming, reach for your information governance framework, and show how you can meet their requirements at the lowest possible cost without disrupting your organisation.

When you hear the IT department propose more useless IT systems and reject your proposals for next-generation records management as a foundation stone for information governance, you know what to do… ❖

Records managers confessional

Strategy Partners is currently documenting examples of major success and major failures in records management. If you have any stories of an accidental (or misguided) breach or problem please contact us on info@strategy-partners.com. We guarantee that any contributions will be suitably anonymised and redacted.

COULD YOU BRING YOUR COMPANY TO ITS KNEES?

There's a saying 'do as I say, not as I do' which seems to resonate in the executive corridor of far too many organisations. In this cautionary tale, we use the saying to create a fictitious scenario. This is created to illustrate just how dangerous double standards can be. Our unfortunate protagonist is the managing director, who believes the rules don't apply to them.

By **Dominic Saunders**

The headlines said it all, Tom Smith's company was splashed across the news and he knew someone in his company was in trouble. As a call centre it wasn't just his own database that was now hanging out to virtually dry, but also those of his 400+ clients, which contained some very personal information. He wasted no time, someone was to blame, and the root of the problem had to be dug up. Tom contacted his Chief Information Security Officer, Rob Banks. The instruction was simple, find the source of the leak, plug it and whoever was responsible was out.

Rob wasted no time in trying to find who was to blame; Tom was more than happy for him to do so. Of course, being interviewed by Rob was weird, but his thoroughness demonstrated that he was taking the situation seriously. As they sat down, Tom reassured Rob that he should treat him as he would 'any other suspect' and forget their respective positions within the organisation.

So Rob did.

Rob's first question caught Tom a little off guard. Yes, he'd seen, read and understood the policies and procedures surrounding information governance. In fact, he'd been instrumental in helping Rob write them!

Moving quickly on to security policy and Tom began to feel like a suspect. He confessed he hadn't changed his password recently even when the message flashed up prompting him to do so. Making up new complex passwords is not best done under pressure. Yes, in an ideal world, he would change it every four weeks but in reality who was actually doing that? The fact that everyone Rob had spoken to so far said they knew the rules, didn't mean they actually were following them. And his comment that Tom was in violation of the security policy, was just churlish.

story snapshot

Even if an organisation is doing all the right things, if the people within it aren't, then it's all for nothing.

IT departments should be able to count on senior management to lead by example.

Organisations need to take an enterprise approach to IT security awareness programs.

Rob asked Tom if he was aware of the protective technologies the organisation had deployed to provide a formidable security blanket. Aware of them, Tom had had to sit through endless presentations with Rob from various vendors touting them. The social engineering test that the penetration team had conducted was infamous with the stunts they'd pulled. Tom was quick to remind Rob that every highlighted area had been addressed, with no expense spared.

Tom's encryption habits were the next element Rob scrutinized. Tom had to admit he hadn't upgraded the program on his PC yet as he was worried about compatibility problems opening older files. He'd started to do it, but he'd been under pressure and it was taking so long, so he'd had to abort it – it didn't mean he wouldn't. When he confessed he'd 'switched off' encryption on his laptop Rob became really agitated. In Tom's defence, it had slowed down performance, admittedly not by a huge amount, and Rob had to realise that every second counts. Yes, Tom agreed, he knew this violated the security policy.

Rob's interrogation continued, this time asking how many other devices Tom used during the day. A little more bullish, Tom pulled out his corporate-owned smartphone that he used for emails. Rob asked if there were any 'personal' devices Tom owned and, rather proudly, Tom pulled his shiny new iPhone 5 and laid it rather tenderly on the table. He didn't use it for business so it was okay he'd not told anyone. Rob snatched it up and his horrified expression said it all as he accessed Tom's personal hotmail account and started looking at the various messages, complete with attachments, Tom had forwarded to himself. "It's got a better screen to see the graphs and charts on" sounded a little hollow to even his own ears and Tom knew what was coming next. It was a clear violation of the security policy.

In for a penny, in for a pound, Tom decided to come clean about his iPad. He'd wanted to work on the train and the laptop was just so cumbersome to haul backwards and forwards so this was far more convenient. He'd transferred some documents to work on – the payroll, some R&D reports, a few tenders, and of course the latest board minutes. He'd never dream of moving a whole database to it! Rob then showed him how he could access the corporate SharePoint site and its Aladdin's cave of information. If only Tom had known, he could have been so much more productive. Rob did warn that this too was a violation of the security policy.

Rob moved on to examine Tom's laptop computer and it didn't take long to identify the malware skulking in its operating system, spewing passwords and login credentials across the ether. Rob had identified where the leak was and could plug it. The question was, did Tom still want the person responsible out?

So, what does this scenario demonstrate? Even if an organisation is doing all the right things, if the people within it aren't, then it's all for nothing. It would seem that although security and governance issues are increasingly being discussed at board level, the perception remains that senior personnel believe that IT security policies and procedures apply to the general workforce, but they don't necessarily practice what they preach.

When data loss has become a daily news headline and regulators are hitting hard on organizations with lax attitudes towards data security, IT departments should be able to count on their board members and senior management teams to lead by example.

To prevent falling into the same trap organisations need to take an enterprise approach to IT security awareness programs and take the following steps:

- Introduce policies and procedures that keep the organisation safe.
- Write them clearly so everyone can understand them.
- Think carefully when signing off policies and procedures about whether the measures outlined are workable in daily practice. People will always find ways around rules that prevent them from doing their jobs effectively.
- Improve IT security education, so that every single person not only knows what they should be doing, but also why they're doing it and the consequences of not following them.
- Differentiate IT security awareness programs, so people don't get bogged down with policies and procedures that don't apply to them. People are far more likely to remember and adhere to security rules that are applicable and relate to their job function.
- Regularly update policies and make sure everyone knows when this has happened.
- Important security practices and technologies should be enforced without the option to be overridden.
- Disciplinary action should be applied consistently across the organisation when an infringement occurs. ❖

ABOUT THE AUTHOR

Dominic Saunders is Senior Vice President of the NETconsent business unit at Cryptzone.

✉ He can be contacted at info@cryptzone.com

Are these the **world's tallest** information managers?

It may sound like an old-fashioned shaggy dog story, but this is true. There was a very tall American, Australian and Dutchman and they went to the Brisbane congress of the International Council on Archives in August.

By **Mike Steemson**

They all have scars where they've argued with doorjambs and rafters… violently. For sure, they are among the tallest information managers in the world, perhaps the tallest. Looking down on us lesser mortals as they do, they are also cheerful, happy-go-lucky types. Look at those sky-wide grins.

So now, in loft order, meet Earl Cahill, Hans Hofman and Greg O'Shea. Next conundrum: guess which national is which. A clue: one of the surnames is not Irish.

Quite right! It's Nederlander Hans (actually Johannes, but don't tell him we told you) Hofman, 64 (left). He is a high-profile information management Euro-guru sought worldwide for his archival and records management expertise,

Collectively, this high-altitude trio reaches just under six metres or almost 20 feet; higher than a double-decker bus, or two house storeys

Left to right Hans Hofman, Earl Cahill and Greg O'Shea caption to go here please caption to go here please

especially on digital preservation. One of the original ISO15489 standard authors, he has worked for the National Archives of the Netherlands (Nationaal Archief) for 40 years, broken briefly by a two-year stint at the Dutch Ministry of the Interior.

Hans lives in a little eastern *dorp*, Ellecom, near the 'bridge too far' city of Arnhem. He runs out at 197cm tall, a shade under six feet six inches, not ideal for the 20 years he was also honorary archivist for the 13th century castle, Huis Bergh, also near Arnhem, where the stucco ceilings, chandeliers and inglenook fireplaces were a constant threat to his cranium.

THE TALLEST AMERICAN

Tallest by a couple of inches (and youngest) is the American with one of those Irish names. Earl Cahill, 41 (centre) is 6ft 8in high, just a tad over two metres, three centimetres. He started business life as an IT geek, but saw the light and now manages information on the host website of the genealogy firm L.D.S. – Family Search, a department of the Church of Jesus Christ of the Latter Day Saints based in Orem, Utah, a community that likes to call itself 'Family City USA'.

He's been with the company for five years and was helping man the company's display booth in the ICA Congress exhibition hall, literally head and shoulder above his colleagues. He lives in Pleasant Grove, Utah's 'City of Trees', a community of some 30,000 in the north of the state, 100 kilometres or so below Salt Lake City.

The other Gaelic name among the three belongs to Australian Greg O'Shea, 56, (right) who tops 194.5 centimetres, that's six feet four and a-half inches in the 'old money'. His career began in 1977 with one of Australia's earliest IM qualifications, a Diploma of Archives Administration at the University of New South Wales in Sydney and, a year later, a job with National Archives of Australia (NAA).

In the 1990s Greg became an early e-records policy advocate and represented NAA on the committee that developed the world-leading Australian Records Management standard, AS4539. He's covered big chunks of the Australian public sector: National Archives, Communications, IT and the Arts, Foreign Affairs and Trade, and Finance. Since 2007, he's headed the independent IM and RM consultancy, Valhalla Enterprises while also honing his beach-combing skills at Valla Beach, NSW.

