Vol 32 / Issue 2 / May 2016 / issn 0816-200x
AU $90.00 incl GST ($81.81 + GST) for four issues

iQ THE R·I·M QUARTERLY

Professionals Australasia

+ The role of information management in preventing major disasters

PRIVACY AND SECURITY

Privacy and security in our complex digital world

Managing change in information security

New Victorian data security standards roll-out

See more at www.rimpa.com.au

iQ THE R·I·M QUARTERLY
Professionals Australasia

VOLUME 32 / ISSUE 2 / MAY 2016

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.

COPYRIGHT & REPRODUCTION OF MATERIAL
Copyright in articles contained in *iQ* is vested in their authors. Most editorial material which appears in *iQ* may be reproduced in other publications with permission gained through *iQ*'s Editor.

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.

DISCLAIMERS
Acceptance of contributions and advertisements including inserts does not imply endorsement by RIM Professionals Australasia or the publishers. Unless otherwise stated, views and opinions expressed in *iQ* are those of individual contributors, and are not the views or opinions of the Editor or RIM Professionals Australasia.

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

IN THIS ISSUE

CONTENTS

View from the Chair

From the CEO's desk

Industry news

Psychology of RIM

Cloud content

Privacy & security

Government

Disaster management

inForum 2016

Awards

Digital dreams

Debbie Prout, Chair of the Board, RIM Professionals Australasia

Privacy and security, and the value of training

The issue of privacy and security is something that concerns us all, but it is not something that is handled particularly well in many organisations. I remember when the *Privacy Act 1988* was first introduced, and we were all very proactive in implementing many processes and reviewing the security of our information. We undertook audits to understand how our information was being managed, and as a consequence changed many processes particularly in relation to access and storage. We also ensured staff undertook compulsory privacy awareness training.

But have we kept it up or have we got complacent as time has gone on? When I undertake audits and ask questions around privacy or records management training, most organisation say “yes, we trained all staff a number of years ago but haven’t done anything for a while”. It is up to us – the information management specialist – to keep this type of training current and relevant. It should form part of any induction training, and refresher training should be done every two to three years.

INFORUM 2016

While on the subject of training, advertising for inForum 2016 has commenced, and the full program is now available. The theme for this year’s conference is ‘The Value of Information’, and the focus will be on how RIM professionals can assist their organisations to reduce costs and increase efficiency through effective systems and processes. As always the exchange of information and ideas is critical to the success of these events and the contacts you make are invaluable. This year inForum is being held in the beautiful city of Perth, and I am going to take the opportunity to extend my stay and explore parts of this amazing state.

At the Gala Dinner at inForum 2016, we will be announcing the winners of the prestigious RIMPA Awards. We often hear about the wonderful people in our industry and the amazing projects they have undertaken, so this is the opportunity to have them recognised and celebrated. I encourage you all to nominate. Categories of awards include:

- Industry Contribution
- *iQ* Magazine Article of the Year
- J Eddis Linton Awards
- Research and Education Grant

For full details of these awards and others offered by individual branches, please go to rimpa.com.au/grants-and-awards.

Debbie Prout
RIMPA, Chair of the Board

Kate Walker, Chief Executive Officer, RIM Professionals Australasia

Looking outside the square in a time of change

The traditional model for associations is not working the way it used to in today's digital business environment – and it means that RIMPA needs to make some changes.

You have no doubt noticed that today's association model isn't nearly as effective as it once was. There have been irreversible trends that are making the traditional model and accepted practices obsolete (things such as rapid advances in technology, higher member expectations, increased competition and diverse member markets).

Perhaps the biggest significant and permanent change that has occurred is that the internet has substantially changed traditional information delivery models.

In today's environment, the traditional model for associations doesn't work well and it means that we need to make changes. We need to adopt different approaches and methods. When changes in the environment are significant, radical changes are necessary; and in undertaking radical change, we must challenge our basic thinking.

In the first instance, we want to start a thought-provoking discussion, not only with our Board and our Branches / Chapter Councils, but as an informal conversation between our members. Ideas, once casually batted around, take root and begin to grow. As one conversation leads to another, the merits of change develop, paving the way for a new way of doing things.

RIMPA needs to look at some changes – these include:

- overhauling the governance model and committee operations
- rigorously defining the member market
- rationalising programs and services
- building a robust framework.

The changes will lead to a streamlined and nimbler governance; a realistic, well-defined member market that's easier to find and market to; product offerings that are desirable and beneficial for members; and increased financial and human resource capital.

Radical change is necessary because the environment has changed, and associations have not kept pace. Here is a list of marketplace realities that have changed the playing field for membership:

- Time – Everyone still has 24 hours in the day, but what has changed is how much people are trying to cram into those 24 hours. People will make time for projects that are meaningful, ideas that help them perform in their work, initiatives that are interesting and causes that they care about. RIMPA needs to consider these elements when developing programs and opportunities.
- Value expectations

- Market structure – Specialists want specialised knowledge. They want to network with other specialists.
- Generational differences – While I don't want to label or stereotype, it's clear that every generation has its own values when it comes to volunteer service and expectations regarding return on investment for membership dollars.
- Competition
- Technology

RIMPA needs to make some changes

So, basically, it all comes down to:

- meeting the needs of members and prospective members
- providing a sense of community, with an emphasis on enabling members to congregate physically, even in a world characterised by frugal travel budgets
- offering opportunities to network and facilitate
- providing credentials differentiated by industry
- advocating for RIM professionals with every entity likely to impact their careers.

I invite, and welcome, all comments, suggestions etc as we need to continue to look outside the square at how to move forward and ensure that we remain vital in the future.

I will, as some of you will have already seen, be undertaking 'quick questions' and surveys to measure metrics and gain insight into the issues and needs of all RIM professionals.

Please feel free to contact me directly (everyone's voice is welcome, new or experienced) at: kate.walker@rimpa.com.au

Kate Walker
Chief Executive Officer

WORLDWIDE NEWS

Director appointed for new NT Archives Centre

Phyllis Williams has been appinted as the director of the new Northern Territory Archives Centre in Darwin, commencing in the role earlier this year.

Phyllis Williams

The National Archives of Australia and the Northern Territory Department of Arts and Museums joined forces in 2013 to provide a one-stop archival shop, co-locating the collections of the National Archives of Australia and the Northern Territory Archives Service on one site. As part of their co-location, the organisations agreed to jointly appoint a director to oversee the centre.

Ms Williams has been working with the National Archives since 1996 and in the contract role of director of the co-located Northern Territory Archives Centre since January 2013. She played a key role in ensuring the smooth and successful co-location of the two organisations over the past three years.

As an Indigenous issues specialist and policy adviser, Ms Williams chairs the Aboriginal advisory groups for both the National Archives and the Northern Territory Archives Service. She continues her involvement with Northern Territory link-up organisations and stolen generations reference groups.

Ms Williams was awarded a Public Service Medal in the Queen's Birthday Honours 2011 for 'outstanding public service in driving significant reforms to communications and service delivery in the National Archives of Australia, particularly in relation to Indigenous Australians in the Northern Territory'.

Professionals roused to oppose Trove funding cuts

Archivists, historians and writers have declared war against Australian Federal Government plans to slash its National Library funding – cuts that threaten continuation of the country's world-leading on-line 'knowledge repository', Trove.

The $20 million cuts were announced in December, like so much other government bad news, just before the long holiday period. Immediate reaction was muted.

The threat to Trove was revealed in mid-February. The National Library confirmed that, to meet the cuts, it would haul back on staffing and slash its digitisation program, including the Trove service. After accumulating 20 million pages from 100 historic Australian newspapers among 300 million items from publications, archives and datasets, the NLA announced:

"The library will cease aggregating content in Trove from museums and universities unless it is fully funded to do so."

Furious bloggers

Information management blogs burst into fury, backing Trove and demanding government re-thinking. Authors on Melbourne-based *The Conversation*[1] site, Deakin University Professor Deb Verhoeven and Melbourne University Research Archivist, Mike Jones, hit out in a posting 'Why defunding Trove leaves Australia poorer', demanding:

"If the National Library puts Trove to the sword as a result of the government's cuts, this innovative stash of content may end up dispersed and buried again, taking Australia off the map. That would definitely leave us poorer, an information desert island in an increasingly interconnected world."

'Recently-departed' Trove manager, Tim Sherratt, thundered on his own Discontents blog[2]:

"Trove's changing the practice of history, changing our relationship with the past. But it is not just newspapers. Trove brings together collections of hundreds of other organisations large and small. Together with the National Library's own digital collections, Trove creates a resource profound in depth and meaning, and brimming with the capacity to surprise."

Monash University School of IT masters scholar, Annelie de Villiers, posted[3] a #fundTROVE letter template for protests to Communications Minister, Mitch Fifield, highlighting the "detrimental impact (the cuts) will have on Trove, the NLA's world-leading knowledge repository."

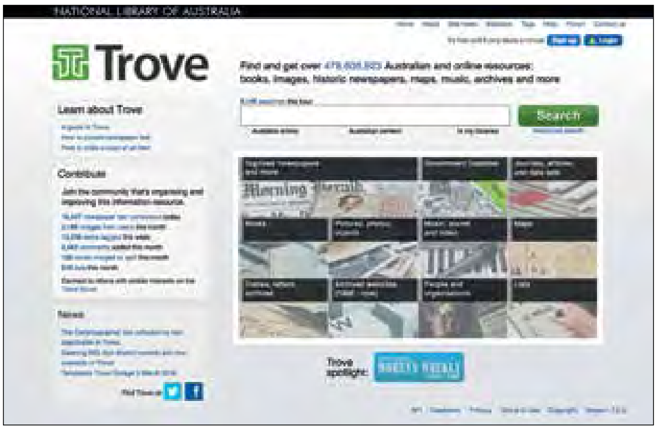
Media joins in

National and international media quickly joined the fight. The ABC news service quoted Australian Library and Information Association CEO, Sue McKarracher, saying: "Trove isn't just a nice thing to have; it's not just about digital access to museum pieces or library documents. This is a fundamental piece of our national research infrastructure."

In the British daily, *The Guardian*, Australian columnist and author, Paul Daley, furiously declared: "We invest governments with the confidence to make spending decisions. And they do – like increasing defence spending to 2% of GDP so that Australia might 'invest' $50bn in 12 new submarines, while cutting $20m from national collecting institutions in the arts portfolio."

Media sports commentators protested, too. *The Australian* cricket writer Gideon Haig, had a colourful, non-sporting view: "Trove is our canary in the coalmine. That a resource so effective, efficient, advanced and accessible can be degraded is an indictment of our political and our cultural priorities."

Sydney Morning Herald 'Third Degree' blog columnist Eric Cervini, caustically challenged the threat to "hugely popular" Trove's "wonderland of information". She posted: "There are government funding cuts that are dumb. Then there are cuts that are the dumbest."


NATIONAL LIBRARY OF AUSTRALIA
Trove
Find and get over [illegible] Australian and online resources: books, images, historic newspapers, maps, music, archives and more
Search
Learn about Trove
Contribute
News
Trove spotlight:

NAA prepares to move 15 million treasures to new cold storage

National Archives of Australia is getting ready to move more than 15 million items from its old Canberra storage facility to its huge, new $64 million coolstore just across the road in the suburb of Mitchell.

Building completion is due early next and will almost triple the amount of chilled shelf space available for preserving historic Australian treasures like early documents of Federation, sensitive classified material, photographs, interviews and even airline boarding passes of The Beatles and David Bowie, among others.

The move will take eight months, officers calculate. The new building will hold more than 100 kilometres of shelving … the bulk of the project's cost … offering options of cool, cold and sub-zero storage.

Treasures deserve better

National Archives Director-General David Fricker told *ABC News* that the move was primarily to keep up with the times and digitise the collection.

"We're just running out of space, and also we're getting a bit old here," he said. "The original building was state-of-the-art when it was first constructed, but that was many decades ago. These records deserve a state-of-the-art and modern facility."

The new building walls are constructed from hundreds of giant concrete slabs made in Adelaide. The builders say these will do most of the work keeping the documents cool "rather than air conditioning running 24/7".

NAA conservators are repairing and restoring as the packing goes on. Senior conservator Clair Murray told *ABC News*: "It's painstaking. We're having to take off old repairs that have been done in the past, perhaps not as sympathetically as we would wish."

New material will join the NAA holdings, among it the 80-year-old Stanley Fowler collection of more than 13,000 items of film and photographs portraying the Australian coastline and fishing industry and rare aerial photos from 1936 to 1947. The collection, including highly-flammable nitrate-based negatives, has been held by the CSIRO for 16 years. It will join the NAA's two kilometres of photographic shelf space safely in chill-rooms until it can be digitised.

Artist's impression of National Archives Preservation Facility, Mitchell ACT

Branch blasts Archives NZ 'Draft Regulatory Statement'

RIMPA's New Zealand Branch has challenged Archives New Zealand's 'Draft Regulatory Statement'[4] for the covert "totally out of the clouds" release of the publication and its "vast change in paradigm" of prescriptive terminology.

The branch backed a workshop in Auckland late last month. The gathering was the first Auckland recordkeeping network event organised by Archives NZ. Archives' Government Recordkeeping Directorate staff could "talk about their work to optimise Archives New Zealand's regulatory role," NZ Branch president, former RIMPA chair, David Pryde, MRIM, announced in April's edition of RIMPA's *Around the RIM* e-zine.

Vale: Karen Chetcuti

By **Debbie Prout**, RIMPA Chair of the Board

In January 2016 the records management community tragically lost one of the most respected records managers in local government, Karen Chetcuti.

I remember meeting Karen at an Infovision user group meeting many years ago and my first impression of her was her love of life and her ability to make people feel at ease. She and I had many discussions over the years on the difficulties of managing records in local government and the good and bad of systems. I know she was looking forward to bringing the digital age to the Rural City of Wangaratta by implementing RM8 (TRIM), and the project team is determined to make her vision happen. The work she had started will be completed and will stand as a testament to her determination and persistence.

Karen was a very active member of the Victorian Local Government Chapter and had also joined the North East Region Information Management Group which had only recently been set up. The convenor of this group, Leanne Wegrzyn, said that the meetings were always a lot of fun because of Karen's wonderful sense of humour.

Her dedication and commitment to her staff were evident and she regularly gave them the opportunity to attend industry events. She had formed close ties with other records staff in the region and was always willing to share her knowledge and provide any assistance when needed.

I was very privileged to have known her for over 15 years and will miss her beautiful smile and calm presence. On behalf of the Association, I would like to pass on our sincere condolences to her two children, her family and the staff at the Rural City of Wangaratta.

In his release entitled 'Apparition or God send', David protested: "Don't get me wrong. RIMPA supports any initiative from regulators that is proactive and prescriptive, that removes assumption and confusion and facilitates 'best practice' solutions. However, the language and the tones used in the (draft statement) are a vast change in paradigm from the consultative, supportive partner that practitioners have been used to at ANZ Forums."

RIMPA NZ Branch President, David Pryde, MRIM

"Why the secrecy?"

He asked the meeting to question the draft's "inconspicuous entry into the government recordkeeping community" without fanfare and chief archivist Marilyn Little's failure to introduce the document, "the most significant change in ANZ operation since 2010", the year the NZ *Public Records Act* came into force.

Speaking to *iQ* later, David argued: "The draft's use of the term 'regulated sector' is incorrect because we only have Mandatory Standards that require *'public sector organisations to achieve a range of records management outcomes but recommends or suggests rather than prescribes specific methods for doing so'*. This is totally opposite to the language used in the draft."

He charged that the statement contained "a number of components clearly cut and pasted from ANZ parent Department of Internal Affairs documentation which are not applicable." He concluded: "The only way to win back the support of the profession is through a concise change management process clearly lead by the Chief Archivist."

Up-dated ISO15489 is launched in Wellington: big improvement for RM standard

A new, vastly updated version of the international records management standard, ISO15489, is being released at a big gathering of world standards makers in the New Zealand capital, Wellington, in the first week of May.

The revised standard is being released before an invited big-wig delegation from New Zealand government agencies and ISO standards makers. Leader of the ISO15489 working group, Nederlands archives doyen, Hans Hofman, is scheduled to examine the changes he and his committee have fought over long and hard during the past five years and explain their impact on end-users.

ISO has, as usual, been slow to disclose much news before the launch, but the new chair of the Standards Australia Records and Document Management Systems committee, Barbara Reed, told the February 2016 edition of *iQ* (Vol 32, Issue 1) that the ISO work had focussed on appraisal and digitisation methodologies.

Hans Hofman

Barbara Reed

Highlight of gathering

The launch highlights the week-long gathering (9 to 13 May) of upwards of 100 world experts on information and documentation standards setting working with the subcommittees of the International Standards Organisation technical group for information ands documentation, TC46.

It will be the first time that the TC46 sub-committees have all met in New Zealand: Sub-committee 4 (SC4) on technical interoperability, SC8 concerned with quality statistics and performance evaluation, SC9 on identification and description and SC10 establishing requirements for document storage and conditions for preservation. SC11, author of the original ISO15489, published in 2001, met in Wellington in 2008 to develop their revision work.

The 2016 gathering will focus on the continuing development of many of the dozens of standards for which the subcommittees are responsible[5]. The groups will cover everything from international archives statistics (SC8), an international library item identifier (SC9) and a data exchange protocol for interoperability and preservation (SC4), SC10's work on management of the environmental conditions for archive and library holdings and SC11's implementation of further guidance for information management systems. The week's event begins and ends with plenary sessions reviewing overall developments and deciding next steps.

Vale: Lisa McDonough

By **Kristen Keley**, RIMPA Marketing & Convention Officer

It is with sadness that RIMPA also acknowledges the passing of Lisa McDonough on 3 April 2016.

Lisa was a valued member of the South Australian records management community and served on RIMPA SA Branch Council from 2009 to 2015.

She worked as a senior account manager at Recall, and in 2009 was awarded the Recall Global Salesperson of the Year.

Lisa was helpful, friendly and positive, even throughout her long illness which she fought with grace and determination. She made every day count and always had a smile and a laugh to share.

Lisa leaves behind a husband and three young children. Our thoughts are with her family and co-workers. As a friend and a colleague she will be greatly missed.

Irish public record embargo rule coming down to 20 years

The Irish Government is planning 'gradually' to reduce its 30-year State papers release rule to 20 years, putting it back into line with Britain's new schedules.

