idm.
information & data manager
OCTOBER-NOVEMBER 2023

The Robodebt Aftermath

Reflections on the Future of AI in Government

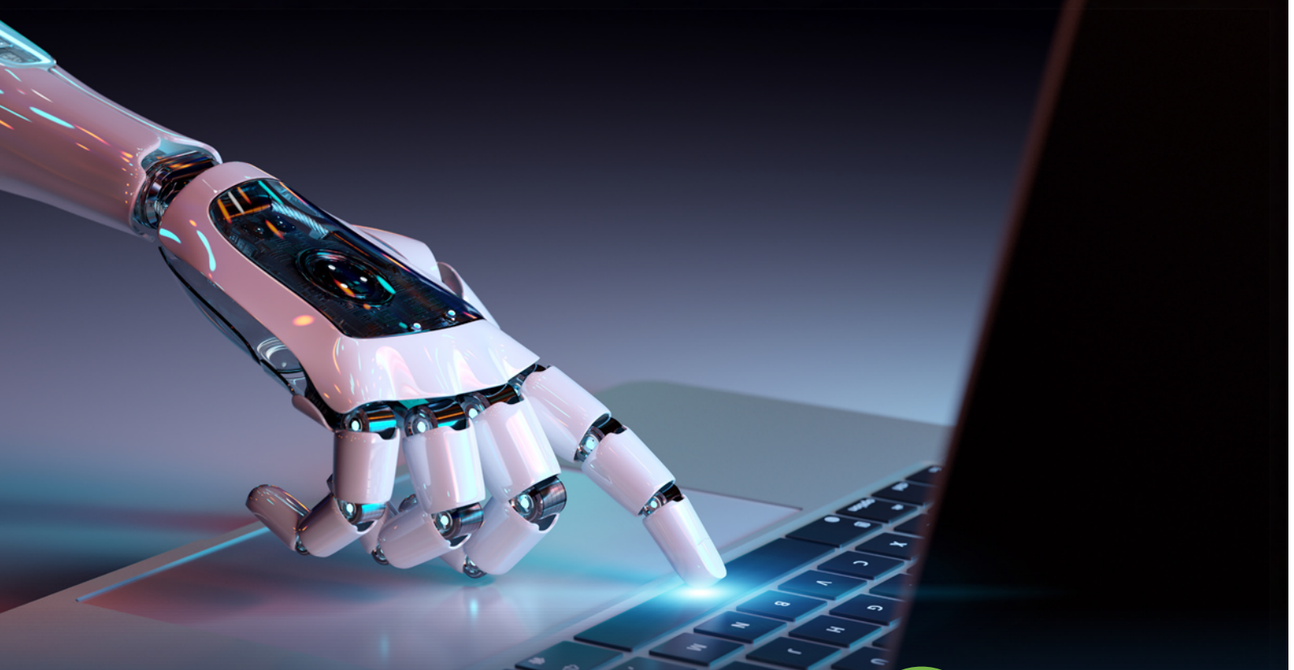
Why It's Time To Rethink Your Scanning Operation

Content Everywhere - A Scalable Plan Leveraging the Best of Purview

AFP Modernise Record-Keeping with $A3.6M Deal

Is Business Serious about Generative AI?

GONE DIGITAL
but still doing manual data entry?



ezescan.
Automated Intelligence

- Process Automation
- Corporate Email Capture
- eForms Capture
- Digital Mailroom
- Backscanning Projects

Call: 1300 EZESCAN (1300 393 722)
www.ezescan.com.au

Data Subject Rights Penalties Will Exceed $US1B by 2026: Gartner

By 2026, fines due to mismanagement of subject rights will have increased tenfold from 2022, to total over $US1 billion, according to Gartner, Inc.

Gartner defines subject rights requests (SRRs) as a set of legal rights that enable individuals to make demands and, in some instances, changes for clarity regarding the uses of their data.

"For security and risk management (SRM) leaders in B2C organizations, automating subject rights or consumer privacy rights management has become a basic requirement and a prerequisite for building trust," said Nader Henein, VP Analyst at Gartner.

"The management of SRRs can enhance customer trust levels by providing a positive privacy user experience (UX)."

However, inefficient handling of SRRs and an immature privacy UX can erode the benefit from millions of dollars spent on developing positive customer sentiment.

Business Impact of Poor or Inefficient Handling of SRRs

Organizations handling data must address SRRs in a defined time frame. Poor or delayed responses to SRRs can negatively impact an organization's trust with its customers.

As a result of long waits for a response, customer experience (CX) and sentiment are also negatively impacted. In addition, regulators regularly impose fines for failure to comply. These rulings also mandate prompt execution of requests.

SRM leaders should take the opportunity when they receive an SRR to engage with privacy-aware customers.