Collectively, this high-altitude trio reaches just under six metres or almost 20 feet; higher than a double-decker bus, or two house storeys. Anyone beat them, height-wise? ❖

ABOUT THE AUTHOR

Former London newspaperman Michael Steemson, ARMA, is the principal of the Calderson Consultancy in Wellington New Zealand and a member of the editorial committee of *iQ*.

✉ He can be contacted at mike.steemson@xtra.co.nz

Tweets, check-ins and status updates: keeping track of social media at Victoria University

Use of social media by companies, universities and government has increased dramatically in the last few years. Victoria University (VU) in Melbourne, Australia, was aware that many activities were being undertaken on social media – but it wasn't known what channels were being used, for what purpose or by who. This article describes some of the activities undertaken at VU to keep track of its social media, including finding out what was out there, creating a governance framework for social media, and dealing with the records of social media.

By **Kirsten Wright** and **Kathryn Crawford**

Social media at Victoria University is used as a tool to help communicate with the many diverse communities that exist within its more traditional networks. It is used widely by both staff and students, who have differing levels of engagement, experience and expectation around the use of social media.

WHAT IS SOCIAL MEDIA?

The term social media covers a broad and varied range of online sites. Online communities exist and interact across a number of (almost immeasurable) platforms – wikis, live-casting, social bookmarks, crowd-sourced content, blogs, Twitter eco-systems, forums and chat-rooms, curated networks and geocaching … and the list goes on.

For the purpose of this article, social media refers to the 'official' channels used by the University to communicate with its stakeholder groups. A list of those appear later in the article.

There are many uses of social media at VU. It is used to market to future and current students, and to engage with past and current students. It is used collaboratively, by staff, to foster information sharing not only with other staff members, but with industry and business partners outside of the University. Academics use social media as a learning and teaching tool, and it can, in some cases, be an effective tool to monitor student welfare (and intervene if necessary).

There are also more intangible reasons for using social media.

- It has significant **reach** – to facilitate a global exchange of University ideas, dialogue and communications.
- It is **interactive** – it attracts and engages audiences using two way communication channels.
- Its **flexibility** is critical – it utilises a set of tools that can be harnessed to suit a wide range of purposes and audiences.
- Social media can drive **leadership** – positioning the university as an **innovative** leader, and it enhances the student experience by improving the 'on-campus' **social** experience, as well as providing support networks & information.
- It's **efficient**, improving the speed by which information can be distributed.
- It also encourages **networking**, which in turn can reduce the need to respond individually, or allows others to respond – creating healthy engaged online communities.
- Social media is also a relatively **inexpensive** alternative to traditional means of communication, info sharing and promotion.

story snapshot

The number of social media sites maintained by VU staff has grown exponentially.

This has necessitated a need for greater governance and control of VU's social media outputs.

VU developed a social media register and examined the records management needs and considerations around capturing social media outputs.

WHAT CHANNELS DOES VU USE?

The social media landscape – it's big. In 2011 a University-wide survey on social media use at VU was conducted. The survey was done as part of a general staff leadership development program project, with the target audience being VU staff. The aim was to understand existing applications of social media within VU. The results were used by the Web Intranet Social Media Advisory Group (WISMAG) to provide guidelines to improve the user experience of social media, and to help build a governance framework for social media at VU. The results were interesting – if not a little terrifying. The audit results showed the following:

- Facebook – over 70 groups and pages
- Twitter – over 20 accounts
- YouTube – over 10 channels
- Foursquare – campus 'mayors' were all current students who did not broadcast VU-focused content

WHAT ABOUT GOVERNANCE OF SOCIAL MEDIA?

At VU, the Web Intranet Social Media Advisory Group (WISMAG) had overall 'governance' of social media. However, it wasn't until 2010 that the University recognised it needed to address some the issues around the social media use in a more formalised way.

In 2010, draft guidelines for use of social media were developed. These guidelines were developed by a web and communications coordinator, who had carriage of a large portion of the responsibility for the official (more visible and accessible) social media aspects the University participated in. Those guidelines were developed in consultation with other committees and working groups across the University, including marketing professionals, academics, e-Learning groups and student representatives.

In 2011, the Social Media Working Group (SMWG) was established to provide opportunities for a network of interested parties to meet monthly to share experiences, co-ordinate activity and monitor social media at VU and report back to WISMAG. Its members included representatives from marketing, student life, current student communications, VU International, counselling, records management, and academics who used social media in their teaching or research.

The SMWG activity included finalising and publishing the guidelines, collaboration on projects, sharing knowledge, and discussing best/worst practice from around the globe with individuals from various departments. The group had a good base to work from – WISMAG were already talking about how to handle social media, and the SMWG also made our regular communications a lot easier and more structured.

A SOCIAL MEDIA REGISTER

The final deliverable of the social media project was to devise a social media register, and a set of criteria for staff wishing to create a new channel. This record of social media channels created by staff across the University encouraged staff to think strategically about their choice and use of the channel. Questions such as "How many people are you looking to attract?", "Will you moderate it and how?" and "How will you keep records of your activity?" were part of the registry process, which also served as a subtle education process around social media etiquette.

Chaos versus control

Through the survey results, the SMWG identified some key findings from the project about social media. It can't be controlled, and it can't be ignored. There will always be cross-over between personal and professional boundaries, and as an institution, we rely on people being 'decent'.

In general, it was accepted that both staff and students from around the University will set up groups regardless of the existing groups which may be serving exactly the same purpose – so the social media register became a way to help monitor and evaluate some of the online activity. It was also useful in understanding the volume of activity that might be happening from a recordkeeping point of view.

RECORDKEEPING CONSIDERATIONS: WHAT TO CAPTURE

It was clear from the audit of social media that there was a variety of interactions occurring on VU's social media platforms. From a recordkeeping point of view, it was highly likely that records were being created over the various channels.

A risk-based approach was adopted and an assessment on the content and type of social media interactions was undertaken. This looked at the types of issues being discussed on the various social media channels, what information VU was broadcasting, and how complaints or moderation issues were dealt with. We determined that the social media interactions mainly fell into customer enquiry or marketing records. Due to existing staff guidelines about social media use, little to no personal information was being exchanged on VU's social media channels. Enquirers were referred to the relevant department if they needed to share personal information. We therefore determined that the risk associated with both the type and content of the social media interactions was low.

Next, we turned to assessing the records themselves. By reading the various guidelines available about records management and social media[1]; and through discussions in the Victorian Higher Education Records Management and Archives Group (VHERMAG), a simple decision tree was developed to determine if the records needed to be kept:

- Are the records unique?
- Do the records provide evidence of business?
- Is there an ongoing need to retain the records?
- What constitutes the records as a whole?

It should be noted that these questions are hardly unique to social media; instead, it was more a matter of applying recordkeeping principles to social media. Answering these questions meant some interesting issues were raised which helped clarify our position about what needed to be captured.

First, it was apparent that social media records did not exist in isolation. Their relationship with other University information and records, for example, the VU website or student grievance records, became evident.

Second, it became clear that the value in VU's social media presence was in its interactions with current and prospective students and staff, and members of the public. Therefore, capturing comments and replies was necessary.

In addition, what made up the 'social media record' was not just the social media itself. There were also various policies, procedures and guidelines which provided the overall framework for using social media at VU. Therefore, to see the full context of social media use at VU, these records also needed to be captured.

…it was the interactions, comments and replies which made the social media records worth capturing

Using the checklist, we determined that both the primary VU Twitter account and Facebook page should be captured. We then considered methods of capture.

Criteria for capture

In order to best judge which product or process to use when capturing records of social media, we came up with a list of criteria against which we could assess various products or services available. Our criteria were as follows:

- **Automated capture:** The volume of material on both Twitter and Facebook meant that manually capturing would be very time consuming for the staff involved, particularly for staff who answered enquiries on evenings and weekends. Additionally, automatic capture better preserved the context in which the interaction occurred, rather than presenting each message in isolation.
- **Multiple searches and accounts captured:** While we were concentrating on capturing the material from the primary VU accounts, the audit and register showed us that there were many other VU-related accounts on social media. We wanted to have the ability to add these to the capture process in the future.
- **Replies captured and conversation threads maintained:** As noted above, it was the interactions, comments and replies which made the social media records worth capturing. Therefore, it was essential that that these were captured along with the original message.
- **Output in known format(s):** While there were various programs and services available, many of these used proprietary formats. For both general control, and long-term preservation reasons, we wanted to use open, known formats.
- **Basic metadata captured:** As well as the content of the message, we also wanted the metadata to be captured. This included date and time of message, account name(s) involved in the interaction, if it was in response to another message and any audit information available from the site.
- **Able to run on VU systems/servers:** We preferred it if the program or system capturing these records could run on our own infrastructure, allowing us better control.

The way Twitter was developed, as well as its terms of use, meant that it was much more accessible and easier to capture than Facebook. We therefore concentrated on assessing products for capturing tweets.