The republic's Minister of Arts and Heritage, Heather Humphreys, confirmed the plan earlier this year at an Irish National Archives event launching the design stage of an eight million Euros (Au$12m) extension to the institution's Dublin headquarters due to start in September.

The Minister stated: "Expanding and upgrading the National Archives is essential to cope with the increased demand that will come about as a result of this change and as we turn to resources held by the National Archives and other institutions to reflect and remember on the events of 1916 and beyond as the Irish State emerged from the Rising, and the Civil War."

Approximately four million files, containing an estimated 100 million pages will be stored in the new Archives building once it is completed. The National Archives stores a wide range of public material, including Government papers, Census records and files dating from the country's revolutionary period, including secret Royal Irish Police files and compensation claims made after the 1916 Easter Rising. ❖

Bibliography

1 The Conversation site: theconversation.com/au
2 Discontents blog: discontents.com.au/
3 #fundTROVE: anneliedevilliers.wordpress.com/
4 Archives New Zealand's Draft Regulatory Statement, Wellington, NZ, Dec 23, 2015, archives.govt.nz/advice/guidance-and-standards/draft-regulatory-statement.
5 TC46 subcommittee publications: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=48750

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

Next issue

The value of information

The August 2016 issue of *iQ* will feature a section on 'the value of information'. If you have a story to tell on this topic, or any other RIM related topic, we would love to hear from you.

Articles due: Wednesday 29 June

ENERGISE COMPLIANCE WITH COMMUNICATION

Having a communications plan – with regular communications about information governance (IG) and records and informaton management (RIM) – will enable the workforce to see IG/RIM as dynamic, a corporate priority and relevant to daily activities.

By **Craig Grimestad**

Communication? Yes, communication. We already touched on communications when we discussed that training will energise compliance (*iQ*, August 2015), but communication goes *much*, *much* deeper than that. There is such a tremendous benefit to having an ongoing communications plan, and regular communications about your IG/RIM program, that it is its own energising strategy.

I digress, but lack of communication can be devastating. In fact, lack of communication is often used as a heightened level of punishment. For penal institutions there is solitary confinement. No contact – no communication with others. A well-known institution calls its most severe form of punishment "excommunication" – no communication. Now no one is suggesting that organisations that do not communicate about IG/RIM are punishing their workforce, but if there is lack of communication, it is undermining your program.

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 blogs to: blogs.ironmountain.com/author/cgrimestad

Communication has two major components, the message and the delivery. It is important for the message to be clear, relevant and purposeful (hence the need for a plan). It is important that the delivery be timely, authoritative and across the company. Here are some thought-starters for message and delivery options to develop or enhance your plan.

Communication has two major components, the message and the delivery

COMMON IG/RIM MESSAGES

- **Value**: ie, the importance of IG/RIM to the organisation: What benefits does the company expect overall? What benefit is expected from the current initiatives?
- **Initiatives/goal setting**: What specifically are you asking departments and individuals to do? What is expected to be accomplished when the initiative or goal is complete?
- **Status**: What is the company's status in accomplishing IG/RIM initiatives and goals? What are the departments' statuses in accomplishing IG/RIM goals? This can be presented in a way that either directly or indirectly encourages competition between work groups, providing additional motivation to accomplish the goal.
- **Instructions**: ie, specific things to do to become compliant and stay compliant: How do individuals and departments get from their present state to the desired state and stay there?

COMMON DELIVERY METHODS

- **Say it**: Include an audible messaging component in your communications plan for keeping the workforce current with IG/RIM program messages. Messaging can be provided live, as video clips during company meetings, or as on-demand video clips. Establish an IG/RIM 'Speakers Bureau' to maintain a pool of speakers that are well informed and able to communicate IG/RIM messages periodically per your plan, and also on short notice as special needs arise. Include executives and organisational leaders in the Speakers Bureau.
- **Print it**: Utilise all forms of print including memos to staff, memos to workforce, newsletters, tip sheets, training manuals and desktop manuals.
- **Post it**: Utilise bulletin boards and other common posting locations for highly visible concise informative messages including flyers, notices, bulletins, graphs and charts.
- **Show it**: Utilise stand-up presentations, instructional video clips, hands on demonstrations and training.

Healthy IG/RIM programs are dynamic with a lot of moving parts. Hence, there is always something to talk about. Records are a company's greatest asset, so why shouldn't the company establish continuous IG/RIM communications as an ongoing strategy? Consider your communications plan as part of the necessary maintenance for these corporate assets. Regularly communicating about IG/RIM will enable the workforce to see IG/RIM as dynamic, a corporate priority, and relevant to daily activities. Utilising an appropriate mix of messages and delivery methods will energise your program and keep it at a high level of energy. ❖

Collaboration in the cloud

New Zealand Department of Conservation embraces content as a service to engage and empower its broader community.

By **David F. Carr** | Photography by **Mark Tantrum/Getty Images**

story snapshot

NEW ZEALAND DEPARTMENT OF CONSERVATION
doc.govt.nz

Headquarters: Wellington, New Zealand

Agency Function: Conservation, land management, and recreation

2015/2016 Budget: NZ$452,465,000

Oracle products: Oracle WebCenter Content, Oracle WebCenter Portal

MIKE EDGINTON
CIO (12-month secondment), and Director of Partnerships, Historic and Visitor Management

Length of tenure: Three years as director of Partnerships, Historic and Visitor Management, 25 years at DOC

Education: Diploma of Parks and Recreation, Lincoln University

Personal quote/mantra: “Design systems that motivate and drive the search for innovation in conservation management.”

The New Zealand Department of Conservation (DOC) manages 30% of the entire nation’s land area, plus offshore protected areas that could soon include one of the world’s largest marine sanctuaries. To meet that mission more effectively, the department will be tapping into collaboration in the cloud and improved search for internal documents. DOC maintains national parks, protects wildlife and ecosystems, and keeps the public informed about the environment. When hikers or backpackers go “tramping” through protected lands, it’s the Department of Conservation that warns them of the dangers of being caught in seasonal flooding. When debates flare over whether the introduction of honeybees has harmed the region’s ecology, or worries spring up about a plague hitting the nation’s bird population, DOC organises the scientific research. But the agency can’t do it alone.

“The job is much larger than the department, and much larger than the budget the government can put into it,” says DOC CIO Mike Edginton. “It requires a conservation community that is highly engaged and can make a considerable contribution beyond what the government can do in terms of conservation.” Particularly over the past five years, the department has made a concerted effort to work more closely with private conservation groups, universities, scientists, and other constituencies who share an interest in preserving natural habitats.

A big part of that cooperation is sharing research and data – “essentially sharing our systems,” Edginton says. “To do that with literally millions of documents and research articles, we needed a much better way of searching them and storing them.” DOC needed a new document management system, and Edginton’s team picked ContentWorX, a cloud content-as-a-service offering created specifically for the government by TEAM Asparona – a joint venture of two Oracle implementation partners, TEAM Informatics and Deloitte Asparona. DOC’s strategy for its new system shows how cloud offerings and cloud architecture are changing the way leaders think about new IT projects. DOC wasn’t ready to move to a public cloud platform, but Edginton and his team wanted a system architected and priced like a cloud service. They wanted the system to run in a government-managed data centre, but with the option of linking to other public cloud services. And they wanted the option to someday run entirely in a public cloud. The resulting initiative showcased a collaborative, problemsolving mindset – where government agency, implementation partner, and Oracle each applied fresh thinking to craft a new approach for the cloud architecture era.

A NEW AGE OF OPENNESS

DOC’s efforts also fit a strategic government push to share information more openly to increase productivity and connectedness. Though DOC is using a private cloud strategy today, Edginton expects to take greater advantage of public

The New Zealand Department of Conservation's Mike Edginton (left), CIO, and Allan Ross, Director of Transformation and Threats

⇛

cloud services in the future, particularly to share data for third-party collaboration. At the most basic level, ContentWorX helped reduce the risk that DOC would be found in violation of New Zealand's *Public Records Act*, says Allan Ross, DOC director of transformation and threats and the senior leader responsible for the ContentWorX implementation.

Under the law, the government has largely switched from "the assumption that information is closed unless we decide to make it open, to now saying it's open unless there is a damn good reason it has to be closed," says Ross. In the past, DOC couldn't produce documents quickly on demand because it had 2.3 million of them stored in folders with poor searching ability, Ross adds. With the new system's strong search capability (see sidebar, "Better Search Replaces Folders"), that information is much more readily accessible. Better information makes everyone, from cabinet ministers to DOC field personnel, better able to fulfill the DOC's conservation mission. "Every decision-maker, at every level, now has much better access to information and the documents they need to make decisions," Ross says.

ORACLE WEBCENTER IN A PRIVATE CLOUD

ContentWorX is based primarily on Oracle technologies, including Oracle WebCenter Content and Oracle WebCenter Portal. New Zealand government agencies can buy the service à la carte from a catalog of business application services, with cloud-style subscription pricing based on users per month. While Oracle offers its own software-as-a-service and platformas-a-service offerings on the same foundation of enterprise technologies, the government of New Zealand wanted a private cloud approach running on hardware in a government data center connected to the government's wide area network (WAN) – an "inside the firewall" configuration.

A second phase of DOC's ContentWorX project is in the active planning phase, which includes exploring the best way for DOC to selectively make documents available to volunteers, researchers, and other conservation partners. Employees will also get mobile access and the ability to securely access the repository from public internet connections.

> *"Every decisionmaker, at every level, now has much better access to information and the documents they need to make decisions."*
>
> *– Allan Ross, Director of Transformation and Threats, New Zealand Department of Conservation*

2.3 MILLION

Number of previously unmanaged DOC documents now searchable and accessible – an increase from 7.4% to 80% of all DOC content objects

30%

Share of New Zealand land area managed by DOC

14

Number of New Zealand's national parks, which DOC manages

Mike Edginton (left), CIO, and Allan Ross, director of transformation and threats at the New Zealand Department of Conservation, worked with Oracle and an implementation partner to create a new document management system.

⇛

"Eventually, we will be pure cloud," Edginton predicts. One way for DOC to provide that third-party access collaboration could be syncing between ContentWorX and public cloud file and document sharing services, potentially using Oracle Documents Cloud. DOCSConnect, a TEAM Informatics product offered through the Oracle Cloud Marketplace, makes it possible to synchronize Oracle WebCenter Content with Oracle Documents Cloud, while still enforcing an enterprise's access and security policies. The thorniest implementation challenge has been network performance problems that affected document search and retrieval, particularly for employees in remote offices.

"Some of it is just the size of the documents, combined with the bandwidth we're able to supply out to remote areas," Edginton says. "When you're trying to download very large documents, that gets very slow."

Part of the problem is that many of those field offices are on remote islands "halfway to Antarctica," notes Volker Schaberg, director of TEAM Informatics operations in Australia and New Zealand. Finding and addressing the root cause of the slowdown required a closer look at the government's WAN infrastructure. For example, the new content management system works over encrypted web connections—HTTPS, rather than HTTP—and the department's network acceleration hardware wasn't configured to optimise HTTPS traffic. Following an upgrade to those network optimisation devices, Edginton and Schaberg believe that the remote-office challenge has been mitigated. A network bandwidth upgrade in progress should also help.

Better search replaces folders

When the New Zealand Department of Conservation (DOC) implemented its new content management system, one of its boldest steps was shedding the traditional folder structure for electronic files, and instead relying on search for employees to find what they need.

The system implementer, TEAM Asparona, enabled that strategy by adding automated document tagging and classification to its cloud implementation of Oracle WebCenter, using a custom integration with Smartlogic's Semaphore software.

DOC mapped out a taxonomy of important terms to be used in the classification, amounting to some 95,000 terms and the relationships between them. Employees can add terms manually, but they generally shouldn't need to, since the vocabulary is designed to match the terminology commonly used within the department, says Volker Schaberg, director of TEAM Informatics operations in Australia and New Zealand.

The document analytics that power the automated tagging could in the future also help with information governance, for example by flagging sensitive information and classifying documents according to the government's disposal and retention rules. Meanwhile, Oracle WebCenter Content provides a rich audit trail of who created, edited, and accessed documents, with the option to revert to an earlier version if necessary without having to ask a system administrator to make such a change.

The biggest change, however, was moving away from placing documents in a hierarchy of folders. Some employees did miss the folder structure at first, says DOC CIO Mike Edginton, and they had to do some things differently. But the most-positive reactions quickly came from the people who matter most – "scientists and people who use documents a lot," Edginton says. With the ontology, "searches can be far more sophisticated and people are able to recover a lot more material."

SIMPLER SEARCH DRIVES ADOPTION

For DOC's ContentWorX solution, TEAM Asparona integrated Oracle WebCenter with Semaphore, a third-party autoclassification solution from Smartlogic. Semaphore automatically adds new metadata tags to records when they are saved into the ContentWorX repository, classifying according to their DOC-specific purpose (such as a conservation policy document or a supplier contract) and their DOC-specific contents (for example, conservation projects, locations, or groups). This means that users don't have to select the correct folder or manually add metadata when saving a document, and they can find a document or other content without knowing which folder it's stored in. With this ease of use, more than 95% of the DOC workforce regularly uses ContentWorX to support dayto-day needs, driving both user adoption and DOC's return on investment in ContentWorX.

Ross says it helped that TEAM Asparona was highly motivated to make the system a showcase it could use for other customers. He was also pleased at how much attention the Oracle team gave the project when his team asked for help. "This was a small project, and New Zealand is a small part of the globe for an organisation like Oracle," he says. Yet Oracle saw the potential to showcase Oracle WebCenter as a foundation for cloud computing and gave DOC high priority for technical support.

Another challenge turned out to be timing. DOC was among the first New Zealand government agencies to implement a cloud computing service on a large scale. Although the cloud approach is consistent with the New Zealand Department of Internal Affairs' IT policy, the oversight group hadn't nailed down all its data security certification standards by the time DOC was ready to go live with ContentWorX. "Because we didn't have the official government agreements in place, it left us quite exposed," adding a lot of stress, Ross says. "We did our own risk assessment to compensate."

FROM CONTENT TO COLLABORATION

One of the department's main reasons for adopting a new content management system is to enable collaboration with partners outside of government. But before creating a public login page for external collaborators, DOC needs to finish implementing the identity management infrastructure for authenticating outside users. Once that is in place, DOC is planning on "using the collaboration tools available in the system and putting documents into a publicly accessible web service," Edginton says. "That's what we've been designing for from the beginning, to provide access to all of the content and the search tools in the system."

How might public cloud services work for external collaboration? Edginton sees potential advantages in connecting ContentWorX to Oracle Documents Cloud, since they're based on the same underlying technology. However,

"Eventually we will be pure cloud," predicts Mike Edginton (right), CIO, with Allan Ross, director of transformation and threats, at the New Zealand Department of Conservation.

he would also like to build bridges to services such as Google Drive, upon which some DOC partners such as universities have standardised.

Selectively synchronising ContentWorX content with public cloud storage would also widen the circle of potential collaborators who can access DOC's content, Schaberg says. Partners outside government can only get online access to the content today by getting an account on the government network as if they were employees.

Researchers at the University of Otago, for example, have access to ContentWorX because they play an important role in DOC programs. However, granting that kind of system access requires a great deal of trust, and it's not a model that scales to encompass all the private conservation and community groups DOC would like to engage with. If documents classified as public information could be replicated to a public cloud service, access to that content could be granted much more readily, he says.

Another important scenario for hybrid cloud use would be sharing documents with specific people but not the general public, such as in contract negotiations. While it's still common for businesses to handle drafting and signing of contracts by email, "that's a very insecure and inefficient way to do it, where you lose the audit trail," Schaberg says. "A much better way would be for me to put that document in a folder on Oracle Documents Cloud Service and then share that folder with you." The parties to the contract can then mark up the document, exchange updated versions, and finalise it with a digital signature.

Though further decisions remain, DOC is off to a good start. Edginton describes it as a "large, audacious stretch goal" to ensure that DOC could facilitate document sharing with others looking to do conservation work with the department. To do it right, he says, "we needed to find tools that were appropriate and hopefully future-proof. We see that with Oracle, ContentWorX, and the other things that come with the Oracle platform." ❖

This article was first published in *Profit* magazine, February 2016.

ABOUT THE AUTHOR

David F. Carr is a freelance writer, a student of digital business, and the author of *Social Collaboration for Dummies* (Wiley, 2014).

ACTION ITEM
Scan to learn more about the Oracle solutions featured in this story.

New Victorian Protective Data Security Standards roll-out: will you be at the table?

Following the introduction in 2014 of the *Victorian Privacy and Data Protection Act*, new Protective Data Security Standards have been developed. As information managers, it's important to ensure that you are at the table when the rollout of the new Standards takes place within your organisation.

By Alison Toohey

story snapshot

The release of the new standards will mean significant work in terms of compliance.

As a skilled information manager, it's important for you to understand the requirements and what it means for your data security team.

On 17 September 2014, the *Privacy and Data Protection Act 2014 (Vic)* (PDPA) came into effect. The PDPA has been implemented to address the security of information and privacy in the Victorian public sector.

It provides for responsible handling and collection of personal information, and has initiated the establishment of a protective data security regime for public sector data managed within the Victorian public sector[1]. Part of this regime included the merging of two previous commissioner roles – Privacy Commissioner and Commissioner for Law Enforcement Data Security – into the Office of the Commissioner for Privacy and Data Protection (CPDP).

Under Part 4 of the PDPA, CPDP has been tasked with developing the Victorian Protective Data Security Framework (VPDSF), which is made up of the Victorian Protective Data Security Standards (VPDSS or 'the Standards') and an Assurance Model, which is currently being finalised. Approval and formal issue of the VPDSS is expected in 2016.

The VPDSS is comprised of 18 standards. Each standard provides a 'statement of objective' which is supported by four mandatory protocols. The four protocols provide a 'plan, do, check, act' structure to each standard enabling organisations to implement continual improvements as required.

Controls listed for each standard provide information on the correlation of the standard with other materials that should be referenced when assessing your organisation's adherence to the standard.