Capturing tweets

We quickly determined that there were a number of products available to capture tweets[2]. We determined that Your Twapperkeeper, an open source version of the formerly popular Twapperkeeper[3], suited our needs best. This ran on our own servers and allowed the capturing of any Twitter search including text searches, accounts and hashtags. Basic metadata was also captured. With some minor modifications, we could export the tweet stream in a variety of formats[4].

After setting up the program on our server, it was simply a matter of setting up the various search terms and watching the tweets get captured. Exporting the data meant we could not only create 'snapshots' of tweets which could then be imported into our EDRMS, but also that we had an interesting set of data to analyse.

Using the information

While our primary purpose in capturing the VU tweets was one of compliance, it also meant we had an interesting data set that various parts of the University (such as the Marketing Department) could analyse for trends and sentiments. This was useful in analysing the impact of key University events, such as Open Day. Examples of the types of analysis performed included tweets over time; word or sentiment analysis; and how much content from the VU Twitter account was retweeted or rebroadcast across Twitter.

Providing the data to be analysed helped the SMWG see the value in capturing tweets outside of meeting risk and compliance requirements.

OTHER RECORDKEEPING ISSUES

While VU's Twitter records are currently being captured, there are still many other issues to consider regarding social media and recordkeeping.

- **Appraisal:** As VU's social media presences create records which fall across multiple business functions and activities within the same outputs, appraisal is not a simple task. Separating the individual records out into their specific retention classes would be not only time consuming, but would also remove much of the context with which the records were originally captured.
- **Moderation:** Moderating social media channels may result in records being deleted. There is an ongoing issue with how best records of moderation should be captured, so that the full context of the moderation can be maintained. It is currently a manual process.
- **Other channels:** While Twitter is relatively straightforward to capture, other social media channels are not. This becomes even more important when social media is used for teaching and learning purposes, and more critical records are kept on social media.

ABOUT THE AUTHORS

Kirsten Wright is the University Archivist at Victoria University, Melbourne. Prior to this, she worked at the Public Record Office Victoria.
✉ She can be contacted at kirsten.wright@vu.edu.au

Kathryn Crawford works in Public Affairs at Victoria University, Melbourne.
✉ She can be contacted at kathryn.crawford@vu.edu.au

- **Change is quick:** The social media world moves swiftly – and Terms and Conditions change frequently. This means that capturing records of social media can never be considered a 'one-off' process; instead, methods of capture change as sites and conditions shift.

CONCLUSION

While we can certainly not claim to have sorted out all of VU's social media presences, we are now at least aware of what they are, who is administering them, and what the purpose of the channel is. In addition, the Register allows us to better monitor and track existing social media presences and make staff aware of existing sites.

The acknowledgement that records were being created on our social media sites led us to consider what was important to capture. This risk-based approach allowed us to prioritise the capture of the various social media channels and meant we had a greater understanding of not only the records being created on social media, but also the way these records interacted with other records.

Finally, the development of criteria used to assess the various social media capture products will certainly be used in the future with other social media channels. While it is probably impossible to capture all the records of social media that we would wish to, we now have an overall framework for determining if there are records to capture, mitigating the risks for the records we cannot capture, and feeding back the entire process into the overall governance of social media at VU.

Note: Since the initial work done on capturing tweets at VU, the Twitter Terms of Service have changed. It is now possible that this method of capturing tweets is against the latest Terms of Service. In addition, as this article was being prepared, the CEO of Twitter, Dick Costolo, announced that Twitter users will be able to "download a full archive of tweets" by the end of 2012. What form this will take, or what will be able to be downloaded, is not clear at this stage. ❖

• This article is based on a presentation delivered at inForum Melbourne on 28 August 2012.

Bibliography

1 See for example, Ferriero, D (2010). *Guidance on Managing Records in Web 2.0/Social Media Platforms*, http://archives.gov/records-mgmt/bulletins/2011/2011-02.html; State Records NSW (2009) *Guideline 24 – Records management and Web 2.0*, https://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/guidelines/guideline-24 ; and the recently released Public Record Office Victoria (2012) *Recordkeeping Policy: Social Media*, http://prov.vic.gov.au/government/standards-and-policy/policies/social-media

2 Katharine Stevenson discussed a different product used to capture tweets in the recent *IQ* article, Stevenson, K (2012), *Managing 'tweets' as records*, *IQ*, Vol 29, Issue 3, August 2012, pp 24-27.

3 Twapperkeeper was a popular method of capturing tweets. It was bought out by Hootsuite in January 2012 and its functionality is now part of the Hootsuite product range.

4 Bruns, A (2011), *Switching from Twapperkeeper to Your Twapperkeeper*, http://mappingonlinepublics.net/2011/06/21/switching-from-twapperkeeper-to-yourtwapperkeeper/

inForum 2013: Information Governance

8-11 September 2013
National Convention Centre, Canberra

Parliament House

2013 marks a milestone in Australia's history. It is Canberra's centenary and RIM Professionals Australasia is excited to be hosting inForum in Canberra in its centenary year, giving delegates the opportunity to part of not only the celebrations of a historical moment for Australia but also in the incredible number of unique activities and celebrations being held as a result.

With the call for papers closing on 1 February 2013 the program planning is well underway and the full program will be released online in mid-March, in the meantime here is a sneak peek of the inForum 2013 program:

SPEAKERS

With fond memories of inForum 2011 in Darwin, Australia's Information Commissioner John McMillan has agreed to open inForum and provide the opening keynote presentation, this time on his home turf.

Another keynote speaker is Rory Staunton from Strategy Partners, UK, the author of 'Always-on compliance: the value proposition for information governance', which appears in this issue of *IQ* (page 28). Rory will also be providing an Information Governance workshop.

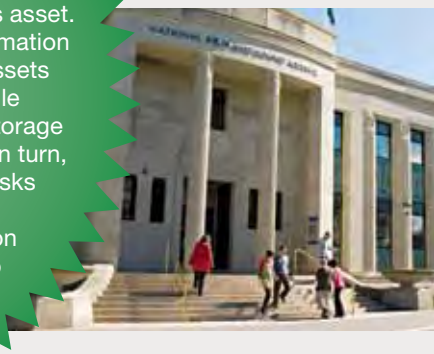
An article featuring other confirmed inForum speakers will appear in May *IQ*.

SITE VISITS

Canberra is home to many of Australia's information institutions and a number of them have generously agreed to provide us with onsite presentations of 30-40 minutes followed by a behind-the-scenes tour and a viewing of their current exhibition as part of the inForum program. The institutions involved are:

- National Film and Sound Archive
- National Library of Australia
- National Museum of Australia
- National Gallery of Australia
- National Archives of Australia
- Australian War Memorial

Information governance is a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset. The goal of a holistic approach to information governance is to make information assets available to those who need it, while streamlining management, reducing storage costs and ensuring compliance. This, in turn, allows the company to reduce the risks associated with unmanaged or inconsistently managed information and be more agile in response to a changing marketplace.



WORKSHOPS AND VENDOR PRESENTATIONS

Five workshops will be held covering topics such as building and sustaining governance frameworks, performance management fundamentals, managing information in organisations and addressing information sustainability and vulnerability, with others to be confirmed.

A breakfast workshop will be held on Wednesday morning on Coaching and Mentoring skills.

There will also be six 40-minute presentations by vendors on RIM relevant topics including representatives from iCognition, RSD, Recordpoint, Open Text and Recall.

FROM TOP: AUSTRALIAN CAPITAL TOURISM; TOURISM AUSTRALIA; NATIONAL FILM AND SOUND ARCHIVE


National Gallery of Australia


National Museum of Australia


Australian War Memorial


National Film and Sound Archive


National Library of Australia

SOCIAL EVENTS AND NETWORKING OPPORTUNITIES

Like any good conference inForum will also offer many networking opportunities.

In addition to the opportunity to network over tea breaks and lunch each day there is also the traditional Welcome Reception on Sunday evening, RIM Professionals Australasia's Gala Awards Dinner held on Monday night, with this year's theme being 'A Garden Party' honouring Canberra's famous Floriade festival and a Listserv Users networking function on Tuesday evening. Separate to the conference but a mainstay in the program anyway are the Branch Dinners which are also hosted on Tuesday evening.


Floriade

TRADE EXHIBITION

inForum 2013 will feature a trade exhibition of products and services that are completely relevant to the RIM industry. With 50 stands to view every delegate will come away with new contacts and information, guaranteed. ❖

Sponsors:

Platinum sponsor ezescan. transforming paper into knowledge

Gold sponsor recall™ Your Information. Securely Managed.

Silver sponsors FUJITSU Avision

CONTACTS

- For more information on exhibition and sponsorship opportunities please contact Wendy Morris **wendy.morris@rimpa.com.au**
- Any other enquiries can be directed to Kristen Keley **kristen.keley@rimpa.com.au**
- For general information about Canberra, the venue, the program or to register, visit the conference website: **www.inforum.net.au**

FROM TOP: TOURISM AUSTRALIA; AUSTRALIAN CAPITAL TOURISM; TOURISM AUSTRALIA; NLA

The case for *aggregated information management roles*

This article explores the changing roles and functions of information management professionals and information technology professionals, and their associated convergence – or, at the very least, collaboration. It also explores a number of other questions (see 'Story snapshot' right).