The Standards fit within the following five domains:

- Governance
- Information security
- Personnel security
- ICT security
- Physical security

Within the governance domain, the Standards address:

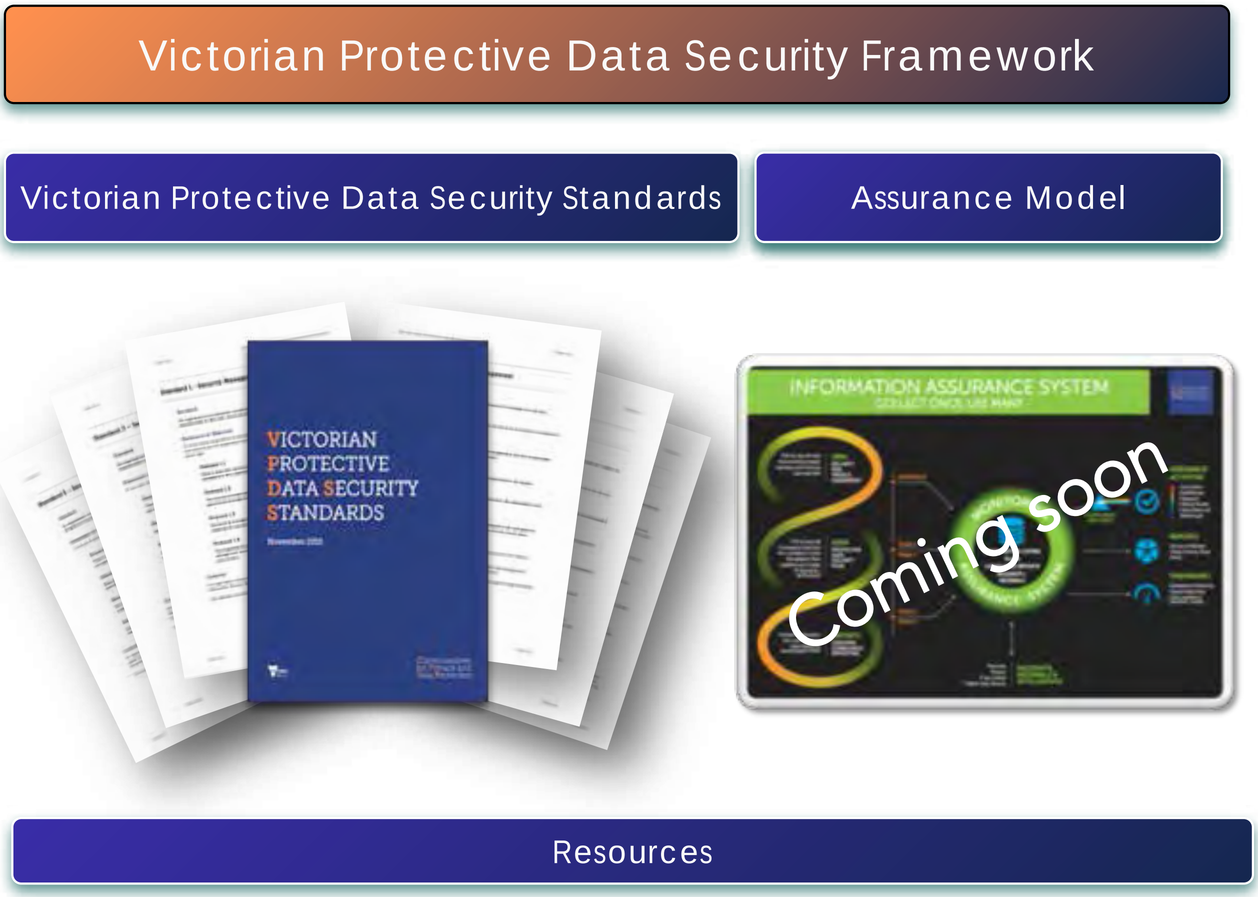
- establishing a security management framework
- enhancing current risk management frameworks and policies and procedures ensuring the element of security is identified
- implementing secure management of access to information
- including security aspects within organisations' training and awareness programs
- establishing governance around public sector data that is accessed or used by contract service providers
- ensuring compliance with the VPDSS by undertaking annual assessments of the implementation of the Standards.

The Information Security Standards deal with establishing controls around access to information and data, identifying the value of organisational information which allows for prioritisation of information protection.

The Personnel Lifecycle standard considers all persons eligibility and suitability to access and use information.

ICT Security requires robust controls within ICT management, as does Physical Security for its management regime.

The Assurance Model will enable a monitored and measured approach to the implementation of the VPDSS. The relationship of the VPDSS and Assurance Model as the foundations of the VPDSF with support from resources is represented by the following diagram:



Victorian Protective Data Security Framework

Victorian Protective Data Security Standards

Assurance Model

VICTORIAN PROTECTIVE DATA SECURITY STANDARDS
INFORMATION ASSURANCE SYSTEM
Coming soon

Resources

Victorian Protective Data Security Framework[2]

WHAT DOES THIS MEAN FOR INFORMATION MANAGERS?

Part 4 of the PDPA sets out applicable organisations. Your organisation (Victorian Government or private sector handling public sector data) should identify if it is an applicable agency or body under the Act and commence discussions on what adoption of the Standards will mean for you.

At the Water Industry Information Management Special Interest Group conducted in March, we were fortunate enough to have Anthony Corso, Assistant Commissioner – Data Protection, and Laurencia Dimelow, Senior Data Protection Advisor, from the CPDP present on the rollout of the VPDSS. It gave us the opportunity to identify what information/records managers should expect to be doing to help implement the Standards within their organisations.

One of the most important pieces of advice for information/records managers is to leverage a combined approach to assessing and developing an action plan for compliance with the VPDSS. This means ensuring you are 'at the table' and included in any working groups or discussion on the implementation of the Standards.

As information managers, we have the skills that our organisations need to help with some of the first steps in applying the Standards. The key steps include:

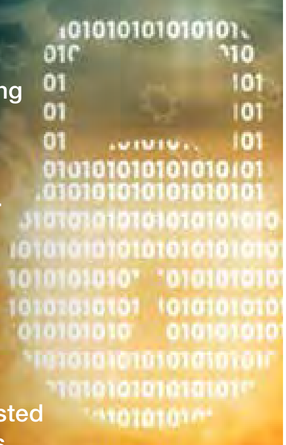
- identifying your information
- assessing your information
- valuing your information.

These steps are critical to commencing a successful program and information managers should ensure that they are included in this process, given that many of us have undertaken these tasks to a certain extent already when working towards compliance with PROV Standard PROS 10/17 – Operations Management.

> *A key component of identifying your information in readiness for the application of the Standards is the creation of an information asset register*

Privacy and Data Protection Week

PDP Week is being held from 9 to 13 May and the CPDP is hosting a number of events throughout the week, including general information sessions about the work of the office (co-hosted with the Freedom of Information Commissioner and the Health Services Commissioner), a specialised information sharing seminar, and two public forums: one on de-identification and one on smart cities. If you are interested in attending any of the events, please check the CPDP website or get in touch with the office for further information.



Identifying your information

A key component of identifying your information in readiness for the application of the Standards is the creation of an information asset register.

Many information managers have possibly already created a vital records register in accordance with PROV Standard PROS 10/17 – Operations Management: identifying what records in their keeping are vital, what format the records take, and where the records are. This could act as the base document in identifying your organisation's information and allow other members of your working group to add to this, identifying other information sources that need to be included for assessment. This document is of value to your organisation when addressing Standard No. 13 – Information Value. The Standard states "…An organisation must conduct an information assessment considering the potential compromise to the confidentiality, integrity and availability of public sector data…"[3].

The information asset register becomes a more in-depth document that not only identifies your information but also acts as a means to highlight the importance and value of this information to your business.

Assessing your information

With a register of information your organisation is holding, you will then be able to assess your information and provide a clear picture of the overall value of the information. To make an assessment of information, consideration must be given to the confidentiality, integrity, and availability of the information.

Valuing your information

The ability to generate an overall value or rating as an identifier for your information allows you to prioritise the information you are holding, and therefore more accurately manage the risk associated with each type of information. Identifying the risks then enables you to apply appropriate and proportional security measures.

THE SKY IS FALLING … OR IS IT?

Like Henny Penny in the classic children's fable who was convinced that the sky was falling, our initial reaction may be to panic about the amount of work that may be needed to ensure compliance with all of the VPDSS. Organisations will need to consider resources available; cost to implement, update, or upgrade security assets; as well as the time it will take to implement these changes. It really does seem like the sky is falling! However, it isn't as bad as it may seem. CPDP have instigated a three-year timeline for the ongoing implementation of the VPDSS in the Victorian public sector.

2016 will see the formal release of the VPDSS under which organisations will need to operate. The CPDP will grant a two-year period to enable organisations to develop a Security Risk Profile Assessment (SRPA) and Protective Data Security Plan (PDSP). The SRPA and PDSP can be thought of as the risk identification and risk treatment plan respectively. They are based on existing risk management practices.

In 2017 organisations will be expected to have developed their SRPA with outputs that identify any remedial activities. It is these outputs that will then be fed into the PDSP.

Organisations will then be required to submit their PDSPs in 2018 to the CPDP. Organisations can then continue to address the risks and gaps that have been identified and submitted to the CPDP in their PDSPs.

This timeline demonstrates that compliance with the VPDSS is not expected to occur without a generous lead-in time. This will allow organisations to plan for compliance realistically as they develop their SRPAs and PDSPs.

MAKING IT HAPPEN TOGETHER

Significant emphasis is being placed on ensuring that various parts of an organisation are working together to implement the necessary changes. Key areas within your organisation that should be involved in the development of your plan are as follows:

- Legal
- HR
- Facilities
- Information Management
- ICT
- Finance
- Risk Management
- Governance.

All of these areas have a key role to play and have different skill sets required to identify information they manage, risks that are present, and how governance and technology can be leveraged to ensure that an increased importance on security of data and information within organisations becomes embedded in the day-to-day practices of the organisation.

The CPDP will also be working with organisations to ensure they have as much assistance and resources as possible to enable them to effectively assess their information, create their SRPA, and provide the CPDP with their PDSPs.

This means that the CPDP is working hard on creating tools and resources to help organisations to step them through the process.

These tools will include:

- an assurance model, which is part of the foundation of the VPDSF. It is still being finalised and will be an important tool in assisting in monitoring and measuring the rollout of the VPDSS within your organisations
- guidelines to assist with assessing and understanding each of the standards. These will continue to be developed and made available
- applications to assist with working through the assessment, including:
  - the CPDP App, which will include content from the Privacy, Protective Data Security and Law Enforcement areas of the CPDP
  - a second app that will assist users to assess likely impacts arising from a compromise of the confidentiality, integrity, or availability of information using Business Impact Levels (BILs).

VPDSF Applicability

In August 2014, CPDP along with the Victorian Public Sector Commission (VPSC) and Victorian Government Solicitors Office (VGSO) identified public sector organisations that are captured under Part 4 of the *Privacy and Data Protection Act* as 'applicable organisations', including public sector agencies, 'special bodies', a body declared by the Governor in Council, and contracted service providers that are dealing with, or have access to public sector agency data.

The VPDSF does not apply to local councils, universities, public hospitals, ambulance service, or government bodies or appointed persons of another government jurisdiction.

Within these exceptions, however, it is important to understand that your organisation may still be dealing with public sector data that has been shared with you and the protection of that data needs to comply with the VPDSS.

The standards in the VPDSS could also assist councils when working to meet their requirements under IPP 4 (Data Security) of *the Privacy and Data Protection Act 2014*, when dealing with personal information.

In addition, CPDP will consider conducting sessions on how to value information.

As information managers, we can be proactive in identifying where our skills can contribute to the implementation of the VPDSF, where and when we can impart our knowledge, and knowing what assistance will be available to support organisations to ensure that the process is successful. The key message should be to ensure that you are sitting at the table, included in discussion and workshops, and are a part of the rollout of the VPDSS within your organisation. ❖

Assistance can be provided by the CPDP by using the e-mail security@cpdp.vic.gov.au , or using the enquiries number – 1300 666 444 – to provide feedback and comments.

Bibliography

1 Media Release – Privacy by Design: How to manage privacy effectively in the Victorian public Sector. 20 November 2014 – Office of Commissioner of Privacy and Data Protection

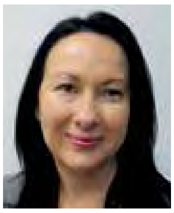
2 Presentation: Victorian Protective Data Security Framework (VPDSF) – Information Management Special Interest Group – 3 March 2016

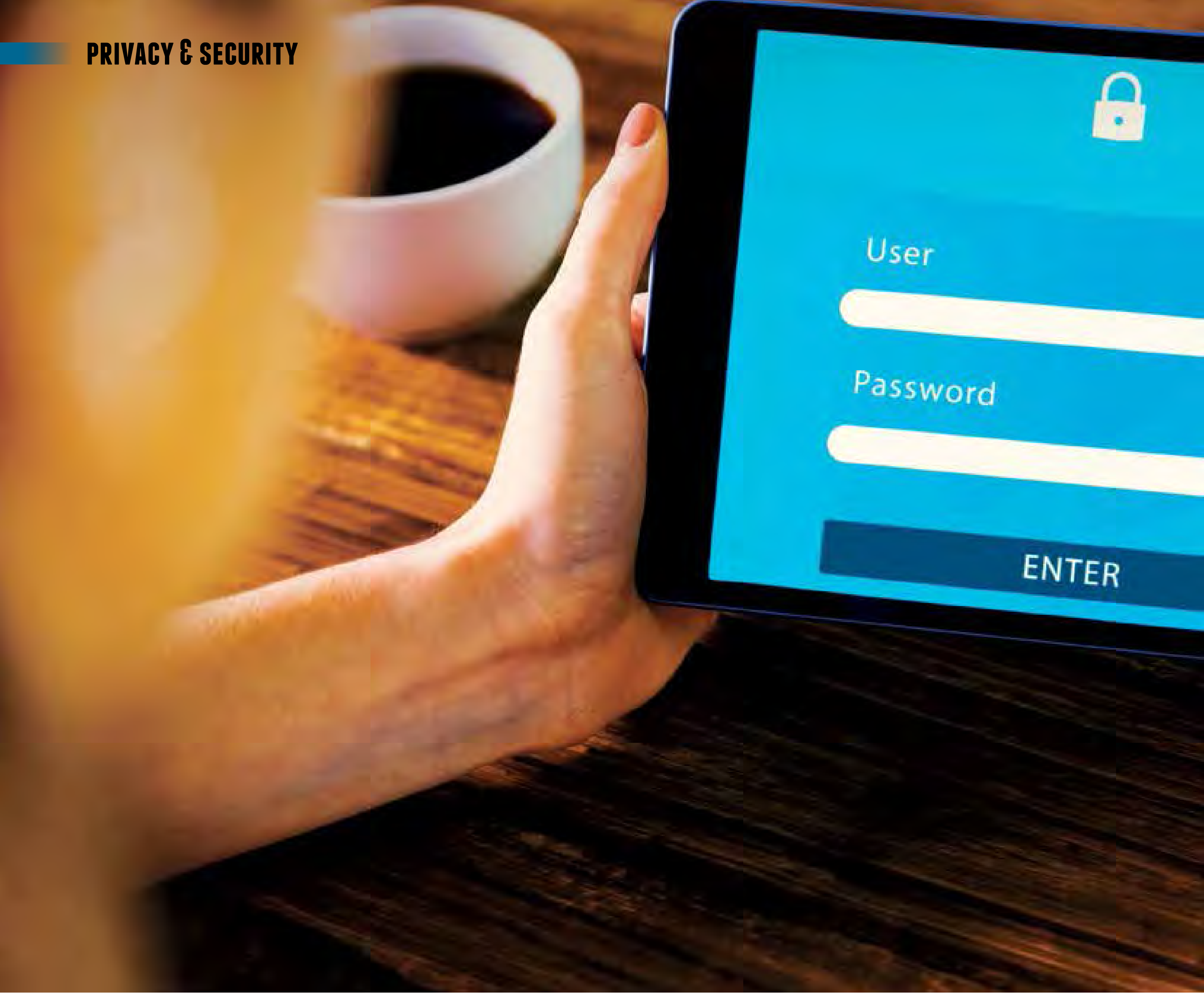
3 Victorian Protective Data Security Standards (VPDSS) – Standard 13: Information Value – Office of Commissioner of Privacy and Data Protection

ABOUT THE AUTHOR

Alison Toohey ARIM is Records Team Leader at Wannon Water. Alison has worked in record keeping within the water industry for nine years. She spends her time working on project delivery and is currently involved in an EDRMS upgrade. She also works closely with team members to provide functional and useful record keeping and EDRMS training to Wannon Water employees, and identifies methods to enhance the end-user experience when working with organisation information.

✉ She can be contacted at alison.toohey@wannonwater.com.au





PRIVACY AND SECURITY IN OUR COMPLEX DIGITAL WORLD

In an era where digital footprints, digital shadows and dark data pose a new set of challenges for privacy and cybersecurity, how we continue to manage the changing landscape and moving goal posts is a topic worthy of discussion.

By **Linda Shave**

The protection of individuals, the state and its secrets, and indeed countries themselves against pilfering, fraud, and espionage attacks is not new – and history suggests this will continue to be an issue.

Privacy is very often united with security; however, they are two separate concepts. Privacy is about the appropriate collection, use and sharing of personal information whereas security is about protecting such information from loss, or unintended or unauthorised access, use or sharing.

THE ANALOG ERA

Let's take a step back in time to the old physical paper folder in the days of the Cold War espionage, spies, secret files and intelligence gathering. Physical folders came in different colours representing different levels of security. For example, a red folder might represent 'top-secret' or a vanilla folder with a red hallmark stating secret, private, classified, confidential or personal stamped on it marked their importance. These files could be considered the 'hush-hush' files; security was by means of locking them away in filing cabinets for safekeeping and these filing cabinets sat within protected rooms. The aim of keeping these files secured was to protect individuals' privacy and state secrets from theft and espionage attacks.

Risk management and governance were managed by means of your role, responsibilities and accountabilities. Compliance was determined by Acts, rules, regulations, policies and procedures which detailed, for example, who had access rights to the secured room and filing cabinets, who could sign in and out these folders, who could view the folders, the management of the destruction of carbon paper, typewriter ribbons, telex machine tapes, shorthand notebooks etc. All of these precautions provided the framework for security and privacy protection and carried various penalties for failure to adhere to such instructions.