By **Joy Siller**

During the course of its operations, an organisation creates and receives information that pertains to its business activities. The organisation must manage physical and technical infrastructure to support its information as well as managing the information content itself. The organisation will be required to create and keep certain information for legal and operational accountability, decision-making and historical reasons.

There are undoubtedly challenges in the way organisations manage their information. Adding to these challenges are the vagaries as to what constitutes organisational information (is it data, documents, records, archives, content, knowledge?) and who is responsible for managing it. The responsibility is fragmented in many organisations, and such fragmentation can lead to mixed messages, competing resources, professional jealousies and organisational inefficiencies.

A recent American study into executives' views on their organisations' information management functions and roles found that one particular executive saw "IT as the plumbers – hooking up the pipes – and IM as the architects – doing the design work, being the key custodians of information, creating the overall picture, and eliminating fragmentation of information." Another saw information managers as responsible for the "repository of the organisation's knowledge and resources" with a secondary responsibility to "be consultants to facilitate transfer of that knowledge".[1]

The changing roles and functions of information management professionals and information technology professionals, and their associated convergence or, at the very least, their collaboration have been highlighted recently in a number of papers. This article builds on that theme and raises other issues.

ORGANISATIONAL INFORMATION

Let's start with some definitions of the key concepts here – information, organisational information assets and information management.

Engelsman provides the following definitions for *information:*

- data presented in a form that is meaningful to the recipient
- data processed for a purpose (of making us aware)[2]

Middleton (and others) positions information in a continuum between data and knowledge:[3]

Data → Information → Knowledge

So, put simply, information could be described as processed data that makes us aware of something. Organisational information, and its transformation into knowledge, could be said to keep an organisation aware and create an intelligent organisation.[4]

Accordingly, it is proposed that the concepts of enterprise content, records, documents, and archives should be considered within the realm of information management, rather than as separate (albeit related) entities. This issue is discussed in greater detail below.

INFORMATION RESOURCES OR INFORMATION ASSETS? OR BOTH?

There is some discussion in the literature as to whether information is an organisational resource or asset or both. For example:

- *Information is a core resource and asset of modern public sector organisations, together with people and finance.*[5]

story snapshot

The author puts the case for aggregated information management roles, and explores the following questions:

– What is organisational information and information management?

– Is information being treated as a business asset and managed accordingly by appropriately skilled professionals? Is the employment of separately skilled professionals a viable option for organisations facing tough economic times?

– Where do the skill sets of the various information professions currently fit within organisations?

– Are there likely to be winners and losers if information management roles are aggregated? Where is the current organisational power with respect to such roles and what is the basis for this situation?

– Are there sufficient differences in the professions to facilitate the ongoing survival of a multitude of bodies representing them? Does the existence of a variety of professional information associations actually promote harmony or discordance?

– Should education institutions focus their information management curricula on the production of graduates who are able to oversee the management of both information content and infrastructure?

– Are information management roles clearly defined and appropriately identified within organisational structures?

– What is the ideal positioning of information management within an organisation, and why?

- *Information is an intangible asset with relevant attributes of having service potential and being able to give economic benefits to its owner, but not possessing the physical form of an object.*[6]

- Information *is recognised as a significant organisational resource in much the same way as people, machines and capital.*[7]

Some suggest information is not a resource because it cannot be depleted, whereas it can be an asset because it's possible for it to lose value over time (like other tangible organisational assets).[8] Conversely, it could be argued that some information assets actually increase in value over time, depending on their purpose and use.

To some, discussion over whether information is a resource or an asset may be playing with words. However, it is important to recognise that information has value for an organisation. As such, it may be preferable to refer to *information assets* rather than *information resources* because *asset* may provide a greater semantic link to the concepts of *value* and *accountability*.

INFORMATION ASSETS AND RECORDS

If we accept that an organisation can have information assets just as it can have other assets, what do they comprise?

The NSW State Records Office provides a practical summary of information assets:

- (They) *include documents, emails, web content, business data, images, video and other content in both physical and digital form.*[9]

The Queensland Governments Chief Information Office expands on this definition by defining information assets as:

- *a collection of data that has recognised value to an agency in performing its business function/s and meeting agency requirements. Information assets can be documents, electronic messages, a row in a database (or the database table itself), collections of metadata, or a table or figure within a document.*[10]

Quite rightly, both sound fairly similar to the types of information that are often described as records.

The proposition that we need to create somewhat artificial boundaries for information depending on its purpose and use may be one of the reasons for the struggle to have sound recordkeeping practices resourced, adopted and accepted in organisations.

Records clearly fall into the definition of an information asset, yet still many refer to records *and* information, which indicates that records are somehow separate to rather than a component of the broader concept of information.[11]

It is assumed that we do this in an effort to ensure that the wider responsibilities for digital information must be factored into records management. Or is to avoid confusion with information technology? Incorrectly, it infers an equality (genus – genus) relationship (Figure 1), rather than accepting that records should be identified in a genus – species relationship with information (Figure 2).

Constantly referring to *records and information* is akin to referring to *fruit and apples* or *humans and women*.

We need to consider whether our efforts to separate the constructs of information management actually make it more difficult to manage information as an asset.

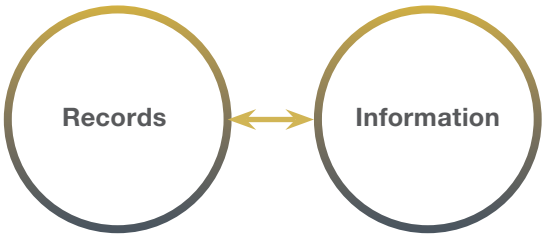


Figure 1: Perceptions of Records and Information

Figure 2: Perceptions of Information and Records

Consultant David Glynne Jones makes the following alarming point:

- *Much of the investment in modern information technology over recent decades has been largely wasted because of the failure to manage information effectively as a core organisational asset.*[12]

In relation to this point, how does technology fit into the above definition of information assets, which is restricted to information content? Technology is required to store, retrieve and disseminate information assets. Is the technology inextricably linked thereby requiring our definition of information assets to include both content and systems?[13] If so, shouldn't the management of these be grouped under a single information management umbrella? It is stressed that this is **not** suggesting that information content management responsibilities such as records management fall under information and communications technology (ICT) management.

INFORMATION MANAGEMENT

Choo says that information management is often (inappropriately) equated with three separate functions, namely:

- management of information technology
- management of information resources, or
- management of information policies and standards.

There is, instead, a need to take a *unifying perspective that would bind these functions together*. She continues with this idea that information management should be *viewed as the management of a network of processes that acquire, create, organise, distribute, and use information... encompassing information processes, information resources, and information technologies*.[14]

Similarly, the Queensland Government views information management as:

- *the means by which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains,*

The various perceptions and treatments of information and information management can lead to confused planning and policy, and fragmentation of responsibilities and resources…

preserves and disposes of its information; as well as any means through which the organisation ensures that the value of that information is identified and exploited to its fullest extent.[15]

The National Archives of Australia has stated that:

- *Information management encompasses all the systems, formats and processes used within an organisation for the creation, management, storage, disposal and use of information. Information management is a broad concept, which has its own discipline and is underpinned by national and international standards. It should not be narrowly applied.*[16]

WHO SHOULD BE RESPONSIBLE FOR INFORMATION MANAGEMENT?

The various perceptions and treatments of information and information management can lead to confused planning and policy, and fragmentation of responsibilities and resources – not just within organisations but also across tertiary education, professional associations, and industry and government bodies setting regulations and standards for information management.

For some writers, the move to managing information as a core organisational asset requires greater education, awareness and collaboration for existing chief information officers and information content managers. For example:

- *There are plans for a national framework for information management. Will this place collaboration between ICT and information specialists more on the agenda?*[17]
- *ICT and recordkeeping professionals in the NSW Government have much to gain from working together to address digital recordkeeping needs… However, the professions often work in 'silos' and fail to grasp the advantages that can be derived from collaboration.*[18]
- *Chief Information Officers must refocus their attention from technology to information…for the effective management, use and dissemination of information.*[19]

Is the issue greater than simply re-education of, or collaboration between information management professionals, because current experience indicates that such an approach is often not successful? How do we overcome the organisational power imbalances that exist between those managing the information technology and those managing the information content?

Glynne Jones proposes that:

- there is *no compelling evidence that effective information governance can be implemented consistently within and across Australian Government agencies without appropriate administrative legislation and regulation (e.g. an Information Management and Accountability Act);* and
- there are *no effective formal mechanisms for the consistent governance and management of public sector information across the government, its agencies and public stakeholders.*[20]

It could be just as valid to say that there is no effective mechanism for the consistent governance and management of information in the majority of organisations; no effective mechanism for consistency in professional qualifications and skills of those responsible for information management; and no effective mechanism for the consistent professional representation of those working in information management.

Let us take just some examples in Australia to support these statements.