Let's fast-track a little to the demise of the typing pool and the introduction of on-premise business systems such as word processing and electronic document record management (EDRM) systems. Security and privacy activities and functions did not change too much; the main difference was the replacement of carbon paper, typewriter ribbons and shorthand notebooks with floppy disks. Floppy disks were stored away in secured fire proof cabinets and physical folders remained the same.

The EDRM system replaced the old manual folder register for the creation, tracking and managing of physical folders. Further along the evolution road, floppy disks where replaced with hard disks, network servers and the establishment of Enterprise Content Management (ECM) systems which captured, stored, managed and protected records. Security within the ECM system was managed by record and information professionals by way of establishing controls and access rights to folders and records. The protection to business systems became the domain of the Information Technology (IT) departments who sat in a secured environment behind glassed doors and whose primary role was to prevent illegal access by providing the appropriate security and access permissions.

MOVING TO THE DIGITAL AGE

We now live in a digital age, in which things that used to be real and tangible are now machine generated or only exist in bits and bytes. Governments and the enterprise are transitioning agile cost-effective cloud deployment models and cloud offerings such as Software as a Service (SaaS). As government and the enterprise move to cloud business solutions, there is a new evolving challenge, government and business are leaving a 'digital footprint'. The digital footprint of the enterprise will continue to grow and so too will the issues around privacy and security. Old legacy IT security approaches consist of a set of highly fragmented technologies that only allow detection of security breaches and attacks once they are already inside the network. The handling of security has now expanded far beyond the domain of the IT department.

> *Risk management and governance was managed by means of your role, responsibilities and accountabilities*

PRIVACY AND SECURITY IN THE DIGITAL AGE

Privacy may have different meanings due to factors such as context, prevailing social standards, and geographic locations. There is no agreed definition of privacy which can make it challenging to debate. However the predominant concept persists that 'privacy' is the appropriate collection, use and sharing of personal information to accomplish business tasks.

Although privacy and security are two separate concepts, the importance of these two ideas intersects for the customer if their personal data is not safeguarded. Risk management for data privacy and security of that data should be safeguard against external malicious breaches, inadvertent internal breaches and third-party partner breaches.

WHAT IS PERSONAL DATA IN THE DIGITAL AGE?

Personal data stem from three data types; these are self-reported, digital exhaust and profiling data (see Table 1).

TYPE	DESCRIPTION
Self-reported data	Information people volunteer about themselves, such as their email address, work, education, age and gender.
Digital exhaust data	For example, location data, browsing history which is created when using mobile devices, web services or other connected technologies.
Profiling data	Personal profiles used to make predictions about individuals' interests and behaviours which are derived by combining self-reported, digital exhaust and other data.

Table 1 – Personal data types in the digital age

Personal data is described in privacy and information security circles as information that can be used on its own or with other information to identify, contact or locate a single person or to identify an individual in context. With the advent of rich geo-location data and associative analysis such as facial recognition the magnitude of personal data collected is greatly expanded and so are challenges for security in protecting such information from loss, or unintended or unauthorised access, use or sharing. Coupled with this, a further privacy challenge is the need to comply with a range of conflicting regulations on privacy, especially as privacy regulations can vary by region and country.

THE INTERNET OF THINGS

The concept of the Internet of Things (IoT) was introduced in 1999 and evolved from the machine-to-machine (M2M) technology that originated in the 1980s, in which computer processors communicated with each other over networks. The major difference today is that modern technology devices cannot be considered processors, but rather sensors and relays that simply facilitate the aggregation of data. As IoT continues to advance the interconnectivity between information sources and individuals, and technology continues to drive connectivity, cloud, data analytics and mobility, the concerns about personal privacy and the security of private information will continue to grow. Therefore, we must look at new models to deal effectively with security and privacy.

DARK DATA

Government and the enterprise continue to collect, process and store massive amounts of structured and

unstructured data as an outcome of business activities. As time passes the information becomes disjointed, the meaning for which it was collected is lost, records are forgotten and files are lost within the organisation's digital repositories. This significant group of uncontrolled information is escalating and is referred to as 'dark data'.

Dark data consists of information assets that are normally created and used once, such as log archives, zip files, project folders, duplication and even active data which becomes inactive and overtime is forgotten. The enormous volume of data being created, captured and stored is ever-increasing and as a consequence dark data is growing. Dark data can include confidential, personal or sensitive information and presents a challenge for security, privacy and compliance.

There are, however, opportunities to make sense of dark data. As record and information professionals, this is a possible new opening for our jobs for tomorrow – that is, as 'dark data' miners armed with data analytic tools and business intelligence.

DIGITAL FOOTPRINTS AND DIGITAL SHADOWS

Governments and the enterprise collect an inordinate amount of information from citizens and customers in the delivery of their products and services. When delivering these services governments and the enterprise create 'digital footprints'. Citizens and customers as consumers of these products and services leave 'digital shadows' – this is personal data left behind by transactions and interactions on the internet, applications, and across other connected devices and sensors.

For clarification, a digital footprint is information that is projected, shared and managed by both public and/or private enterprises. While this footprint can be beneficial, information can be unintentionally exposed through the enterprise footprint; thereby it could be used maliciously and put at risk the security and privacy of information assets. A digital shadow, on the other hand is a subset of a digital footprint. A digital shadow consists of exposed personal, technical or organisational information that is often highly confidential, sensitive or private. A digital shadow can leave the consumer of products and services vulnerable to cyber stalkers and hostile groups exploiting the digital shadow to find an organisation's (the provider of the product or service) weak point to launch targeted cyber-attacks and plant a malicious insider.

…it is essential that the products, information and services shared in the cloud are protected from security and privacy breaches

Digital footprints and digital shadows are growing and, as providers and consumers of products and services, so is the information being collected about you – the individual and/or the organisation. This vulnerability raises another set of challenges for security and privacy for both the individual and the enterprise.

ENTER THE MALICIOUS INSIDER – THE SPY WITHIN

As previously mentioned, government and the enterprises are moving to cloud-based business solutions and cloud offerings such as Software as a Service (SaaS). However, due to the very nature of the internet, cloud, mobile and social technologies are inherently oriented towards the sharing of resources. Consequently, it is essential that the products, information and services shared in the cloud are protected from security and privacy breaches. Make certain that appropriate steps are taken to ensure that policy and procedures for security and privacy protection are in place to counteract pilfering, fraud, and espionage attacks from within the cloud. Government and the enterprise need to be fully aware of third party providers' responsibilities and accountabilities around how they are managing security and privacy risks. Without full knowledge and control, your organsiation may be at risk of data loss and leakage, account hijacking and, worse, the malicious insider.

⇛

The malicious insider is the 'spy' or 'traitor' who represents an inside cyber threat. The malicious insider has access to the enterprise network from inside the perimeter barricades. Malicious insiders know about the organisation information systems, its structure, the people and its internal operations. They are like a rogue administrator who can access your sensitive data, steal information, steal private details and perform any number of other malicious activities.

There is a need for new enterprise governance models to adopt a pro-active perspective for cyber security, privacy and risk management against external malicious breaches, inadvertent internal breaches and third-party partner breaches.

RISK MANAGEMENT, GOVERNANCE AND CYBERSECURITY

Effective risk management, governance and compliance are enablers to ensuring that the security framework of people, policies and technology are consistent and measurable across the entire enterprise. Cybersecurity is defined as the protection of systems, networks and data in cyberspace. Therefore, cybersecurity will become a key component in the process for the identification, analysis and mitigation of risks to information assets.

Understanding, the concept of cybersecurity and associated privacy implications might enable record and information professionals to become part of future digital project teams. This might become more apparent as traditional EDRM/ECM models for record keeping and record management move to the cloud and new tools such as data decision making and active preservation are incorporated into daily activities for record and information management.

As previously indicated, the handling of security has now expanded far beyond the domain of the IT department. Therefore, addressing evolving security challenges will require inserting cybersecurity into both the IT security framework and record and information management policies and procedures.

ABOUT THE AUTHOR

Linda Shave is acknowledged as a thought leader and architect of change. She is a researcher, consultant and auditor in areas of virtual information asset management, business process management, cloud migration, corporate governance and risk management. Linda is a former CEO, CIO and a member of numerous professional organisations.

✉ She can be contacted at linda.shave@bigpond.com

PRIVACY BY DESIGN

The concept of building privacy by design (PbD) into business solutions is not new! Its focus is on integrating and promoting privacy requirements and/or best practices into systems, services, products and business processes. It is essential to do this at the planning, design, development and implementation stages to ensure that businesses meet customer and employee privacy expectations. This may present record and information professionals with an opportunity of being involved in the PbD process.

BACK TO WHERE WE STARTED

As previously mentioned government and the enterprises are moving to cloud-based business solutions and cloud offerings such as Software as a Service (SaaS). Traditional EDRM and ECM models for record keeping and record management are also transitioning to SaaS solutions in the cloud as well as cloud vaults for the capture, storage and management of records and information assets. Security within the cloud ECM as a service can still be managed by record and information professionals by way of establishing controls and access rights.

However, the security and protection of the cloud vault may rest with your third-party provider. As record and information professionals you will need to be fully aware of the third-party provider's responsibilities and accountabilities around how they are managing security and privacy risks around your records and information assets. Also, make certain that records and information assets ownership and the geographical location of storage are clearly articulated and that you can get your records and information assets back and/or migrate them to a new provider if needed.

Intellectual property is another key concern when it comes to cloud services. In some cases cloud providers own the infrastructure or the applications, while the user owns the data; this demarcation is not always clear. For example, open source software often combines data and code, and it is not always clear who owns the rights to what.

As previously defined, privacy is very often united with security; however, they are two separate concepts. Privacy is about the appropriate collection, use and sharing of personal information whereas security is about protecting such information from loss, or unintended or unauthorised access, use or sharing. We have already glimpsed from above that digital footprints, digital shadows and dark data pose a new set of challenges for privacy and cybersecurity.

There is indeed a lot of food for thought around cybersecurity, privacy and risk in our digital world and how we continue to manage the changing landscape and moving goal posts. This topic deserves future round table discussions, not only within record and information management circles but with our colleagues in IT, risk management, auditing and security. ❖

MANAGING CHANGE IN INFORMATION SECURITY

The annals of information management are replete with tales of lost and stolen information. Organisations need to guard against this by cultivating a high level of security maturity. And to achieve this, a change in behaviours for employees is required. In leading that change, records and information mangers need a clear and effective change management plan.

By **Michelle Linton** & **Kevin Dwyer**

In May 2006 an unencrypted national database on a laptop, with names, social security numbers, dates of births, and some disability ratings for 26.5 million veterans, active-duty military personnel and spouses was stolen in the US. Veteran's Affairs estimated it would cost $100 million to $500 million to prevent and cover possible losses from the theft.

In August 2006 data on more than 20 million web inquiries, from more than 650,000 AOL users, including shopping and banking data, were posted publicly on a website.

In 2013 Vodafone Germany admitted that a person with insider knowledge had stolen the personal data of two million of its customers from a server located in Germany.

In 2014 an employee from personal credit ratings firm Korea Credit Bureau was arrested and accused of stealing the data from customers of three credit card firms while working for them as a temporary consultant.

As it can be seen, the annals of information management are replete with tales of lost and stolen information. In managing information security, organisations not only need to guard against this all too frequent loss of confidentiality and integrity of information lack of availability, but also against the lack of accessibility of information to those with a right and a need to know. It is also incumbent upon organisations to guard against fraud and disclosure of sensitive information by allowing individuals with incident history to be in trusted positions. All of the foregoing requires effective controls enabled by a high level of information security maturity.

Many organisations have a low level of information security maturity, failing to align significantly with standards such as ISO27001/27002. In order to improve their maturity, organisations need to embark upon the definition and implementation of an Information Security Management System (ISMS).

⇛

The benefits of doing so include, but are not limited to:

- an understanding of the ongoing investment required as an organisation to appropriately manage information security risks
- a coordinated approach reducing the costs of information security
- adequate information to make informed decisions about managing organisational security risks.

Much of the effort in creating such a system involves building a security architecture and processes across network hardware and software outside the scope of a records and information management system. However, the importance of security management within a records and information management system within an overall information security management system is very high.

Whereas the management of change affecting network hardware and software requires a small number of people to change their habits and practices, the changes in a records and information system to improve the maturity of information security requires major changes in behaviour across the whole of the organisation.

DEVELOPING A CASE FOR CHANGE

The case for change in implementing an information security management system emanates from managing risks to brand, physical, financial and intellectual property assets.

The benefits in making the change include reducing the prevalence of:

- reputation loss stemming from incidents including loss of service
- regulatory non-compliance eg, privacy
- revenue loss eg, through protection of intellectual property and strategic plans or loss of service
- discontinuity of business processes eg, after natural and man-made disasters.

In order to deliver on those outcomes, an information security management system change management plan must deliver on five key changes:

- making staff aware of information security as subject they should be interested in
- making staff aware of information security policies and procedures and their responsibility in executing those policies and procedures
- changing employees' habits in their approach to information security
- motivating managers to assess and evaluate their information security risks, and building appropriate response to reduce the risk to an acceptable level as within the information security management system framework
- changing the perception of line management of information security in order to embed information security in their day-to-day processes and their business planning and evaluation processes.

If individuals do form the intention to change their behaviours, but line managers are not engaged, pockets of individuals do form, albeit short lived, changes in behaviours. The approach is not sustainable.

In order to create the environment where people do change their behaviours, the change management plan must be effective at two levels (Fig 1):

- creating an intention in individuals to change their behaviour
- ensuring that line management are engaged enough in the change to help individuals turn that intention into action.

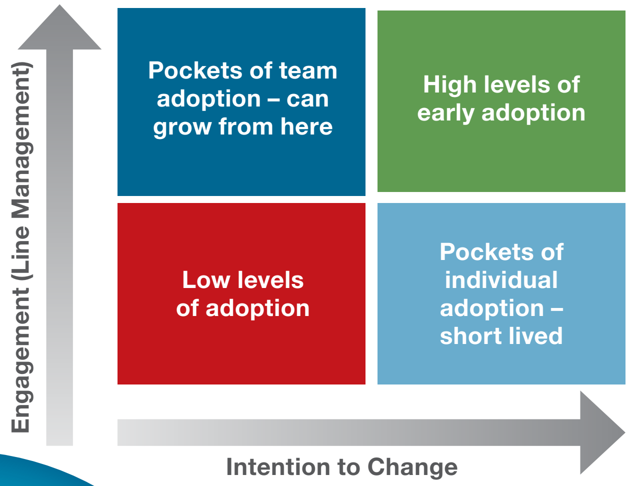

Engagement (Line Management)
Pockets of team adoption – can grow from here
High levels of early adoption
Low levels of adoption
Pockets of individual adoption – short lived
Intention to Change

Figure 1: Change management plan objectives

When the change management plan delivers neither an intention to change nor line management engagement, low levels of adoption of improved security practices is ensured.

If individuals do form the intention to change their behaviours, but line managers are not engaged, pockets of individuals do form, albeit short lived, changes in behaviours. The approach is not sustainable.

Alternatively, when managers are engaged, even if individuals have not independently formed an intention to adopt new practices, charismatic leaders can make it work. The changes resulting from this environment are much slower though, and with many more missteps than when individuals form the intention to change practices and line managers are fully engaged.

CHANGING INDIVIDUAL BEHAVIOURS

Changing people's behaviour is hard work. Organisations which attempt to change people's behaviour usually do not achieve as much change as they would like. One of the reasons is that the process used does not enable change at a personal level.

Organisations which typically rely on a 'change management program' which is a linear project plan of events such as process redesign, standards, key performance indicators and some training, which whilst they are good tactics to use, miss an important aspect of change which is the need to change people's behaviour.

A very useful behavioural change framework is provided by the 'Theory of Planned Behaviour' developed by Ajzen (Ajzen, 1985).

According to Ajzen, intention, as the precursor of human behaviour, is guided by three considerations: behavioural beliefs, normative beliefs and control beliefs (Fig 2).

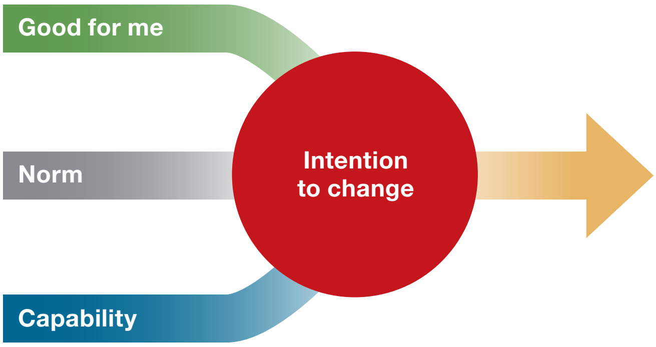


Figure 2: Forming the intention to change (Ajzen)

Behavioural beliefs produce a favourable or unfavourable attitude toward the behaviour. For example, unless an employee believes good information security practices are good for the organisation and themselves, then they are unlikely to change their behaviour. In addition, the employee needs to believe that good information security is better for them than other behaviours that also bring benefits.

Normative beliefs result in subjective norms. For example, if an employee believes that all of his or her colleagues actively support and, especially those they respect, are engaged in good information security practices, then they are more likely to form the intention to do so themselves.

Control beliefs give rise to perceived behavioural controls. For example, if an employee believes they do not know how to adopt good information security practices or that good information security practices are too hard to adopt or that their manager does not rate good information security practices as a priority for them, they are unlikely to form an intention to adopt good information security practices.

Ajzen also notes that actual control and intention form the basis of actual behaviour. This means that staff must be observed to determine whether their perceived control is real and adjustments made if it is not. For example, a person may perceive they have authority to make changes in the way they conduct their business life. However, in reality, their manager controls what they do to such an extent that they have no real authority to make the changes. When they attempt to make the changes in line with their schedule of authorities, their manager stops them making the changes through the force of their personality.

BEHAVIOURAL BELIEFS AND ATTITUDES

For an information security management system program, it is our observation that most people are convinced that good information security practices are desirable. If not, the global levers at our disposal include:

- senior management support
- outstanding audit findings
- examples of information security case studies within and outside of our organisation.

All of these levers can be brought to bear by spreading their understanding amongst the existing low intensity practitioners of information security and potential new practitioners.

What is less certain is our ability to convince individual and team members, using the generic levers described above, at or below branch level, that they should care more about good information security practices than maintaining existing practices that have generated other benefits for them.

For this reason, the change management plan must include a means by which good information security practices are seen as desirable over the status quo at branch level or lower, in addition to the global reasons why the change is desirable.

To change people's beliefs about the desirability of good information security practices we must first raise the issue of the belief in their consciousness; human beings are only capable of holding a few beliefs in their consciousness at one time.

That means a campaign about the topic of information security. The campaign components may include such elements as:

- policies, processes and standards showing how to keep information secure in easy to access and assimilate formats
- an awareness campaign about information security using multiple mediums including video, briefings, face-to-face learning, web pages, brochures, posters, newsletter articles, case studies, quizzes and competitions for the best branch/team or the most improved branch/team.

To change the perception of the desirability of good information security, we may consider:

- a reward and recognition program that rewards the achievement of implementation milestones such as:
  – completing training
  – planning implementation of an ISMS
  – completing implementation of an ISMS
  – using an ISMS effectively or innovatively
- a feedback process that praises or criticises, dependant on the level of deviation from the desired standard of information security
- coaching for people to plan and implement good information security practices
- inclusion of the ISMS milestones in individual manager scorecards, if necessary, matched to the implementation project plan timing.

NORMATIVE BELIEFS AND SUBJECTIVE NORM

To create a set of beliefs of what is normal in good information security practices, there are three elements to consider:

1 Changing the exposure to groups which symbolise what good information security means and its impact on the organisation – for example:
- increasing the degree of interaction between individuals/teams and people who are impacted upon by poor information security in their branch/division
- having people addressed regularly by senior managers on what and why they care about good information security practices and the progress being made
- training people explicitly in the desired behaviours of good information security.

2 Introducing people to new groups that symbolise good information security practices. This might include:
- exposing staff to 'experts' in the business of good information security, for example, the Information Management Council members, and leave them with the do's and don'ts of successful behaviours
- building local expertise amongst people they trust – for example, 'Information security champions'
- exposing people to other state government bodies' approach to information security practices and behaviours.

3 Changing the motivation to comply. This might include:
- measuring the level of errors or positive results in good information security practices and publishing a league table
- building a reward and recognition scheme around the fulfilment of the desired information security behaviours

⇛

– explicitly including the desired behaviours in the organisation's appraisal process for those divisions/ branches affected
– coaching and counselling those who do not exhibit the desired information security behaviours.

Changing normative beliefs and the motivation to comply (subjective norm) is as important as understanding people's attitudes towards a behaviour. Without appropriate subjective norms, behaviour will not change. Attitudes towards behaviour are mainly in the hands of the individual. Creating the appropriate subjective norms is mainly in the hands of leaders.

CONTROL BELIEFS AND PERCEIVED BEHAVIOURAL CONTROL

To change the perceived control beliefs of people with regard to good information security practices there are five elements to consider:

1 Train people to do what constitutes good information security for them – eg:
– make training relevant to the learner's day-to-day life and likely practice of information security
– layer training and build skills at a pace learner's can absorb leaving them with a high perception of control
– segment training so that expectations of what is required of people to adequately execute their role in good information security matches their ability in their day-to-day role.

2 Create pools of expertise that are easy to access so that people can deal with ambiguity about what they should do, easily – eg:
– ready reference sheets containing work instructions, standards, tips and any important policy matters pertaining to the task
– web pages
– information security guides.

3 Train people to be problem solvers – ie:
– information security champions at branch or division level
– ISMS Project team members initially and when implementation has taken place the person responsible for IT Security.

4 Reward people who take control – eg:
– reward innovative development of ISMS processes and procedures at branch level that improves reduces risk and improves information security practices.

5 Use data as often as possible to determine what can and cannot be done – eg:
– create on-line and in-person forums for information security practices.

INTENTION

To change the actual level of control of people with regard to good information security practices there are four elements to consider:

1 Promulgation of information security policy down from the organisation executives through managers to staff involved in day-to-day business processes.

2 Inducting new starters in good information security practices:
– new to company
– new to division/branch/section.

3 Developing and delivering training which is engaging and memorable:
– e-learning for knowledge
– instructor lead training for skills and behaviour
– reference guides
– web pages.

4 Designing point-of-use materials which provide the facts of information security to users in support of the training:
– work instructions, 'how to'
– standards, 'What quality'
– policy, 'Why'.

CHANGING CORPORATE BEHAVIOUR STRATEGY

Getting engagement

The implementation of an ISMS usually occurs at division/ branch level. The success of the rollout at division/branch level is dependent on the level of engagement with management at division/branch level.

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

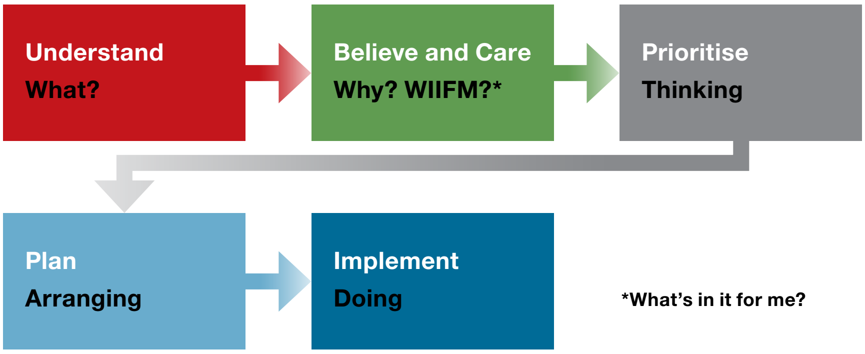


Figure 3: Five stages of engagement

Engagement (Fig 3) can be measured at five levels of increasing depth by finding the answers to the following questions:

- Do they understand the change?
- Do they believe the change is necessary or will benefit them?
- Do they care enough about the change to give priority to learning new skills and knowledge and to change their behaviour?
- Are they consciously planning to make the change?
- Is there evidence that the change is being implemented and that they have the ability to implement the required knowledge skills and behaviours?

Tactics need to be devised to move line managers in the divisions and branches affected through each stage of engagement – eg:

- Understanding the change
  – high impact communication across different channels and repeated often enough to reach most manager's consciousness without becoming annoying
- Believing that the change will benefit them
  – published case studies of success
  – recognition and rewards for implementation and innovation
- Caring about the change
  – division/branch involvement in designing 'their' change
  – inclusion in scorecards
- Planning to make the change
  – assistance in creating a division/branch plan/business case
- Implementing the change
  – training
  – help with implementation issues

During the timeline of the ISMS implementation, the level of engagement with management at division/branch level must be measured to understand what tactics being employed as part of the change management, stakeholder management, communication and training plans need to be revised to create more effective tactics.

SUMMARY

Information security is hardly ever a popular subject and is often left to the controllers of our hardware and networks to manage somewhat behind the scenes. However, records and information management practitioners have a significant role to play in ensuring access to information on a need to know basis is easy for employees, whilst protecting information which should have higher levels of security. To have high levels of information security requires changes in behaviours of all employees in most organisations. Leading that change in behaviours requires records and information mangers to have a clear and effective change management plan that helps employees form the intention to change their behaviours and engages line managers to give them the means and motivation, by which they turn the employee's intention into action. ❖

Bibliography

Ajzen, I. (1985). *Theory of Planned Behavior.* Retrieved from Theory of Planned Behavior: http://people.umass.edu/aizen/tpb.html

Director-General of the National Archives, David Fricker, addressing the National Press Club in February.

What hope is there for transparency and integrity of government in the digital age?

The Director-General of the National Archives of Australia addressed the National Press Club recently about why this issue is so important right now and what the Archives is doing about it. This article is based on his speech.

By **David Fricker**

Social media has given every individual a loud voice – a platform to broadcast their opinion

These are interesting times to be in the business of government information, because right now the public that we're serving is enjoying an unprecedented 'information abundance'. We are all operating in a huge information marketplace serving up oceans of data to a society with an unquenchable thirst. At the same time, perhaps empowered by all this information, we're seeing our society trending away from loyalty to our established democratic institutions and tending instead to engage with specific social issues that cut across boundaries of socio-economic groups, geography and political party. And of course this modern society of ours is fuelled by information – propelled and propagated by 24/7 news providers, social media and a rapidly expanding internet infrastructure.

In this accelerated, modern democracy public opinion can move very quickly indeed. Social media has given every individual a loud voice – a platform to broadcast their opinion. And very quickly indeed other voices can coalesce around that opinion and it becomes a movement. Picked up by news services it becomes a political issue: a job for government.

Government, in response, must move just as quickly. A government which is too sluggish in its response, or is incapable of showing leadership in this public discourse will lose its connection with the people and lose its capacity to effectively and successfully develop and implement policies and programs fit for a 21st-century Australia.

Behind the scenes (and in some cases on centre stage) public servants work at a frantic pace to prepare advice for ministers and reach decisions on key matters of policy and delivery. Here again, things are changing. Across the public service, we are working in new ways, seeking more innovative methods of operation that cut through red-tape, cross departmental boundaries and connect data silos. Within the public service this too is a rapidly expanding information marketplace – a complex and dynamic information eco-system that comprises many technologies, systems and data holdings running on government and non-government platforms. And this is a good thing. We should, indeed we must, embrace new technologies and methods if we are to grow our competence as professional knowledge workers and continue to be the service that Australia requires now and into the future.

But there's another trend that I want to specifically address today. And that is trust. Because it also feels like the general public is exhibiting lower levels of trust in public administration. We are seeing calls for greater levels of transparency and accountability, with expectations of increased scrutiny and faster access to government records as public information. There also seems to an accepted position that the public must always resort to FOI legislation to get the information it wants; because the public service is either unwilling or unable to locate, collate and provide information that should be in the public domain.

The public could be forgiven for thinking that transparency is not well supported by government systems and procedures, instead it seems to be an ongoing battle requiring a disproportionate diversion of resources on all sides.

To understand what's going on here requires us to look at the way government information is managed within the Australian Public Service (APS).

Once upon a time, government records came in a 'file'. A tidy arrangement of A4 pages bundled up in a folder, chronologically arranged on a shelf in the Registry. Minutes of meetings, memos, letters, signed approvals, newspaper clippings, ministerial briefs. All there. Intact, in line, in waiting.

It's a bit different now. Today's digital government record – the trail of evidence of decisions and activities – is peppered across departments: in databases, non-government systems and cloud services, perhaps here in Australia, perhaps in foreign jurisdictions. They're in the emails, the websites, the voicemail, the personal devices. They're stored on new platforms, old platforms, and obsolete and unsupported platforms.

So, the question for today: *What hope is there for transparency and integrity of government in the digital age?*

As the Director-General of the National Archives of Australia, charged with the responsibility to protect and preserve the record of government, this is more than a little important – indeed over recent years we have realigned ourselves and our policies to meet this challenge head on.

THE DIGITAL AGE

We often talk about the three Vs of digital information – the incomprehensible volume of data being created, the velocity at which it is communicated and ingested into systems, and variety of formats that it takes. But there's another V –

vulnerability. And it's the vulnerability of digital information that threatens its value as evidence for accountability.

This is a massive issue for archivists the world over, as we face a rather counter-intuitive probability that this age of information abundance may in fact leave very little useful records for future generations. A prospect that Vint Cerf, vice president at Google and the 'father of the internet' describes as a 'digital dark age'.

How could this be? After all in the digital world, as opposed to the paper world, it's actually very difficult *not* to create a record. We leave 'digital fingerprints' whenever we complete a task on a digital device.

Unfortunately, while we generally believe that digital information once created will always exist 'somewhere' and can one day be retrieved through a ubiquitous search engine, this simply is not the case.

While paper-based records will sit patiently for years in a cardboard box – safe, intact and stable – digital records are extremely vulnerable from the moment they're created. Left unattended and unprotected in email accounts, web servers and shared drives, they easily fall victim to deletion, alteration or are lost through neglect, technological obsolescence or cyber threats.

Bringing this back now to accountability in government – I would point to two factors that jeopardise the long-term survival of government information: the power and convenience of office technology and our overly process-centric approach to innovation.

> *While paper-based records will sit patiently for years in a cardboard box – safe, intact and stable – digital records are extremely vulnerable from the moment they're created*

The APS is, and always has been, an early adopter of ICT. This is a good thing; it has enabled major productivity improvements and streamlining of services. This continues today – right now we are seizing the opportunities of the digital disruption through major initiatives such as the government's Digital Transformation agenda and the Public Sector Data Management program, which also underpins Australia's plans to join the Open Government Partnership.

These are important developments that will re-engineer the processes of government; bringing a change to the services provided by government agencies and releasing more government datasets to uphold accountability and to fuel the digital economy. But these benefits will be short-lived and the processes unsustainable if we adopt a wholly process-centric approach – this time it needs to be different. It needs to be *info-centric*. To make changes that not only redesign transactions but also accumulate information assets that create value well into the future.

We need to understand the difference between technological obsolescence and information obsolescence.

We know with absolute certainty that the technology we use today will be obsolete probably even five years from now, let alone 10 years from now. We know that processes come and go, even whole departments split and merge with periodic machinery of government changes.

But the irony is that we also know with equal certainty that the information we create today absolutely *will* be needed. The information that we can preserve and re-use will deliver benefits and dividends for many, many years to come. Everyone knows that. It's our collective memory, it upholds our rights and entitlements, it's our cultural heritage and it's our national intellectual capital. It is the national identity.

But in our day-to-day work, we don't always recognise this self-evident truth. Information is treated like data, not much more than food for software. And when the software is obsolete, so is the data.

Technological obsolescence is good; we should welcome it. It's a sign of progress. It's a sign of advancement. It's a sign of reinvention. New technology empowers greater productivity and reveals previously unimagined opportunities.

Information obsolescence, on the other hand, is regressive. Information obsolescence takes us backwards, because it means we are losing the raw material of our digital economy and hindering our ability to make real progress.

Information obsolescence is the sign of an organisation that loses its memory and is ill-equipped for the future.

And of course, losing information that is evidence of government activity is a loss of accountability, transparency and integrity.

There are many examples where poor information management, or poor information governance, has led to failures – both in the private and public sectors. Professor Peter Shergold's recent report, *Learning from Failure*, highlights examples such as the APS's management of the Home Insulation Program, the NBN and Building the Education Revolution. The report made conclusions rather than recommendations about improvements that can be made to developing policy and implementing large scale projects.

I've picked out some that relate directly to my topic today:

- Providing robust advice – Public service advice is vital to good government. An APS-wide policy on record keeping should provide practical guidance about when and how records must be created, including that records of deliberative discussions in all forms, including digital, should be retained.
- Embracing adaptive government – The APS should promote new forms of civil participation, including digital and deliberative democracy techniques, in order to enhance consumer-directed care, improve customer service, encourage greater citizen engagement and inform the public economy.

These conclusions hone in on the challenges of the digital age – and highlight the need for action.

ADDRESSING CHALLENGES AND RISKS

I know what you're thinking. You're wondering when I'm going to answer the question: 'What 'hope' is there…'? Or is it hopeless?

No, it is not hopeless. Here are some of the policies and programs that the National Archives has to help agencies manage these challenges and risks.

Check-up Digital

The Archives runs an annual survey tool, known as Check-up Digital which has been assisting agencies to measure their maturity in digital information management practices and improve the ways they manage digital information.

Check-up Digital is designed to assist agencies to:

- improve awareness of what mature practice information management looks like
- identify pathways to improve agencies' digital information management
- set priorities for next steps to increase digital information management maturity
- build a business case for resources to improve business outcomes.

Check-up Digital helps both agencies and the Archives by showing the 'big picture' about how the government is travelling on the path to digital information management.

1 January 2016 target

As part of the government's 2011 Digital Transition Policy, the Archives set a target for 1 January 2016 – for all born-digital records created in agencies to be managed digitally and later transferred to the Archives in digital format only.

Of the 180 Commonwealth agencies in scope, I'm pleased to report that the majority has met the target, and most of the remainder have strategies in place to meet it.

To recognise the outstanding work done to achieve this result and to inspire achievements across the APS, we awarded Digital Excellence Awards for the first time in 2015, shining a light on some exemplars of digital information management. These included:

- the National Offshore Petroleum Titles Administrator (NOPTA), for a seamless integration of EDRMS with other agency business systems

⇛

- the Federal Court of Australia, for the first Australian fully-digital official record of all court documents, completely replacing paper court files; this was accomplished using off-the-shelf technology without additional funding
- the Department of Immigration and Border Protection, for an online self-service facility – *ImmiAccount*, which allows clients to use a secure online account to manage visa applications
- the Department of Human Services, which developed a variety of digital channels for payments and services, including the myGov service which allows people to access a number of online government services and update their own details.

All in one place

A fast, simple way to access government online services.
One login.
One password.
One destination.

The myGov website

Agencies that indicated they would not meet the 1 January target vary in size and profile. Of course we need to understand the impediments faced by these agencies and do all we can to assist, facilitate and encourage the requisite reforms.

One of our early findings is that some agencies failed to meet the target because they had undergone multiple machinery-of-government changes. For the Archives, this understanding revealed that the information these agencies hold is not easily shared, and cannot be merged through machinery of government changes due to data incompatibility. The information may be locked away and safe but it is inaccessible, or is at risk of becoming irrecoverable. So we know that this issue of interoperability is a priority area of focus as we build information management policy.

However, digital transition within the agency is only the beginning. Once agencies have achieved their digital transition, we must look at the long term sustainability of information management across the Commonwealth; this we refer to as 'digital continuity'.

Digital continuity is essential for government moving ahead in the digital age. It is how we will bring the past to the present; how we will account for our actions; and how we will continue to make informed decisions for the future.

Digital Continuity 2020 policy

The steps to achieve digital continuity are laid out in our DC2020 policy. Launched in October last year, it is a whole-of-government approach designed to progressively adopt standard information governance practices by the year 2020.

It advances strong governance frameworks to ensure that information is properly valued, and managed accordingly. Information assets will not be left neglected in uncontrolled environments, enabling requests for information to be dealt with quickly, accurately and comprehensively.

Agencies will transition to entirely digital work processes, meaning complete records will be kept of business processes including authorisations and approvals.

Agencies will also have interoperable information, ready to move between successive generations of software and hardware, and seamlessly shifting through machinery of government changes. No more information obsolescence!