- Australian (Federal) **government agencies** with regulatory and advisory information management responsibilities:
  - The Australian Government *Information Management* Office is within the Finance and Deregulation portfolio. Its role includes the planning, support and standardisation of ICT in the Australian government, facilitating information sharing and access to government information. This role extends to producing broad information management policies and tools (such a subject thesaurus to assist government agencies, and policies and guidance in relation to cloud computing and social media).
  - The Office of the Australian Information Commissioner's functions relate to freedom of information and privacy, as well as new functions relating to information policy advice. The information policy area includes strategies for valuing public sector information as a resource. The OAIC resides within the Attorney-General's portfolio.
  - The National Archives of Australia sits within the Regional Australia, Local Government, Arts and Sport portfolio. As well as preserving, describing and providing access to national archives, the NAA also provides information management products and services to Australian Government agencies. The latter includes the provision of products and services for implementing the disposal provisions of the Archives Act, a standard Commonwealth thesaurus, and promoting digital information management.
  - The Protective Security Policy Branch of the Attorney-General's Department, and the Information Security Operations Branch of Defence Signals Directorate, play a key role in establishment and advice for information security.[21]

Similar situations exist or have existed within state government jurisdictions where various bodies responsible for information management have evolved (although it should be said that whole of government information management principles have been developed in some jurisdictions such as Queensland and Victoria).

- A worker in the information management field could justifiably be confused when choosing from the many **professional and industry associations** now identifying themselves more broadly with *information* and *information management*. In Australia, they include:
  - ALIA (Australian Library and Information Association) - the professional organisation for the Australian library and information services sector. (ALIA was formerly the *Australian Library Association*.)
  - AIIA (Australian Information Industry Association) - Australia's peak ICT industry representative body and advocacy group.

- IIM - aims to become the definitive Australasian industry source on the information management industry.
- HIMAA (Health Information Management Association of Australia) – professional association for at the forefront of health information management in Australia. (HIMAA was formerly the *Medical Record Association of Australia* and before that it was the *Australian Federation of Medical Records Librarians*).
- DAMA (Data Management Association) – association of information management practitioners, with the primary objective to "promote the understanding and practice of managing information as key business assets"; and, of course
- RIM Professionals Australasia (Records and Information Management Professionals Australasia) – supporting the profession of records and information management. (Formerly the *Records Management Association of Australasia*).

- **Organisational structures** vary considerably in the positioning of information management roles within the public and private sector:
  - some organisations completely separate information and communications technology from other information services
  - some make information content management such as records management and library services invisibly and powerlessly grouped under a generic corporate management area while positioning the CIO at the same level as the CFO or Director of Human Resources
  - others include "information management" divisions at a prominent position in the structure but on close examination are actually providing ICT services.

A popular theory claims that organisational structures are indicative of an organisation's culture. Where a particular business activity or unit is positioned in the organisation structure indicates organisational relationships and emphasises what is important to the organisation.[22] The value of tangible information technology assets may be more obvious to an organisation's senior management, thereby according business units with responsibility for their management a higher level of importance within the organisation. This can then result in a higher level of resourcing and power for such units within the organisation.

- **Information management positions** have a variety of names and responsibilities. When we think of the management of other organisational assets, this is not usually the case – chief financial officer, finance manager, director financial services, human resources management, etc. tend to be more consistently identified.

The logical title for the key position responsible for an organisation's information assets would appear to be *chief information officer*. However, current responsibilities, qualifications and skills of an organisation's chief information officer tend to be more those of a chief *technology* officer.

For those organisations that have currently positioned all information management responsibilities under the umbrella of the chief information officer, there is often a disproportionate level of attention still given to the "pipes" (physical information infrastructure) in relation to information content planning, governance and accountabilities. This can possibly be attributed to the way in which the incumbent's educational background prepared them for such a role. This leads to the last example of information management inconsistency and ambiguity – tertiary courses.

- A number of **tertiary institutions** offer information management courses with very similar sounding names but with very different areas of focus, e.g. Master of Information Management and Systems (La Trobe), Master of Business Information Management (University of South Australia), Master of Business Information Management (University of Western Australia), and Master of Information Management (RMIT). The content will often depend on whether the course is offered through information services/studies schools or information technology schools. Many educational institutions continue to offer courses that do not provide the necessary linkage and, as a consequence, do not produce graduates who are adequately prepared to take on an overarching role of business information manager/chief information officer (according to the literal meaning of the role).

THE FUTURE OF INFORMATION MANAGEMENT

In summary, it's time for a change, and it's not simply a matter of broadening ICT practices to encompass information governance and accountability requirements or for records managers to collaborate with ICT managers. It's time to change the way organisational information is defined and valued; and it's time to change the way information management is positioned, regulated, and controlled. In doing so, the existing imbalances of organisational power and recognition in relation to information management roles and responsibilities may be addressed.

Can a consistent future information management scenario include the following:

- Legislation that establishes overarching Federal and state information management agencies with jurisdiction over information governance and accountability. (For example, in British Columbia, the Office of the Government Chief Information Officer is the central authority responsible for management of information and information technology. As such the Government CIO is responsible for government policy and procedures covering Information and Technology, Freedom of Information and Protection of Privacy, Recorded Information Management, and Information Security Policy.)[23]
- Organisational structures that consistently identify the management of information assets at the same level as the management of other organisational assets? (Refer to Figure 3 for a simplistic example of such a structure).
- Organisations that recompense incumbents in these positions equally with others responsible for organisational assets of comparable importance and value?
- Tertiary courses that produce graduates with the necessary qualifications to fulfil an overarching information management role? (University of South Australia's Business Information Management post-graduate program appears to go a long way to providing a suitable mix of records,

ABOUT THE AUTHOR

Joy Siller, ARIM, is a director and principal consultant of Siller Business Administration, an information management consultancy.

✉ She can be contacted at joys@siller.com.au

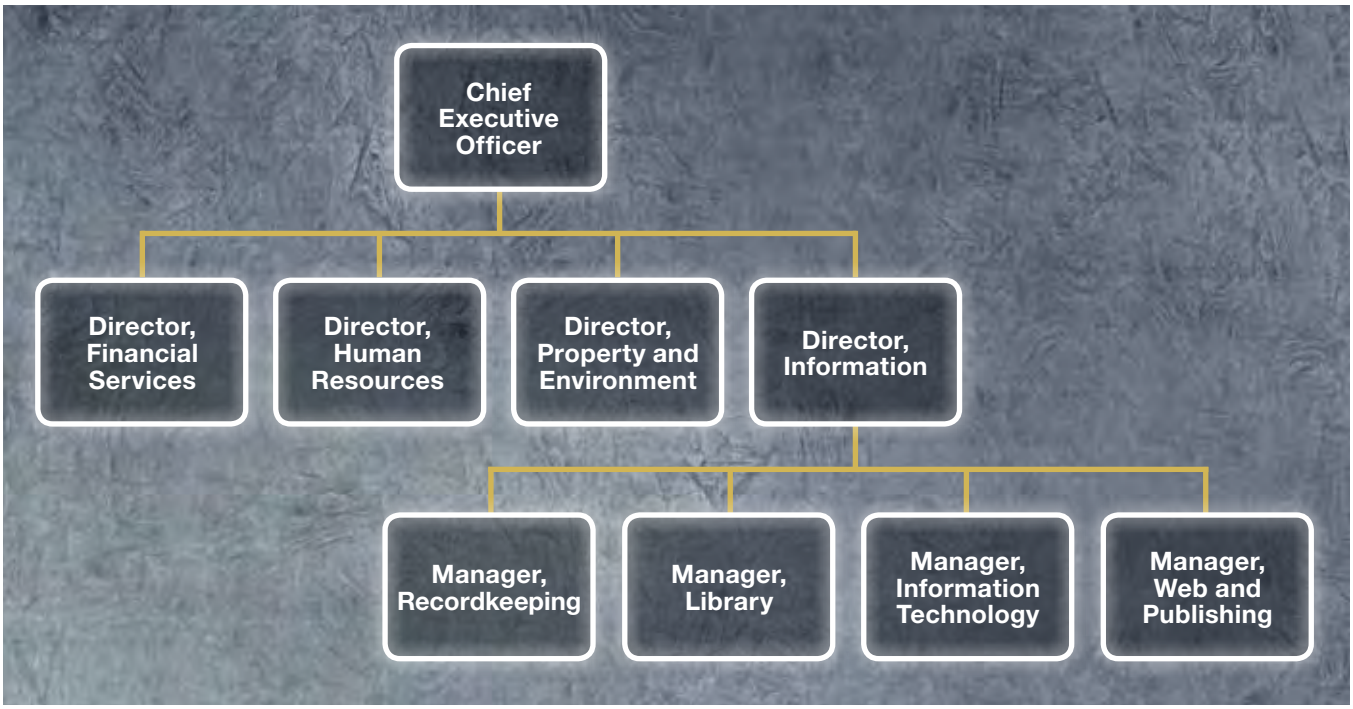


Figure 3: Sample Organisation Structure

archives, information technology, information governance, project management and knowledge management content to achieve this.[24])

- Organisational chief information managers (or other appropriately identified senior positions) with qualifications and skills that enable them to understand and take responsibility for managing the entire information asset management framework including information strategy, governance and architecture?
- Professional associations that have a clear purpose and membership (embracing a broader concept of information management, if necessary)? Is it too late or is the marketplace too competitive for this?