Data and metadata standards will enable stronger intellectual management of records, including fast tracking information into the public domain to uphold transparency and fuel the digital economy.

The policy also recognises the need for certified information professionals across agencies and across government. This network of professionals will work to maintain adequate standards of information stewardship across the Commonwealth.

To get us started on this journey to 2020, the Archives has developed a minimum metadata set, a Business System Assessment Framework and a range of training products, as part of a suite of tools and guidance that will assist agencies to meet the policy requirements.

More immediately, I would draw your attention to Information Awareness Month in May, which includes the launch and the announcement of the National Archives Awards for Digital Excellence on 2 May at the Archives. Also, watch out for more about the Information Awareness Month conference at the end of May.

CALL TO ACTION

The Archives is at the forefront of digital information management and committed to setting the standard for transparency and integrity across all Commonwealth institutions. But the National Archives is not the only player in the game. We see the Digital Continuity policy as the 'information pillar' of the broader Digital Transformation agenda, complementing the role of the Digital Transformation Office and others in forging real and necessary change.

So, I leave you with this call to action: for all Government agencies to take responsibility. I also want to encourage all vendors, commercial providers and supporters to come on board, to get involved and to work collaboratively with Australian government agencies.

We can uphold the transparency and integrity of government in the digital age. It is our duty; we have the tools for the job; and it is within our means. We just have to make it happen. ❖

ABOUT THE AUTHOR

David Fricker joined the National Archives as Director-General on 1 January 2012. Prior to that, he was Deputy Director-General for the Australian Security Intelligence Organisation (ASIO) and Chief Information Officer before that. David has been an active member of the International Council on Archives (ICA) since 2012, hosting the ICA Congress in Brisbane and achieving the office of President FAN in 2013. He took up his position as President of the ICA in October 2014.

THE ROLE OF INFORMATION MANAGEMENT IN PREVENTING MAJOR DISASTERS

From the Pike River coal mine explosion to the Three Mile Island nuclear meltdown, it seems poor information management practices have contributed to a rather large number of disasters throughout history. Managing information well therefore is just good business sense. This article looks at a range of these disasters.

By **Janita Stuart**

When we look at some notable disasters from around the world, it is disappointing to see how often poor information management practices contributed to the cause of the disaster. Before we move onto look at some examples, let's take a look at some principles of information management.

Firstly, from the Archives New Zealand (2000), which says information is to be:

- **complete** – includes structural and contextual information, the process that produced it and other linked documents
- **comprehensive** – records the whole business process
- **adequate** – fit for purpose for which it is being kept
- **accurate** – correctly reflects what was communicated, decided or done
- **authentic** – it is what it purports to be
- **useable** – identifiable, retrievable, accessible, and available when needed
- **tamper-proof** – security maintained to prevent unauthorised access, destruction, alteration or removal.

Secondly, Ross et al (1996) and Johansson & Hollnagel (2007) say IM is about:

- **systems** – computer systems as well as systems such as file classification and security classification
- **business processes** – an orderly sequence of tasks; in essence, prompting people to do the right thing at the right time
- **people** – the people having the skills to do the task and understanding why they are doing it so they do the task willingly.

Ideally, these three should be well balanced. Whenever one of the three is underperforming, the other two have to take up the slack.

With those IM principles in mind, let's look at some disastrous events.

⇛

PIKE RIVER COAL MINE EXPLOSION

On 19 November 2010, an explosion occurred at Pike River coal mine taking the lives of 29 men and injuring two survivors.

About one and a half hours after the explosion, two men walked out of the mine, saying how they were injured by the explosion and had passed out as they slowly made their way out (a two kilometre walk) as the air was unbreathable. The explosion had severed all the electrical monitoring equipment connected to the above-ground control room. An electrician was sent into the mine to try to repair the damaged electrical connections. He turned back without going in very far due to the air being unbreathable. Several air samples were taken indicating the mine was still on fire. A borehole was drilled into the heart of the mine reaching pit bottom five days after the first explosion. Through that hole, they took air samples, bringing hope that the air might be breathable, which would enable people to enter the mine and that perhaps some of the men might still be alive if they had been able to reach some of the ‘self-rescuer’ breathing devices.

However, the experts in coal mining and mine rescues saw the CCTV footage of the explosion at the portal and believed no one could have survived the blast. A few hours after taking the air samples at pit bottom, the second explosion occurred dashing all hope of any survivors as it was multiple times worse than the first. There were two further explosions.

Some coal mines emit methane gas from the coal seam. Pike River was one of these. Hydro mining (like water blasting) produces more methane than dynamiting out the coal. If methane is kept diluted with good air ventilation, it is less likely to ignite. However if there isn’t good ventilation and the gas can concentrate, it is easily ignitable. Methane is lighter than air so it rises, leaving the breathable air at floor level and the methane concentration at the ceiling. The equipment that took readings of the air quality showed throughout October and November numerous times when the methane concentration was at dangerous levels. These readings didn’t go to the managers nor did they receive publicity. They were not reported in daily production or weekly operations meetings, nor through the deputies’ production reporting system (as demonstrated later). They were not reported to the regulator as the regulation required.

At management level, there were committee meetings which had action sheets that recorded the person responsible for the action and expected completion date. If it was simple, it generally was done. However actions required of some departments were routinely left undone. The actions that required a coordination of several departments were also routinely left undone.

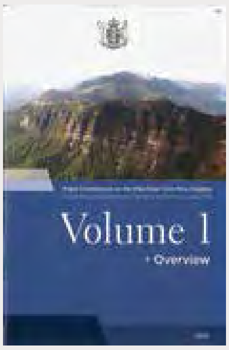
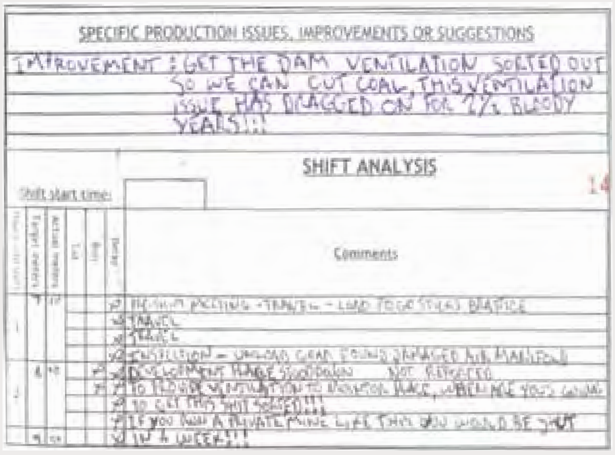


Image 1 is an example of a deputy production report: this example was completed by Dene Murphy on 21 October 2010, less than a month before the explosion. On average, Mr Murphy put in one of these reports every day for two years. So you can see the frustration he was feeling in the language he used to express himself. This was Pike River’s system of identifying matters that presented safety risks for the employees. There were also many other reports about incidents, accidents and hazards. However, there was no business process for sorting, classifying, passing the concerns on to a manager who could/would do something about it. Many of these were just thrown away. Those not tossed became a large accumulation. In fact the Royal Commission analysed 1083 of them.



SPECIFIC PRODUCTION ISSUES, IMPROVEMENTS OR SUGGESTIONS

IMPROVEMENT : GET THE DAM VENTILATION SORTED OUT
SO WE CAN CUT COAL, THIS VENTILATION
ISSUE HAS DRAGGED ON FOR 2½ BLOODY
YEARS!!!

SHIFT ANALYSIS

Shift start time:

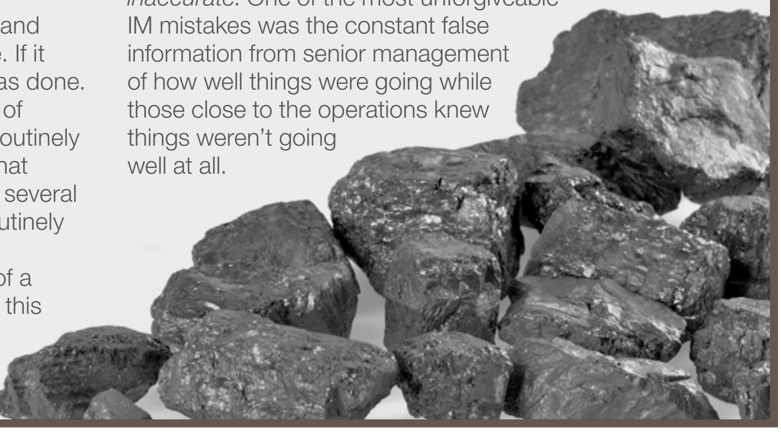
Comments

PRE-SHIFT MEETING - TRAVEL - LOAD TOGETHER BRATTICE
TRAVEL
TRAVEL
INSTALLATION - UNLOAD GEAR FOUND DAMAGED AIR MANIFOLD
DEVELOPMENT HAS SHUT DOWN NOT REPAIRED
TO POOR VENTILATION TO DEVELOPMENT PLACE, WHEN ARE YOU GOING
TO GET THIS SHIT SORTED!!!
IF YOU RAN A PRIVATE MINE LIKE THIS YOU WOULD BE SHUT
IN A WEEK!!!

Image 1: Extracts from Dene Murphy’s 21 October 2010 deputies production report (Royal Commission, 2012, vol. 2, p. 105).

Amongst the victims of the poor information management were the families of all the mine workers. Pike River’s system of identifying who was underground and who wasn’t did not receive full compliance. At the time of the explosion, they could not quickly identify who was affected by it. Over the 20 hours it took to ascertain exactly who was underground, the families were distressed.

Reflecting back on the IM principles outlined at the top, how could they have made a difference at Pike River? There was no management information system. Vital information was not brought together, summarised and analysed for executive managers. The key information on health and safety incidents was available but was not handled systematically and therefore did not receive a response. Therefore the information was not *usable* because the *business processes* didn’t have it go to the right person who could/would respond to it appropriately. The system for recording who was in the mine at any given moment didn’t work. Therefore the information was *inaccurate*. One of the most unforgiveable IM mistakes was the constant false information from senior management of how well things were going while those close to the operations knew things weren’t going well at all.



CAPSIZING OF THE *HERALD OF FREE ENTERPRISE*

When the *Herald of Free Enterprise* ferry capsized between Dover and Bruges-Zeebrugge on 8 March 1987, 193 people were killed.

On that fateful day, 650 passengers were on board. The doors to the car deck were left open. Water entered the ship at the car deck and caused it to capsize. The doors being open would not have in itself caused the ship to capsize because a sister ship made the crossing with her doors open without incident.

This ship did not normally do the Dover to Bruges-Zeebrugge run. The pier and the ship's decks didn't match each other. The drawbridge could only go to one deck and vehicles could only go to that one deck. The ship had to fill its forward ballast tanks to lower the ship in the water to enable cars to use the drawbridge and load onto it. The ship was due to be modified during its next refit scheduled for later that year to overcome this limitation.

Most ships are divided into watertight compartments below the waterline so that, in the event of flooding, the water will be confined to one compartment, keeping the ship afloat. However the car deck was open with no dividers.

Normal practice was for an assistant boatswain to close the ferry doors before dropping moorings. Usually the first officer would remain on deck to ensure they were closed before returning to the wheelhouse.

On 8 March, they were running behind time. The captain was under pressure from the owner of the ferry (Townsend Thoresen) to be on time. The ship was designed for quick acceleration. The weather brought calm conditions. Although there was a high spring tide, the water was shallow especially with the ballast.

The first officer returned to the wheelhouse before the ship dropped its moorings (this should not happen but commonly did). He trusted the assistant boatswain to close the doors. However the assistant boatswain went to his cabin and took a nap. The captain presumed the doors were closed. He couldn't see the doors from the wheelhouse. The doors are held by massive hydraulic rams, so they couldn't open by themselves or by water pressure. There was no warning system in the wheelhouse to alert the captain if the door was open.

In the hurry to get away without falling further behind time, they neglected to dump the ballast. The ship was in shallow water and was going too fast. They only got 91 metres from shore.

Reflecting back on the IM principles, how could they have made a difference for the passengers on *Herald of Free Enterprise*? The ship's captain acted on the inaccurate presumption that the doors were closed and did not have access from the wheelhouse to the information to tell him they were still open. He did not have access to accurate information. The business process broke down in two ways: firstly, the process of the boatswain informing the captain broke down as the captain did not get the information about the doors before dropping moorings; and secondly, the process for the crew to dump the ballast before dropping moorings broke down. There were also human errors. It doesn't help when a key crew member is asleep in his cabin or when a captain is in such a hurry to keep to the schedule that he neglects to complete the checks before dropping moorings. In this case, the checks were closing a door and dumping ballast.

⇛

TANGIWAI RAILWAY DERAILMENT

On 24 December 1953, the Tangiwai Railway derailment killed 151 people. There were 285 people on the train.

In 1925, the railway bridge at Tangiwai was weakened by a lahar (a type of mudflow or debris flow which flows down from a volcano). A civil engineer's report describing the damage said pier 4 was tilted half an inch (12 mm) and the track above had bulged to the same extent. The pier was also scoured out at its foundation.

Before the railway bridge was built, the engineers documented that it was the wrong place to build a railway and bridge. It seemed risky to place two state highways and the railway line so close to three active volcanoes.

Experts warned of the likelihood of a lahar. A mountain guide had warned that the crater lake was rising: the officials laughed at him. In 1951, some men who often canoed the crater lake noticed the rising lake level and began to record soundings showing it was rising at half an inch a day. One of them wrote a letter to the geological scientists warning of the risks. They were ignored.

At about 8 pm on that fateful evening, there was an earth tremor on Mt Ruapehu. The outlet of the crater lake (consisting of only ash) collapsed starting the lahar. Lahars travel at about 19 kilometres per hour.

The lives of 151 people were lost for lack of a phone-call to stop the train

The train was running on time. While sitting at Taihape at 8.30pm the roaring noise of the lahar could be heard. The noise grew increasingly louder until at 900pm it was 'a terrific roar'. At 10.06pm, the train hadn't yet left Waiouru. No one stopped the train even though they could hear the mountain's 'terrific roar' for over an hour.

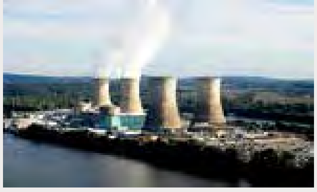
The lahar struck the bridge at 10.15pm; the train went into the river at 10.21pm. The lives of 151 people were lost for lack of a phone-call to stop the train.

Reflecting back to the IM principles, what went wrong? The history of lahars didn't inform the right people. The numerous reports and letters that were written about the risks and conditions, didn't inform the right people who could or would do something about it. The people who were informed chose to do nothing. The damaged bridge wasn't repaired. Those monitoring the seismograph didn't raise an alarm/alert. The people who heard the mountain roaring didn't inform the right people. There was no business process put in place after the numerous warnings to enable the train to be stopped.

The rail bridge at Tangiwai. This photo was taken about 30 hours before it happened.

THREE MILE ISLAND NUCLEAR MELTDOWN

The Three Mile Island accident, which occurred on 28 March 1979, was a partial nuclear meltdown that occurred in one of the two nuclear reactors in Dauphin County, Pennsylvania.



Although no lives were taken on the day, over the following two years, there was a noticeable rise in mortality rates of the very young and the elderly.

From the perspective of the staff on duty, the accident was "unexpected, incomprehensible, uncontrollable and unavoidable". It began with a typical maintenance mistake of not returning equipment in the non-nuclear secondary system (such as safety interlocks) to the operational mode. This was followed by a stuck-open pilot-operated relief valve in the primary system, which allowed large amounts of nuclear reactor coolant to escape. The mechanical failures were compounded by the initial failure of plant operators to recognize the situation as a loss-of-coolant accident due to inadequate training and human factors. In particular, a hidden indicator light in the control room led to an operator manually overriding the automatic emergency cooling system of the reactor because the operator mistakenly believed that there was too much coolant water present in the reactor and causing the steam pressure release.

This accident occurred precisely because the operators *did* follow the predetermined instructions provided to them in their training.

An indicator misleadingly showed that a discharge valve had been ordered closed but not that it had actually closed. In fact, the valve was blocked in an open position. The valve was not equipped with a valve stem position monitor, so the control room operator only knows that a signal has gone to the valve for it to close but not whether it has actually done so.

The shift supervisor at the Three Mile Island hearings testified that the control room never had less than 52 alarms lit. During the TMI incident, more than a hundred alarm lights were lit on the control board, each signaling a different malfunction, but providing little information about sequencing or timing. So many alarms occurred at TMI that the computer printouts were running hours behind the events and, at one point the printer jammed, losing valuable information. Operators commonly suppress alarms in order to destroy historical information when they need real-time alarm information for current decisions. Too many alarms can cause confusion and a lack of confidence and can elicit exactly the wrong response, interfering with the operator's ability to rectify the problems causing the alarms.

In the nine years before the TMI incident, 11 of those valves had stuck open at other plants, and only a year before, a sequence of events similar to those at TMI had occurred at another US plant. Nothing had been done about correcting them.

While the Nuclear Regulatory Commission (NRC) collected an enormous amount of information on the operating experience of plants, the data were not consistently analysed until after the Three Mile Island accident. The engineering firm for TMI, had no formal procedures to analyse ongoing problems at plants they had built or to review the reports filed with the NRC.

The information needed to prevent TMI was available, including the prior incidents at other plants, recurrent problems with the same equipment at TMI, and engineers' critiques that operators had been taught to do the wrong thing in specific circumstances, yet nothing had been done to incorporate this information into operating practices.

Reflecting on IM principles, the staff were deciding what actions to take based on inaccurate information – the indicator showing that a discharge valve had been ordered closed, but not that it had actually closed. Information is unusable when there is too much of it in such a short period of time that it is impossible to take it all in, including in this case, for the computer to put it all out. The information that could have prevented this accident existed, not just where it could be used. There was no business process to analyse the available data that would have identified a safety issue. A known problem had been left unresolved. Training of staff contributed to the problem as the staff were trained to do the wrong thing in these situations.

CHINA AIRLINES FLIGHT 140 CRASH

On 26 April 1994, China Airlines flight 140 crashed, killing 264 people.

Flight 140 was approaching Nagoya, Japan to land. The takeoff/go around button had been pushed as usual activating the autopilot. There were two bursts of thrust applied in quick succession and the airplane was nose up in a steep climb. Airspeed dropped quickly, the plane stalled and the nose dropped. The captain tried to pull back the control column but was unsuccessful because the autopilot could not be overridden. So when the pilot wanted to take control, he couldn't.