CONCLUSION

Current approaches to the management of our information assets are failing. Sources, channels and repositories of information are proliferating and devolving in a way that is creating capture, access and management difficulties for organisations, governments and society generally. This situation is occurring in global economic conditions that dictate the need for greater reductions in expenditure and, as a result, the logical aggregation of resourcing and responsibilities. It's time to think about smarter, overarching policies and strategies that will facilitate this for information management. Without such an approach, there is a risk that the information disciplines and services that offer the greatest economic benefits will survive and those that offer the qualitative benefits will not.

Finally, to quote Anthony Wong who presented at the Darwin inForum in 2011:

- *"One thing is certain – we (RIM/ICT professionals) either continue to evolve and grow or risk becoming irrelevant".*[25]

Part of this evolution and growth may mean aggregation. ❖

• This paper was first presented at inForum 2012 in Melbourne and Perth.

Bibliography

1 Outsell, p.5
2 Engelsman, s3.1
3 Middleton, p.1
4 Choo, raises the issue of information management as key to creating an intelligent organisation
5 Glynne Jones (Information Policy Conference, November 2011)
6 Engelsman, quoting others, s2.
7 Trauth, p.257
8 Higson and Waltho explore this issue as does Engelsman.
9 State Records, *http://futureproof.records.nsw.gov.au/information-asset-management-assessment-tool/*
10 Qld Government CIO Fact Sheet, p.1
11 The use of *records and information* or *information and records* is now a common theme nationally and internationally, e.g. the National Archives of Australia refers to information and records in its literature, there is a NSW Health Records and Information Privacy Act, Records and Information Management Professionals Australasia, Information and Records Management Society UK, ARMA International states that it is the professional association for records and information managers, and so on. The library associations took a similar path many years ago, e.g. the Australian Library Association became the Australian Library and Information Association. My own organisation has been guilty of the same tautology.
12 Glynne Jones (presentation 2011)
13 James Robinson took the definition of information management further in his 2005 paper by including people, process, technology and content.
14 Choo, p.xiv
15 Queensland Government Information Management Strategic Framework, p. 5
16 NAA submission, OAIC Understanding the value of public sector information in Australia: Issues paper 2: Public consultation
17 State Records NSW, *Future Proof –" Information Management – is it the new thing?"*
18 Ibid, *ICT Attitudes Survey Report – Executive Summary*, p1.
19 Glynne Jones (presentation 2011)
20 Glynne Jones Public Submission, March 2011
21 Based on "About us" information obtained from the websites of the various agencies.
22 Beshay and Sixsmith discussing the Cultural Web model of organisational culture (p.84)
23 http://www.cio.gov.bc.ca/cio/about/about.page
24 http://www.unisa.edu.au/bim/BIM/default.asp
25 Wong (2011).

Digital records management in the Canadian Government: a strategy for 'success'

Digital records management in the Canadian Government is part of records management, which in turn is part of information management. Government of Canada information management was publically reported as one adverse factor to departmental performances under the Canadian federal Access to Information Act in recent years, which motivated an academic inquiry into this matter. This article reports on the inquiring process and the preliminary findings it generated.

By **Sherry L. Xie**

story snapshot

An assessment showed that many institutions in the Canadian Government (CG) mismanaged or did not even know about the existence of their 'information holdings'.

A subsequent study into information management (IM) in the government focused on the status of digital records management (DRM).

It was established that records management (RM) is part of IM, and is disappearing in the IM landscape.

RM and DRM in GC will disappear by June 2014.

Digital records management (DRM) is not a term used in the Canadian Government (GC), nor the term electronic records management. Electronic or digital records, however, have never been excluded from the scope of the Canadian federal archival legislation. The 1912 Public Archives Act (the first) addressed "public records … of any kind, nature and description"[1] and the 1987 National Archives of Canada Act listed explicitly "machine-readable record" as one type in addition to the phrase "regardless of physical form or characteristics" in its definition of record.[2] The 2004 Library and Archives Canada of Act (the current) follows basically the mode of the 1987 law, defining record as "any documentary material other than a publication, regardless of medium or form".[3] In the GC workplace, similar to other developed countries that entered the world of the computer in the 1950s, computerised/digital records have ever since been created and used, and have gradually become the de facto main type of institutional records. In the 2007 Policy on Information Management, the Treasury Board of Canada requires departments to ensure that "electronic systems are the preferred means of creating, using and managing information",[4] establishing at a GC-wide level the endorsed status of digital records.

Records management (RM) has existed in GC since 1978, when a dedicated, government-wide policy was used to mark the starting point.[5] As records encompass digital records, RM includes DRM. It is in this sense that DRM exists, or should exist, in the government. This article uses the term digital records management or DRM as it has gradually gained acceptance in the international records community and as the term digital describes computerised records more accurately than the term electronic. It reports on a project that focused on the status of DRM in the Canadian Government and its preliminary findings.

A GROUNDED THEORY STUDY OF IM CRISIS

The project, entitled 'A grounded theory study of the information management crisis in the Government of Canada', was inspired by the strong criticism of the Information Commissioner of Canada on IM being one of the major contributing factors to the GC institutions' poor performance under the Access to Information (ATI) Act, the Canadian federal freedom of information legislation.[6] The phrase "information management crisis" was originally used by the Information Commissioner of 2009 when reporting on the results of his office's assessment over selected GC institutions.[7] The IM crisis referred to the fact that many GC institutions mismanaged or did not even know about the existence of their "information holdings", thus consequently having failed to respond to ATI requests within the legally stipulated timeframe. In the context of the ATI Act, information means that held "in records under the control of a government institution",[8] and with respect to the administration of the ATI Act, information holdings mean the aggregations of records produced by GC institutions' "functions, programs, [and] activities."[9] Thus, the IM crisis indeed points to RM issues.

The selection of grounded theory (GT) as research methodology was motivated by the intention of finding explanations for the issues presented. The grounded theory methodology specialises at probing a general problem in a substantive area by collecting, analysing, and constantly comparing first empirical then all relevant data regardless of sources, in order to produce theories/explanations that fit or work for the substantive area under investigation.[10] To probe a general problem (eg, the IM crisis) means not to formulate specific research questions based on existing theoretical framework(s) or comprehensive literature review as typically required by social science research methodologies. How to avoid reinventing the wheel thus becomes a challenge for employing this method. To satisfy program requirements as established by the University, a literature survey was conducted to first, demonstrate that there was no academic research done on this subject, second, present the research setting (i.e., GC and its structure), and third, justify the significance of the research.[11]

DRM IN THE GOVERNMENT OF CANADA

For understanding DRM in GC, two types of data were collected and analysed. The first type consisted of relevant information on the various GC websites and was categorised as GC-wide and institution-specific. The GC-wide group included policies, directives, standards, and guidelines issued by agencies responsible for IM at the GC level such as the Treasury Board of Canada Secretariat (TBS) and Library and Archives Canada (LAC), and the institution-specific group included department organisational structure, annual report and internal audit report, as well as the management accountability framework assessment report by TBS.

The second type of data constituted records on departmental IM/RM operations obtained from 24 departments by ATI requests, intended to complement the first type of data. The departments to which ATI requests were sent were those evaluated by the Office of Information Commissioner in the fiscal year of 2008;[12] the received records constituted *released data*. In addition to the released records, the ATI request handling process generated data including communications with ATI analysts (emails and phone conversations), and communications with IM personnel (emails and teleconferences), both of which constituted *process data*. The researcher also visited four GC institutions, each for a unique reason: TBS, for its central role of issuing GC-wide IM policies and directives, LAC, for its legal role of advising IM in GC institutions, PWGSC (Public Works and Government Service Canada), for its role of providing departments access to the Electronic Document Records Management System (EDRMS) as a shared service, and AAFC (Agriculture and Agri-Food Canada), for its invitation to experience its EDRMS implemented in that department. Data generated in this process constituted *field data*.

Eight among the 24 institutions were first selected for analysing institution-specific data. The selection was based on a criterion that combined the OIC's rating over ATI performance and the fact that RM issues were explicitly pointed out as associated. This group included those with an OIC rating below satisfaction (ie, D or F in a scale from A to F). The first type of data (ie, data online) relevant to the eight institutions, the process data, and field data were analysed following the GT method. The findings that came out of the long process of collecting and analysing data can be categorised as three threads: 1. IM and GC business 2. IM and Information Technology (IT), and 3. IM, RM, and DRM.

IM AND THE BUSINESS OF THE CANADIAN GOVERNMENT

The current GC IM strategy is conspicuously marked by its focus on business, as evident in all types of data. Three areas reflect this focus: IM characterisation, IM business alignment, and IM specialist-business manager/employee collaboration.