Problems with the flight control computer software (which didn't allow the captain to override autopilot) had been identified and a service bulletin had been released. The 'fix' was available from September 1993 (six months earlier). However because the computer problem had not been labelled a 'cause' of the previous incidents, the modification was labelled 'recommended' rather than 'mandatory'. China Airlines was planning to fix the flight computers the next time they needed repairs.

Reflecting on IM principles, the information was inaccurate that categorised the computer 'fix' to be discretionary.

China Airlines was planning to fix the flight computers the next time they needed repairs

SUMMARY

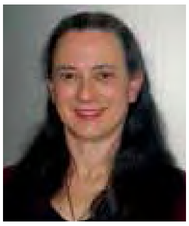
In conclusion, all these precious lives, and their grieving family and friends, were impacted by preventable, predictable disasters. Let's learn from these mistakes and not let them happen again. ❖

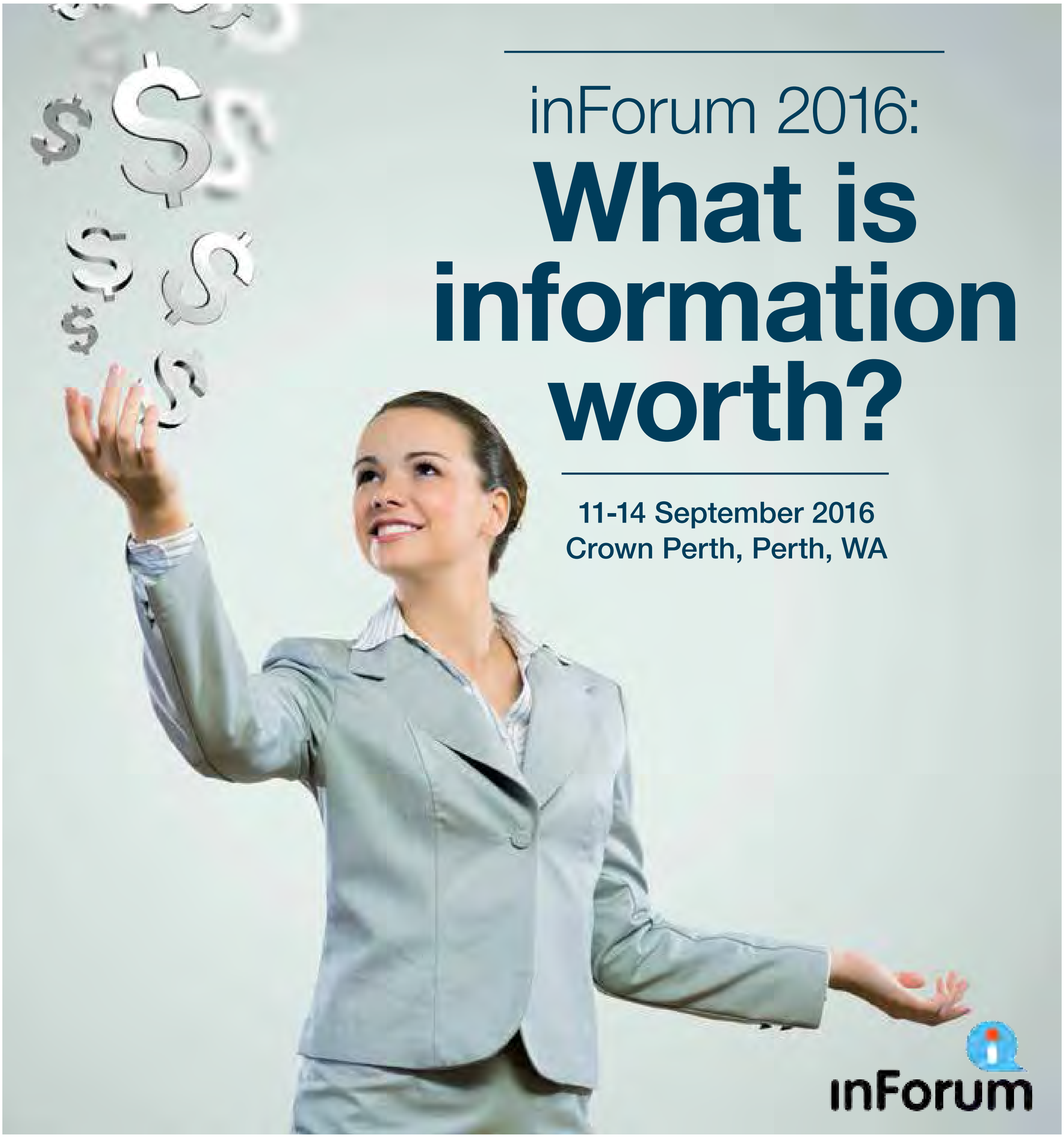
Full references for this article are available on request.

ABOUT THE AUTHOR

Janita Stuart began her career as a librarian. Over time she branched out into web development, records and archives management, knowledge and information management. She completed the MIM and Nat Dip Business Management in New Zealand and is currently researching for a PhD in Information Management.

✉ Janita was the treasurer of the New Zealand branch of RIMPA. She can be contacted at janita.stuart@worksafe.govt.nz





inForum 2016: What is information worth?

11-14 September 2016
Crown Perth, Perth, WA

The theme for inForum 2016 is 'The value of information'. With most organisations drowning in data, paper-based and electronic documents, e-mails and social media messages, this information is stored (if at all) in operational systems, hidden on employees' disk drives or scattered across multiple repositories. This conference will focus on RIM professionals assisting their organisations to reduce costs and increase efficiency through effective systems, and will touch on a wide range of relevant topics.

There is an excellent line-up of topics and speakers to inspire, inform and engage delegates. No matter what your level of expertise or current role, there is something for everyone.

The program includes two concurrent streams, optional workshops, 20-minute vendor presentations, a trade exhibition, networking opportunities and social events. Highlights include a number of local and overseas keynote speakers, panel discussions and interactive sessions.

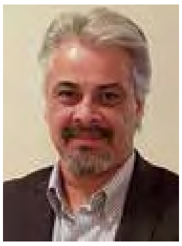
> *No matter what your level of expertise or current role, there is something for everyone*

FOR MORE INFO The full program has now been released and can be viewed or downloaded at: **inforum.net.au**

Keynote presentations

Innovation to INNOVATION: Use cloud to enable individual, team and enterprise innovation

Chris Walker, PHIGs IMC, Canada



This session will explore, through stories and discussion, how cloud technologies enable individual, team and organisation innovation. We'll also look at what rules and organisational attributes and attitudes are required to allow innovation.

Change your organisation's culture to make data and information quality a part of its DNA

Jay Zaida, AlyData, USA

Welcome to the 'Dawn of Data'. Volume of data is projected to grow 50-fold between now and 2020. Mobile, social, and cloud applications are creating a highly decentralised data eco-system, with complex data sets becoming the norm. We are in the midst of a historical event – organisations are slowly transitioning from an IT-centric environment to a data-centric one.

What is needed is a major cultural transformation within organisations – to become data-driven, and data and information quality focused. This will require support from the highest levels, long-term investment and a change management strategy. Changing the culture of an organisation is challenging, but it has been done before.

The speaker will share his experience with you, discuss best practices, implementation challenges, core capabilities required in an enterprise data quality program and critical success factors, so that you can use this knowledge to influence change within your organisation. After all, quality isn't just about slogans, but about transforming organisations and their staff, so that they have a 'quality mindset' and weave quality into everything they do!

Volume of data is projected to grow 50-fold between now and 2020

Optimising electronic documents and records management technologies for e-government efficiency in Kenya

Cleophas Ambira, Kenya Association for Records Managers and Archivists, Kenya

This paper is based on findings of a doctoral study on a framework for managing e-records in support of e-government in Kenya. It provides insights regarding the state of EDRMS technologies implementation in Kenya in an attempt to improve efficiency and cost-effectiveness in government operations within e-government space. The study looked at a wide range of issues regarding management of e-records in the e-government context, including the role of effective EDRMS implementation as a driver of effective records management impacting on efficiency and cost optimisation.

Persevering to achieve results: an eight-year battle to save a man's life

Colleen Egan, WA

This Perth-based journalist was the first to properly investigate the case of Andrew Mallard, convicted and detained in 1995 for the murder of Perth jeweller Pamela Lawrence. Approached by the Mallard Family in 1998, Colleen's subsequent investigations revealed that Mallard's conviction had been largely based on a forced confession.

Since then, she has been the driving force behind an eight-year campaign to prove the Western Australian's man innocence. Her stories and commentary on Mallard, published in *The Australian* and *The Sunday Times* over many years served to spark public interest in the family's campaign to have him released.

After years of work, Colleen helped uncover new evidence that led to Mallard's release after 12 years of imprisonment, and a public apology from WA police commissioner Karl O'Callaghan. The conduct of the police involved in the case is now under scrutiny by WA's Crime and Corruption Commission.

VISIT PERTH FOR INFORUM 2016

Perth, capital of Western Australia, sits where the Swan River meets the southwest coast. Its suburbs lie along sandy beaches, and the huge, riverside Kings Park and Botanic Garden on Mt Eliza offer sweeping views of the city. The Perth Cultural Centre houses the state ballet and opera companies, and occupies its own central precinct, including a theatre, art galleries and the Western Australian Museum.

Experience Perth and surrounds, and you'll find all of the essential ingredients for a great Australian holiday – some of the country's best beaches, plenty of nightlife, bustling markets, inner city parks, outdoor dining and amazing marine adventures. ❖

AWARDS 2016: NOMINATIONS ARE NOW OPEN

RIMPA presents a range of awards each year at our annual inForum convention. Some awards are by nomination, others are on merit.

J EDDIS LINTON AWARDS 2016

The J Eddis Linton Awards 2016 are open for nomination, in six categories:

Innovation

Sponsor: Information Proficiency

The J Eddis Linton Award for Innovation recognises leadership through the practical application of innovative solutions for new and existing market needs resulting in a commercial, environmental and/or social benefit.

Collaboration

Sponsor: EzeScan

The J Eddis Linton Award for Collaboration recognises an exemplary skills development collaboration between a department, employer or industry body and, at least, one other stakeholder (including vendors and consultant).

INDUSTRY CONTRIBUTION AWARD

Introduced in 2014, these awards recognise industry contributions by RIMPA Professional members.

Nominations can be submitted by any member of the Association, however every Branch Council should submit at least one nomination per year.

Nominations must include a brief supporting statement about the nominee and their nomination (ie, what is their contribution to the industry, where, when, how long, etc).

Areas where awards could be awarded include (but are not limited to):

- Involvement with Standards/Education
- Contribution to Standards/Governance / Strategy
- Involvement in Leadership/Mentoring
- Contribution to Local Government
- Contribution to the Company or to a specific Branch

Nominations (which do not require a nomination form) should be emailed to kristen.keley@rimpa.com.au

➲ **Nominations close 30 June 2016.**

Recall *iQ* Article of the Year Award

Any current financial member who submits an article to *iQ* between September 2015 and August 2016 is automatically placed in the running for the Recall *iQ* Article of the Year Award.

Have you considered writing an article for *iQ*? Articles (of at least 750 words) can be submitted on any topic loosely related to RIM and also gain professional members CPD points.

➲ There is still time to be considered for this year's awards, send your article submission to editor.iq@rimpa.com.au

Implementation

Sponsor: FYB

The J Eddis Linton Award for Implementation recognises organisations that have achieved outstanding results through excellence in implementation of a project.

Business benefit

Sponsor: Information Proficiency

The J Eddis Linton Award for Business Benefit recognises organisations that have achieved outstanding success for business improvement.

Student

Sponsor: Records Solutions

The J Eddis Linton Award for Student recognises students who have achieved excellence in educational studies in RIM.

The winner of each category, in addition to being recognised for their excellent contribution to the industry, also wins a prestigious wall plaque and $500 (local currency AU or NZ) in the form of either a gift card or in RIMPA events/membership. ❖

➲ **Nominations close 30 June 2016.**

SPONSORS

Innovation

INFORMATION PROFICIENCY | SIGMA DATA

Collaboration

ezescan

transforming paper into knowledge

Implementation

fyb

Business Benefit

INFORMATION PROFICIENCY | SIGMA DATA

Student

Records Solutions

Helping Manage Information Effectively

Article of the Year

recall™

FOR MORE INFO

For more information about the awards go to: **rimpa.com.au/grants-and-awards/eddis-linton-awards/**

Digital hoarding: perils, pitfalls and paradoxes of the Digital Age

Information consumption is no longer a harmless diversion. Information consumption now consumes our every waking moment. Will our addiction to information consumption destroy us? Are we facing a digital nightmare? Are we passively accepting our own doom? To harness the possibilities of the digital revolution, we must be prepared to revolutionise ourselves. Traditional approaches to information storage, retrieval and disposal are out-of-place in the new era. We need new approaches to age old problems if we are to prosper. Vive la revolution!

By Chris Foley

The Digital Age is founded on a paradox. Our lives and productivity have been radically improved by digitisation. The technology has been accompanied also by an explosion in the sheer volume of digital information. We have now an insatiable appetite for ever increasing volumes of information. We snack, feast and even gorge on information. Information consumption is no longer a harmless diversion. Information consumption now consumes our every waking moment. Under such circumstances, it is not possible to adequately classify, manage and dispose of such volumes information by reference to traditional information management methods. New strategies based on principles of macro appraisal are required. However, for a strategy to be successful it must consider the budgetary context. A strategy that might therefore be successful in an organisation with a large information budget will be less successful in an organisation with a small budget and vice versa.

THE DIGITAL AGE: NEW POSSIBILITIES, NEW PARADIGMS

Suspend belief for a few moments…

- Imagine a world in which....from the moment you wake up, you are connected instantly to digital information...
- Imagine a world in which...you pay your bills and use public transport with a swipe of a personalised card...
- Imagine a world in which...you can have instant contact with family and friends wherever they are in the world…

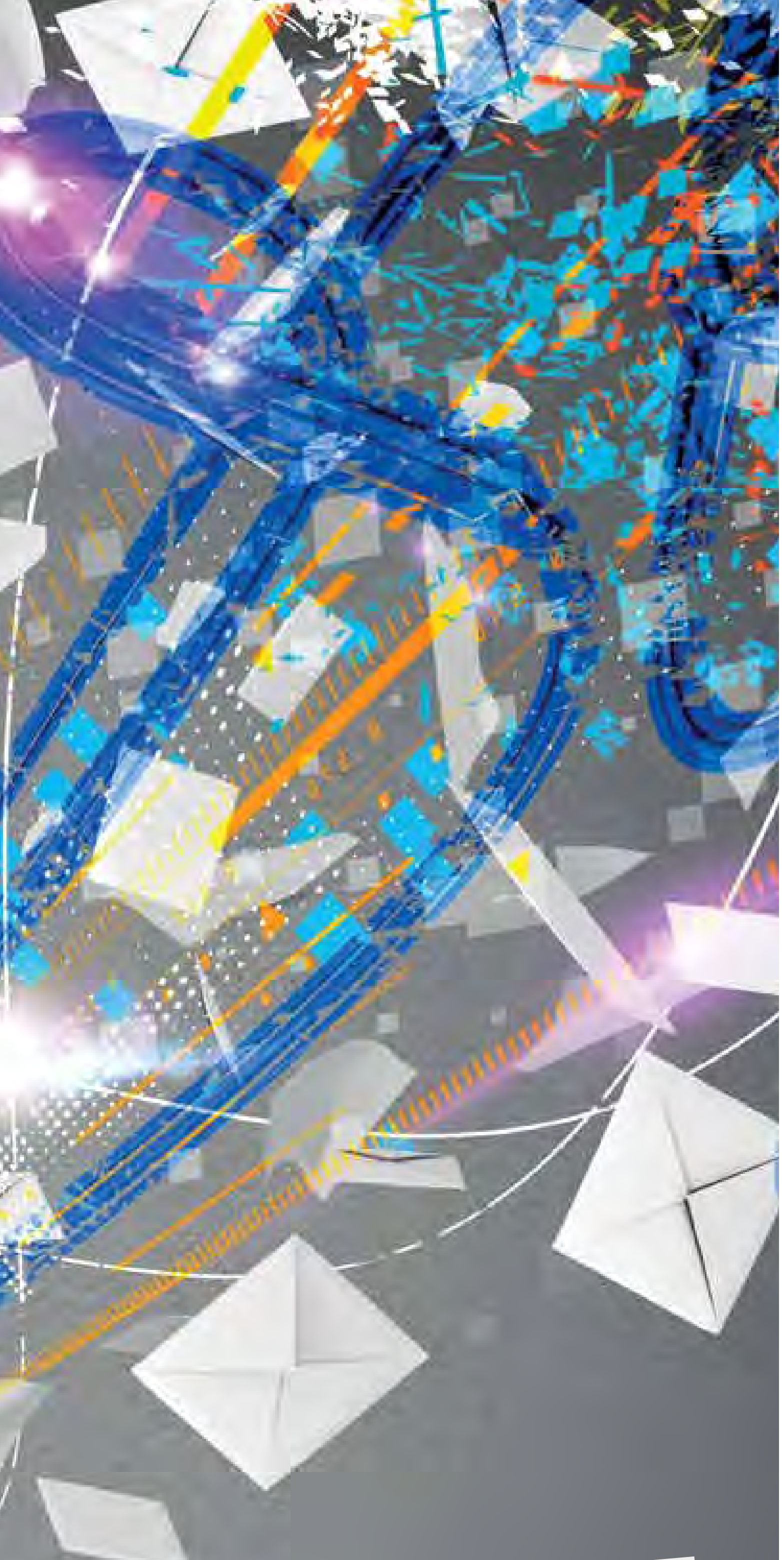
Sound familiar? The Digital Age has crept up on us and swept aside barriers. What was once the stuff of science fiction is now commonplace. We have instantaneous communication between countries, space travel and robots. We can access and control the information we receive using personalised devices and determine for ourselves when and where we receive it. Anywhere, anytime we are digitally connected.