GC-wide policy requirements, standards, and guidelines typically characterise information or information resource as "a strategic business resource", "vital business asset", or "evidence of our business activities", and IM as an internal service that supports "the department's business" and meets "departmental business objectives".[13] Correspondingly, TBS policy instruments displayed strong emphasis on establishing IM-business alignment. Policies and directives prescribed IM practices to be aligned with "business activities" and IM requirements to be integrated with the "development, implementation, evaluation, and reporting activities" of departmental programs and services.[14] To capture the relationship between information and business, LAC developed a methodology for constructing classification system, entitled Business Activity Structure Classification System (BASCS).[15] The IM-business alignment was also reflective of the roles and responsibilities assigned to department senior officials, managers, and employees. IM specialists were responsible for "supporting the effective management of departmental information". They were required to collaborate with program managers for addressing IM requirements in business development and operation, and to assist employees in applying IM "principles, standards, and practices" for performing their business duties.[16]

Departmental IM strategies and sometimes action plans (not all of the institutions analysed had action plans) followed basically the same mode of characterisation, alignment, and collaboration, so did the opinions of the IM specialists communicated. This is in line with the GC whole-of-government approach, which requires cross department functions such as IM to operate in conformance within the GC-wide policy and accountability framework.

RM is, however, disappearing in the IM landscape

The IM-business alignment, however, appears to be only on 'paper', ie, described in departmental IM strategic plans yet lacking concrete implementations. All eight institutions were assessed by TBS as insufficient in implementing their plans, and four of them were not even fully aligned on 'paper'.[17] For the requirement of IM specialist-business manager/employee collaboration, there was one and only one form for its execution, and that is, "if you (business managers/employees) contact me, I (IM specialist) will answer/respond to you". What this form had produced in terms of results remains unknown because there were no records found – either online or from the released packages – regarding its performance in institutions examined.

IM AND IT

The characterisation of IM, IT and their relationship in GC occurred first in 1993, by TBS, which considered both IM and IT as 'powerful enablers' and their relationship as of 'collaboration'.[18] The expression 'IM/IT' was used throughout the document, in which IM was exemplified as information policies and standards, and IT included networks, applications, and systems. The enabling status of IT remains as the same in the Policy on Information Technology, 2007 and the Policy Framework for Information and Technology, 2007,[19] yet the status of information had changed to "an essential component of effective management" in the Policy on Information Management, 2007 and "the cornerstone of a democratic, effective, and accountable government" in the Policy Framework for Information and Technology, no longer an enabling role. The Policy Framework also changed the relationship between IM and IT as it uses the expression "the management of information and associated technologies" and states that "information technology (IT) is a key enabler to achieving well-managed information". This seems to justify the order in the IM/IT expression as IM is put before IT.

IT, however, is in fact the real focus of almost all IM/IT initiatives in institutions examined. As the various types of data revealed, when IM/IT was used, the content was typically about IT. It was rather evident as seven out of the eight institutions fell within this category, and each possesses multiple indicators. Examples include:

- 'IM/IT initiatives' referred to "the implementation of a data centre that houses mission-critical computer systems and associated components"[20]
- 'IM/IT' achievements meant the adaptation of "a new innovative interoperable Web 2.0 tool called Oracle Beehive"[21]

- an audit report entitled Audit of Information Management/ Information Technology (IM/IT) Governance (2009) was entirely about IT as the audit aimed at "the effectiveness of information technology investment management".[22]

There were also indicators demonstrating that in some cases, even if it was only IM that was used, the content was still about IT projects. Examples included:

- using an EDRM system to refer to the implementation of an "IM Strategy",[23]
- using PeopleSoft to refer to the "IM system" for Human Resource management,[24] and
- an audit report with "Information Management" in title but discussed IT projects.[25]

To the extreme, some institutions explicitly used "IT" to represent "IM/IT",[26] or "Information technology" to represent an entire "Information Management Branch".[27]

IM, RM AND DRM

GC establishes that RM is part of IM, along with other IM components such as data management, document management, and library services.[28] RM is, however, disappearing in the IM landscape as evidenced by the following findings:

- TBS policies and directives addresses IM as a single discipline[29] while listing components, there were no separated, specialised treatment for RM or DRM
- TBS MAF assessment, departmental performance reports, audit reports, and occasionally departmental IM annual reports also treat IM as a whole, making it impossible to learn about RM (including DRM) performances – the only channel that revealed, in an indirect manner, some aspects of RM operations was the OIC's assessments over department ATI performances
- There were few or no records positions in organisational charts[30] – when there were, all of them are low ranked
- It was IM – not RM – positions that made RM policies and standards, and provided RM trainings; and
- The actual RM work (i.e., identify, capture, classify, etc.) was conducted by employees and 'ensured' by their managers.

For DRM, it has rarely truly happened:

- Electronic document management could be found under IM in organisational charts but not electronic/digital records management.
- Departmental policies and/or manuals used the term record(s) mainly for paper records.
- No guidance on identifying digital records except for emails.
- Few successful implementations of the GC EDRMS, with AAFC being one of them; LAC represented the worst.
- None of the ATI units in the institutions examined had access to the GC EDRMS.

Bibliography

1 Canada. 1912. Public Archives of Canada Act. s7.
2 Canada. 1987. National Archives of Canada Act. s2. http://laws-lois.justice.gc.ca/eng/acts/N-2.5/20021231/P1TT3xt3.html; accessed June 26, 2012 (Note: all URLs in this article were fully accessible on this date).
3 Canada. 2004. Library and Archives of Canada Act. s2. http://laws-lois.justice.gc.ca/eng/acts/L-7.7/FullText.html.
4 Treasury Board of Canada. 2007. Policy on Information Management. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742&section=text.
5 Treasury Board of Canada. 1978. Administrative Policy Manual, Chapter 460 Records Management.
6 The project was conducted by the author of the article for partially fulfilling the requirement of a PhD degree, at the School of Library, Archival and Information Studies, University of British Columbia, Canada, under the supervision of Dr. Luciana Duranti.
7 Office of Information Commissioner of Canada. A Dire Diagnosis for Access to Information in Canada. http://www.oic-ci.gc.ca/eng/med-roo-sal-med_spe-dis_2009_4.aspx.
8 Canada. Access to Information Act. R.S.C., 1985, c. A-1, s2. (1). http://laws-lois.justice.gc.ca/eng/acts/A-1/FullText.html.
9 Canada. Info Source 2010. http://www.infosource.gc.ca/emp/emp00-eng.asp.
10 Barney G. Glaser & Anselm L. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago.: Aldine.
11 Sherry L. Xie. 2009. Striking a Balance between Program Requirements and GT Principles: Writing a compromised GT proposal. *The Grounded Theory Review*, vol.8, no.2, pp. 35-47.
12 Office of Information Commissioner of Canada. Out of Time. Special Report to Parliament 2008 - 2009 Systemic Issues Affecting Access to Information in Canada. http://www.oic-ci.gc.ca/eng/rp-pr_spe-rep_rap-spe_rep-car_fic-ren_2008-2009.aspx.
13 TBS. Policy on Information Management; TBS. Directive on Information Management Roles and Responsibilities. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12754&section=text#cha4; TBS. Guideline for GC Employees: IM Basics. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?evttoo=X&id=16557&section=text.
14 TBS. Directive on Recordkeeping. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=16552; TBS. Directive on Information Management Roles and Responsibilities.
15 LAC. Business Activity Structure Classification System (BASCS) Guidance. http://www.collectionscanada.gc.ca/government/products-services/007002-2089-e.html.
16 TBS. Directive on Information Management Roles and Responsibilities.
17 TBS. Management Accountability Framework. http://www.tbs-sct.gc.ca/maf-crg/assessments-evaluations/2009/menu-eng.asp.
18 TBS. Strategic Directions for Information Management and Information Technology: Enabling 21st Century Service to Canadians. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/tb_oimp/sdimit01-eng.asp.
19 TBS. Policy on Information Technology. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=12755; TBS. Policy Framework for Information and Technology. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12452&section=text.
20 Canadian Food Inspection Agency. Departmental Performance Reports. http://www.tbs-sct.gc.ca/dpr-rmr/2009-2010/inst/ica/icapr-eng.asp?format=print.
21 Health Canada. Department Performance Report. http://www.tbs-sct.gc.ca/dpr-rmr/2009-2010/inst/shc/shcpr-eng.asp?format=print.
22 Health Canada. Audit Reports. http://www.hc-sc.gc.ca/ahc-asc/pubs/_audit-verif/2009-28/index-eng.php.
23 Canadian Heritage. Department Performance Report. http://www.tbs-sct.gc.ca/dpr-rmr/2008-2009/inst/pch/pchpr-eng.asp?format=print.
24 Health Canada. Department Performance Report. http://www.tbs-sct.gc.ca/dpr-rmr/2009-2010/inst/shc/shcpr-eng.asp?format=print.
25 National Defence. Analysis of Information Management Projects (2009). http://www.crs-csex.forces.gc.ca/reports-rapports/rp-av-eng.aspx.
26 Canadian International Development Agency. Audit of the IM/IT Strategy, Processes and Controls, 2008.
27 Correctional Service Canada. DPR. http://www.tbs-sct.gc.ca/dpr-rmr/2009-2010/inst/pen/penpr-eng.asp?format=print.
28 TBS. Policy on Information Management, s3.
29 Ibid.
30 The exception is with institutions that still manage a large number of paper records, such as the Canadian International Development Agency.
31 See, e.g., TBS Information Management in the Government of Canada: The Business Problem Assessment. http://www.tbs-sct.gc.ca/im-gi/resources/bpa-epo/bpa-epo00-eng.asp, and LAC. Information Management Capacity Check. http://www.collectionscanada.gc.ca/007/002/007002-2008-e.html.
32 TBS. Directive on Recordkeeping.
33 LAC. New Service Model and the Directive on Recordkeeping. http://www.bac-lac.gc.ca/eng/news/Pages/new-service-model-and-the-directive-on-recordkeeping.aspx.
34 Emphasis added.

- None of the many IT initiatives sampled by audit report that produced digital records demonstrated any concerns regarding digital records or any connections with DRM.
- None of the institutions examined had a function-based records classification system based on the BASCS methodology, considered suitable for the digital environment.
- None of the RM component of the IM unit in the institutions examined aid directly retrieval of digital records for ATI requests; the search process mostly depended upon people, sometimes technologies, but not records.
- None of the institutions examined were able to provide records regarding the numbers and locations of digital records produced by their institutions. according to many of the ATI analysts, "records are everywhere".
- Records (including digital ones) on *RM* operations were difficult to be found and/or retrieved if they were older than two years.

All of the above contributed to the poor performance of RM especially DRM, yet GC's strategy for improvement has never focused on solving DRM issues. Instead, the focus was on IM,[31] and most recently on the "keeping" of "information resources of business value". This newest strategy is a TBS directive, issued in 2009 and entitled Recordkeeping Directive. Although "record" appears in the title, it never appears again in the text. The Directive is about "information resources of business value", defined as "published and unpublished materials, regardless of medium or form, that are created or acquired because they enable and document decision-making in support of programs, services and ongoing operations, and support departmental reporting, performance and accountability requirements". No justifications or deliberations found regarding the usage of this term, yet the definition reads evidently similar to that of record. Assuming by its origin, it may be the case that, as IM officials in institutions considered that "electronic document" could raise the RM profile, GC imagined that "information resources of business value" will transform its unsatisfactory IM performance.[32]

Recordkeeping, thus, no longer possesses any relationships with RM. As GC institutions are required to be compliant with the Directive by June 2014,[33] RM and DRM in GC will disappear by that year. Does this matter? Simply changing the name for records may arguably not, yet to forego RM principles at the same time surely does. When the designated departmental 'IM senior official' is required to be responsible for "establishing, implementing and maintaining retention periods for information resources of business value, as appropriate, according to *format*",[34] everybody in the records community should start to ask questions.

SUMMARY

The project at this stage has unfolded the true picture of RM and DRM in the GC covered under the fashionable IM and "information resources of business value" sheet. Although policy requirements firmly connect IM with business activities and rightfully recognise that technology is only an enabler to IM, the performance of RM, the main component of IM, simply could not match up with business needs and has been playing a passive role in technological endeavors.

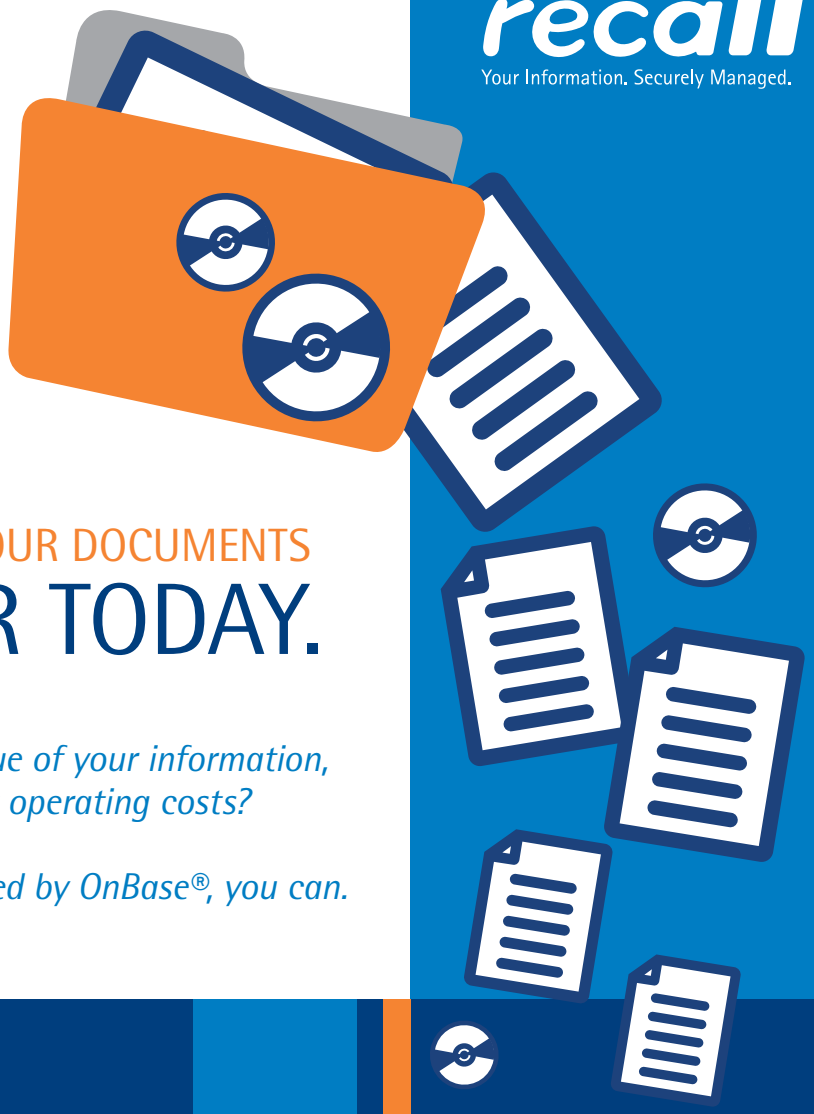
This raises serious questions. *Why have these policy requirements failed to be translated into work performance? Is addressing Information Management as a single discipline a justifiable policy consideration? Will changing the name of record transform the RM performance?* In other words, *will this new Recordkeeping Directive bring success to the current disappointing, even sad situation of RM and DRM in the GC?* The search for answers to these questions continues. ❖

• This article was first presented at inForum 2012 in Melbourne.

ABOUT THE AUTHOR

Sherry L. Xie is a PhD candidate and Adjunct Professor at the University of British Columbia, Canada. She has worked as subject librarian, archivist and records manager in university and government settings in China and Canada.
✉ She can be contacted at sherryx@interchange.ubc.ca

recall™
Your Information. Securely Managed.



GO DIGITAL
& MAKE YOUR DOCUMENTS
WORK SMARTER TODAY.

Are you ready to leverage the intrinsic value of your information, automate your business processes and cut operating costs?

With Recall's highly-rated ReView™ powered by OnBase®, you can.

ReView is an Enterprise Content Management (ECM) software suite that can capture, store, manage and distribute digitised information within a single department or across an entire enterprise.

ReView enables users to:

- Reduce time and cost to perform important business functions
- Improve organisational efficiency and workflow
- Consistently comply with industry regulations and corporate policies

ReView is applicable to companies in virtually any industry including financial, insurance, medical, government, business services, consumer/packaged goods and others. It can support specific departments or functions such as Accounts Payable, Accounts Receivable, Human Resources, Contract Management, Claims or Forms Processing, as well as other paper-intensive activities in today's business environment.

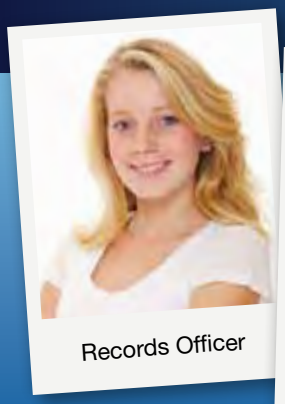
As a global leader in lifecycle information management, Recall has the experience, people and facilities to expertly protect and secure your information. Our comprehensive menu of services includes physical storage, digital management, data protection and secure destruction.

To make the digital leap securely, contact us today at recall.com.au

CONTACT US:

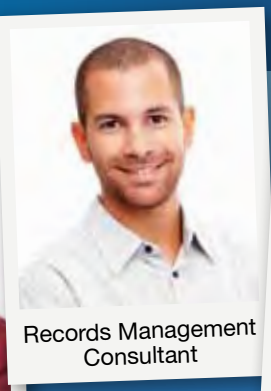
Call 13 RECALL
– 13 7322 55
moreinfo@recall.com
www.recall.com.au

RIM Professionals Australasia supports members' professional development throughout their careers

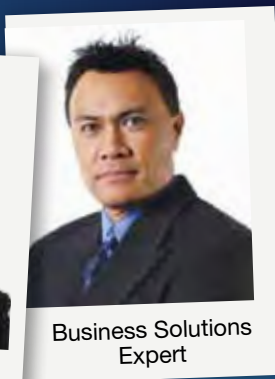

Records Officer


Records Coordinator


Corporate Records Manager


Records Management Consultant


Information Management Lecturer


Business Solutions Expert

R·I·M
Professionals Australasia

Career website
careers.rimpa.com.au

Recognised Courses & CPD Scheme
rimpa.com.au/professional-development/