The Digital Age has enabled us to blur the barriers that separate different parts of our lives. What was once 'down time', periods of time in which through choice or circumstance that are not devoted to work can now be utilised for work. Sitting on the train? No problem. I can access my email or browse the World Wide Web. Running late for my next appointment? No problem. I can send a text ahead to apologise and advise by how many minutes I will be late. Which will be faster for me, train or car? No problem. I can access real-time travel information on my telephone.

Such information consumption involves the creation and distribution of staggering amounts of information. In the current decade, the total volume of digital information is doubling in size every two years. By 2020, it has been estimated that the volume of data that we create and copy annually will reach forty-four zettabytes or forty-four million gigabytes.[1] In other words, this volume of data in 2020 will represent "…more than 5,200 gigabytes for every man, woman and child..."[2]

The nature of such information is also changing. Information was once created by a select group of professionals, administrators and artists for broader consumption. However, in 2012, it was estimated by EMC that 68% of digital information "…is created and consumed by consumers – watching digital TV, interacting with social media, sending camera phone images and videos between devices and around the Internet, and so on."[3]

⇛



story snapshot

Our productivity has been radically improved by digitisation – we can achieve outcomes that are inconceivable without digitisation.

This paradigm shift has brought about an explosion in the sheer volume of digital information.

We now have an insatiable appetite for more information.

New approaches to age old problems need to be found if we are to prosper in this Digital Age.

The world of work has experienced similar trends in in the creation and consumption of information. According to a 2012 survey by the Compliance, Governance and Oversight Counsel (CGOC) (a US based forum of organisational executives), the average employee creates, sends, receives and stores at least 20 MB of data per day. After 15 business days, employees have accumulated 220 MB of new data each and after three years an employee has gathered 15.12 GB of data.[4]

Much of this new information, whether created for work or personal consumption, is of relatively low value. According to the CGOC Study, 1% of organisational data is subject to litigation hold, 5% is subject to regulatory retention and 25% has some business value. The remaining 69% of an organisation's data store has no business value at all.[5]

After 15 business days, employees have accumulated 220 MB of new data each and after three years an employee has gathered 15.12 GB of data

DIGITAL AGE: TOWARDS NEW IM UNDERSTANDINGS

The Digital Age is dominated by the World Wide Web. When the World Wide Web was launched, information was uploaded and displayed primarily as static information pages. The era of Web 1.0, as it is now called, brought with it new technology but it did not challenge the way information was created and distributed. Information was created by a select group of people for consumption by a wider audience. The information transfer experience was one way.[6]

The era of Web 1.0 gave way in turn to Web 2.0 with the emergence of the Social Web. Information is created and shared by all participants of the Web. Through the use of wikis, online forums and social media, individual consumers participate actively in the creation and sharing of information.[7] Indeed, it is this dynamic "democratic" process that gives authority to information and legitimacy to opinions. Information and opinion-making can be created and distributed largely outside the control of institutions. Information exists to serve the needs and desires of individuals and the virtual communities that they wish to inhabit.

The continued development of the Web has also given rise to the concept of Web 3.0, however, the full implications of which are yet to be determined.[8] Web 3.0 is concerned with computers exchanging information with each other in order to predict our desires and to deliver tailor-made content directly to our personalised Wi-Fi enabled portable device.

The ways in which Web 2.0, Web 3.0 and the Social Web have changed information management are summarised in the table on the following page.

INFORMATION MANAGEMENT PRINCIPLES	
Pre-Digital Age	**Digital Age**
All information is knowable. Information volumes can be quantified. A small number of people create information according to specified rules. Once created, that information can be captured into information repositories within which access and maintenance regimes are imposed by the organisation. Business Classification Schemes (BCS) are developed centrally as they facilitate an organisational-wide appreciation of an organisation's information universe. A BCS permits granular classification schemes (eg, Function-Activity-Topic-Sub Topic), and the application of complementary disposal authorities.[9]	**All information is not knowable.** We cannot quantify the available information. There is too much information being created and distributed on a daily basis to adequately capture and manage. Information is created and shared across a wide variety of technological platforms by a diverse range of people for varying purposes. Classification is two tiered: • Macro-level classification is determined centrally within organisations. • Micro-level classification is determined locally within individuals by individuals and work teams. Records Management is concerned with a strategic conceptualisation of information. Automated classification tools are developed and refined to meet changing information types and consumption patterns.
Not all information is of equal value. Some information can be classified as records, while some information can be classified as ephemeral or transitory information. Records retention and disposal authorities are based on this principle. Some information can be classified as records and some information can be classified as not-records. Once appraised as records, information objects can be sentenced.	**Not all information is of equal value.** In the Digital Age, this principle remains true. Some information is of high value. Some information is low value. However, making value judgements is extremely difficult due to: • sheer volume and diversity of information • the segmentation of authority over the information. As information is no-longer created and controlled in a top-down authority structure within organisations and institutions, organisational management structures are not the source of authority over the information.
Information is a static resource. Once information is created (eg, a document), its content is fixed and it is attached to the appropriate file. When the file becomes full or the matter is closed, the file can be archived based on the records retention schedule. Based on the sentence applied, a file can either be transferred to permanent archival storage or securely destroyed when its sentence expires.	**Information is a dynamic resource.** Information is created, updated and referenced during 'run-time' of a business process. Information is stored within a business application, embedded in its business process context. The process is managed as a dynamic information resource rather than simply managing the information artefacts that arise from the process.
Information consumers respect centralised business rules. Information is tightly controlled. The majority of people consume rather than create information. Therefore, the consumers must abide by the centralised access and distribution rules established by sources of authority. Within organisations, the records manager is a gate-keeper for the administration of information access.	**Information consumers respect the rules of the social web.** In a digitally-connected world, information exists in relationship to an individual and the web of inter-relationships in which that individual functions. The motivations of an individual drive the creation, distribution and use of information. Further, the motivations of individuals drive the extent and the form that metadata 'tagging' occurs. This is true in the social media world. It is true in the context of business systems. Individual consumers are the gate-keepers for information distribution.

DIGITAL AGE: APPLYING NEW UNDERSTANDINGS

Once the information management challenges of the Digital Age are articulated, solutions and approaches can be applied to them. Such approaches require different strategies than previously pursued by information managers. Further, with the growing financial costs associated with new technologies, consideration must be paid towards the budgetary constraints of an organisation. The success of an information management regime depends on synchronising the strategy to the available budget.

All information is not knowable. Or more specifically, information is not knowable by individuals. Therefore, business classification schemes should respect the principles of both 'macro appraisal' and 'folksonomies'. In essence, macro appraisal is a refinement of functional analysis in that it takes a 'top down' approach to the analysis of an organisation's functions and the key processes required to deliver those functions.[10] However, in many large organisations or where the matters undertaken are too complex to be adequately described by high level descriptors alone, higher level descriptors (determined centrally) should be supported by folksonomies at the lower levels. A folksonomy is the process by which information consumers themselves determine and apply what metadata is required to describe the information with which they work.[11]

High investment options	Low investment options
Classify information by its function and its process to streamline the design of classification structures and to simplify internal communication strategies. **Capture information** into ECM and business systems and apply 'generalised' automated metadata tagging based on function and process. **Analyse the textual context** of the information, and apply automated text indexing based upon explicit and implicit information aggregations. Simply indexing text is not sufficient. More powerful and more successful text searching is based upon the principles of ontology-based searching.[12] Two key indexing methods using an ontology: • **Explicit**. Capture instances of known keywords within the textual content relevant to the function and process. For example, in a local council, most information will have a locality significance. Therefore apply tags within the content based upon explicit locality references. • **Implicit**. Derive meaning from your text based upon a business understanding of the information. For example (using the local council example), apply tags that aggregate localities into regions etc, based upon known rules. **Devolve granular level metadata tagging** to end users. Exploit the power of the user community. If users find value in tagging, they will tag. There is no way to compel people to tag. They must perceive the benefits to them (not to the organisation) for them to tag.	**Classify information by its function and its process** to streamline the design of classification structures and to simplify internal communication strategies. **Structure network drive folder hierarchies based on "macro appraisal" principles**. Permit users to create lower level folder structures (which they will do instinctively anyway).[13] However, by controlling the upper levels of the structure, information can be managed based upon security and retention considerations. In the absence of sophisticated systems, network folder hierarchies still represent the most effective storage, classification and retrieval approach.

…the vast majority of information created and distributed will be of low value or no value to the organisation

Not all information is of equal value. This will continue to be the case. Indeed, the vast majority of information created and distributed will be of low value or no value to the organisation. Therefore, if information is captured into larger aggregations or 'buckets', then retention and disposal regimes should be applied against the bucket. For example:

Bibliography

1 Vernon, Turner, Gantz, John F., Reinsel, David & Minto, Stephen, 2014. 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things', White Paper, EMC Corporation, April 2014.
2 Gantz, John & Reinsel, David, 2012. 'The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest growth in the Far East', IDC, December 2012
3 Gantz & Reinsel (2012), 'The Digital Universe in 2020'.
4 COGC 2012 Study cited in Tolson, Bill, 2015. 'The Lifecycle of Information – Updated', *Information Governance-101* [website], 20 May 2015.
5 COGC 2012 Study.
6 WittyCookie, 2012. WittyCookie [website] 'What are the major differences among Web 1.0, 2.0 and 3.0?'
7 WittyCookie.
8 WittyCookie.
9 For example, the National Archives of Australia, 2003. 'Overview of Classification for Records Management', July 2003, p.18.
10 Cook, Terry,2009. 'Byte-ing Off What You Can Chew: Electronic Records Strategies for Small Archival Institutions", ARANZ website; Libraries and Archives of Canada, 2015. 'Appraisal Methodology: Macro-Appraisal and Functional Analysis - Part B: Guidelines for Performing an Archival Appraisal on Government Records', LAC website.
11 For a discussion of folksonomies and their application to professional context, see Mathes, Adam, 2004. 'Folksonomies - Cooperative Classification and Communication Through Shared Metadata'. Personal webpage.
12 Snow, Annabel, 2015 [blog]. 'How ontology based search can drive information management', 21 May 2015.
13 Suggestion: Centrally control the upper levels of the folder structure while permitting users to create their own sub folder structures within Year or Subject based folders. Based upon the reporting cycles (such as Calendar and Financial Year), mark the previous folders as read-only and create a new set of folders for the new period. Over time, read only folders can be archived off the network drive or disposed.
14 Archives New Zealand, 2014. 'Appraisal Statement', March 2014, Version 1.0., p.6.
15 Cisco, Susan, 2008. 'How to Win the Compliance Battle Using 'Big Buckets', Information Management, ARMA, July - August 2008.

High investment options	Low investment options
Apply disposal schedules against functions and high level processes, for inheritance by lower level project and matter-based folders. Archives New Zealand on Appraisal: "The quantity of records and information created is increasing and even with reducing costs of digital storage, so too are the costs associated with long-term management and preservation … We are of the view that historic retention practices are neither sustainable nor justifiable …"[14] On improving compliance by employees and by automated tools: "Applying the big bucket approach when developing or updating retention schedules results in significantly fewer record series or 'buckets' and improves the ability of a user or an automatic classification tool to accurately and consistently classify recorded information for retention purposes."[15]	**Apply retention rules** against functions and process based folders. Do not attempt granular differentiation between projects of major or minor importance, or between aggregations of document types. Treat all records of a similar classification in the same way.

Information is a dynamic resource. In the digital world, this principle will become a principle of supreme importance.

Create automated workflows to cover all high-value business processes.

High investment options	Low investment options
Create automated workflows to cover all high-value business processes. Most high-end ECM Systems (for unstructured information) and business systems (for structured information) will support the structuring and automation of business processes. Invest in business process analysis.	**Develop and communicate** simple and clearly understood business processes. Simple and clearly understood business processes will increase the likelihood that information is stored according to business rules. It will also increase the likelihood that your users will find benefit for themselves in adherence to business rules related to information management.

⇛

R·I·M
Professionals Australasia

Directory

Chair
Debbie Prout ARIM
Email prout.consulting@bigpond.com

CEO
Kate Walker FRIM
Email kate.walker@rimpa.com.au
Mobile 0409 250 795

Membership & Customer Services Manager
Maree Cooper
Email maree.cooper@rimpa.com.au

Finance Officer
David Webb
Email david.webb@rimpa.com.au

Marketing & Convention Officer
Kristen Keley MRIM
Email kristen.keley@rimpa.com.au

Branch Manager, & Sales & Sponsorship Coodinator
Wendy Morris
Email wendy.morris@rimpa.com.au

Address for all:
PO Box 276
St Helens TAS 7216

Information consumers respect the rules of the social web. We must move away from simply striving for 'user-friendly' systems. We must create truly 'user-centric' systems that people want and need to use. Once this is achieved, then all the other principles become achievable. If not, then none of these principles will be achievable.

High investment options	Low investment options
Investigate strategies for integrating ECM and business systems and for ensuring that information compliance regimes can occur without the user being aware of them. In the Web 1.0 paradigm, the pendulum of IT investment swung backwards and forwards between 'best of breed' (ie, let's buy as many specialised systems that we think we need) and enterprise-wide systems (ie, let's streamline all our systems into a small number of systems that provide most but not necessarily all the features and functions that we require). In the Web 2.0 and 3.0 paradigms, users are (effectively) beyond the control of command-centric IT departments and executives. Therefore, the information management compliance regimes must occur in the background, whilst in the 'front-end' there must be seamless integration of business systems to permit users carry out their business as effectively as possible.	As above. The strategies required to deliver this principle is the same as required for delivering on the 'information is a dynamic resource' principle.

CONCLUSION

The Digital Age has delivered many technological marvels. It has also created a need within human beings to create and consume ever increasing volumes of information. In the past high-value information was created by a small number of people and managed by specialised information management staff using centralised rules and regulations. However, such information management strategies are impractical in the Digital Age. Instead new approaches are required to manage large aggregations of information rather than rely upon centralised and highly granular classification methods and disposal activities. In the Digital Age, the information manager must move beyond being the information gate-keeper to becoming the facilitator of business processes. ❖

ABOUT THE AUTHOR

Chris Foley BA (Soc Sci), BA (Hons), Grad. Dip. Ed. (Sec), MEd, MA, MIMS has had a life-long commitment to the preparation of high-quality content and the delivery of training services. He also holds Australian vocational training qualifications: Certificate IV in Training and Assessment and Diploma of Training and Assessment. Over a 20-year period, Chris has worked as a university college tutor, school teacher, records manager and archivist, and IT consultant and trainer.

✉ He can be contacted at chris.foley@foleybusinessconsulting.com

RIM Professionals Australasia supports members' professional development throughout their careers

Records Officer

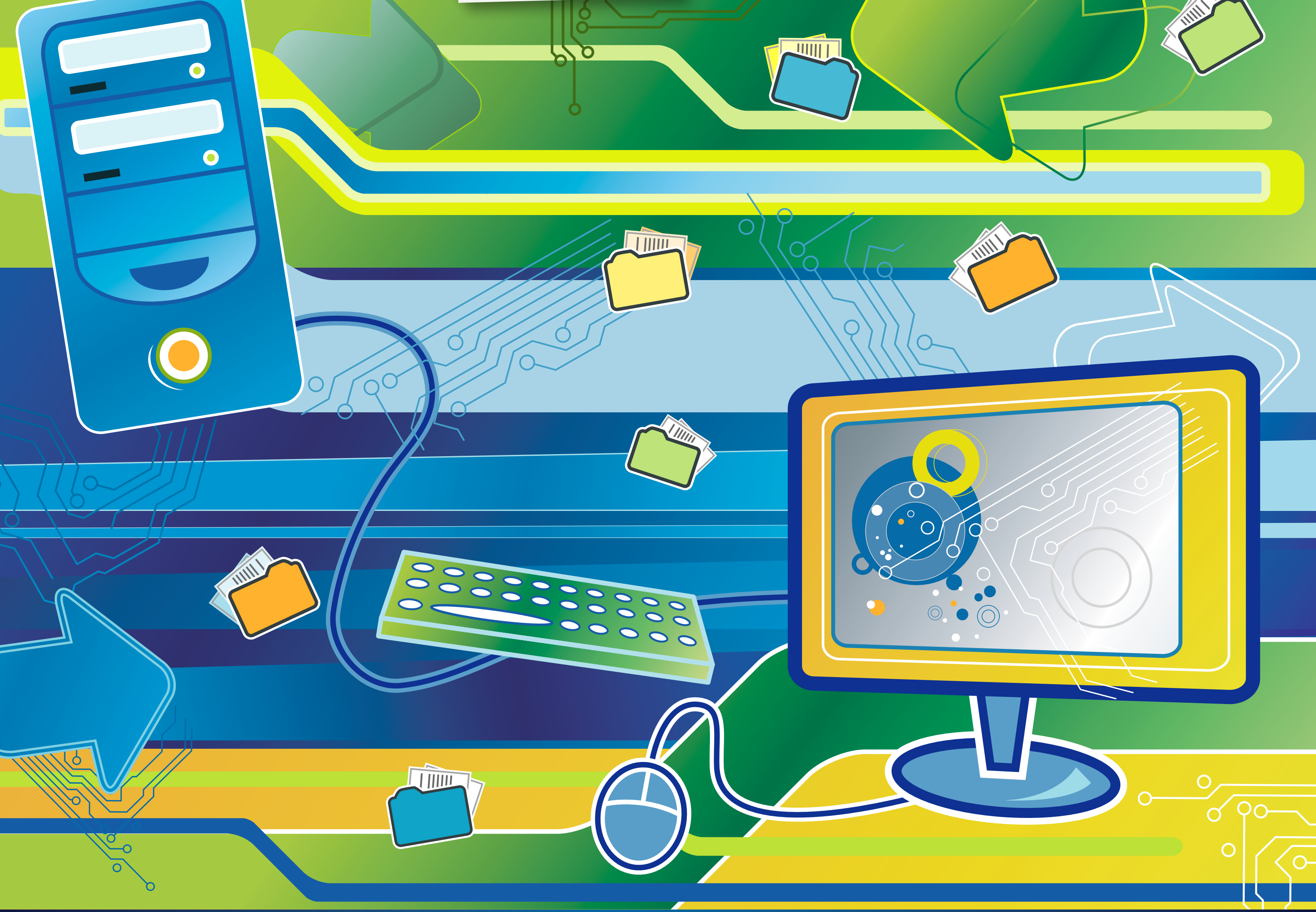
Records Coordinator

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/