"Data subject rights should not be treated exclusively as a legal requirement," said Henein. "To support positive customer sentiment, the organization's privacy UX should be developed with the same care as any customer-facing service."

In addition, many jurisdictions require digital organizations

to address the privacy rights of their employees. Data held on incoming, current, or past employees is worthy of the same care as data pertaining to customers.

The highest cost per request is often attributed to employees' SRRs rather than those coming from customers due to the complexity and the volume of data.

"To ensure data subjects receive responses within acceptable time, cost, and scale limits, SRM leaders should consider establishing a foundation of metrics around SRRs," said Henein.

The Evolution of SSRs

"While the need for scalable subject rights delivery and fulfilment will not go away, the demand for more automation will lead to a faster move toward a zero-touch model," said Henein.

"This model will enable users to self-serve informative rights through a privacy portal where individuals will be able to browse their information in detail and understand how it is being used and by whom."

Maintaining a manual SRR process renders an organization more likely to face regulatory fines and suffer associated reputational damage. It also entails maintenance costs.

By contrast, being transparent about, and involving customers in the SRR process and implementing a more automated approach to SRR fulfilment offers clear benefits to organizations.

idm.
information & data manager

Publisher/Editor: Bill Dawes
Email: bill@idm.net.au

Web Development & Maintenance: Cordelta

Advertising Phone: 02 90432943
Email: idm@idm.net.au

Published by Transmit Media Pty Ltd
PO Box 392, Paddington NSW 2021, Australia

All material in Information & Data Manager is protected under the Commonwealth Copyright Act 1968. No material may be reproduced in part or whole in any manner whatsoever without the prior written consent of the Publisher and/or copyright holder. All reasonable efforts have been made to trace copyright holders. The Publisher/Editor bears no responsibility for lost or damaged material. The views expressed in Information & Data Manager are not those of the Editor. While every care has been taken in the compilation of editorial, no responsibility will be accepted by the Editor for omissions or mistakes within. The Publisher bears no responsibility for claims made, or for information provided by the advertiser.

Cloudy future for NACC with Kapish

The National Anti-Corruption Commission (NACC), a new Australian Commonwealth agency that began operating from July 1, has turned to the cloud for its enterprise software under long term contracts with Kapish and TechnologyOne.

TechOne OneGov Ci Anywhere will be provided under a Software as a service (SaaS) contract with an annual subscription including one-off implementation consultancy service for just over $630,000. TechnologyOne will also provide Online database information retrieval systems under another $780,000 contract.

Legislation to create the agency only received Royal Assent on December 12, 2022, with the agency beginning operations just over 6 months later. The NACC incorporates the previous Australian Commission for Law Enforcement Integrity, which is no longer operational.

Kapish announced it has signed a 3-year contract with the NACC to provide Content Manager Cloud and has worked with them to ensure their required solution was deployed, secure and live to meet the Commission's tight timeframes. Kapish will supply its OpenText records management solution under an annual Software as a Service contract worth almost $220,000 for the first 12 months.

Compliant with global information management government standards such as ISO15489, ISO16175 and ISM-PROTECTED (IRAP-ASSESSED), Kapish Content Manager Cloud is promoted as a one-stop-shop for information governance compliance. It offers support for both Manage in Place and centralisation for the management of records.

The NACC was formed to investigate issues of serious or systemic corrupt conduct in the Australian Government public sector.

The NACC announced on August 1 that it has already received over 500 referrals since commencing operations on July 1. The commission said about one in eight of the referrals related to matters "well publicised in the media".

The NACC can only investigate matters relating to Australian Government public officials.

It will not be able to investigate concerns relating to state, territory or local government officials.

Kodak Alaris Creates New IDP Division

Kodak Alaris has announced the formation of a new dedicated Business Solutions organization supporting the company's goal to accelerate growth within its adjacent intelligent document processing (IDP) offerings, including its IDP software Kodak Info Input Solution, INfuse Smart Connected Scanning Solution from Kodak Alaris, and related professional services.

Angelo Krstevski, GM ANZ, Kodak Alaris, said, "Kodak Alaris will continue to invest in the region, and it is confident that there is a growing demand for its intelligent document processing solutions."

The new Business Solutions organization will be re-focussing its go-to-market strategy across pre-sales, sales, business development, professional services, marketing, and product management, to bring more rapid, compelling business outcomes to partners and customers.

The new Business Solutions organization together with the Australia & New Zealand Team will focus on helping customers to realize the full potential of Kodak Alaris' intelligent document processing solutions.

"We are excited to announce the formation of our new dedicated Business Solutions organization. This investment is an integral part of the company's growth plan and supports our strategic goals to target new markets, build new partnerships, and reach new customers," said Don Lofstrom, President, and General Manager at Kodak Alaris.

For more information, visit https://www.alarisworld.com/

If you are a business in Australia or New Zealand looking to learn more about Kodak Alaris' intelligent document processing solutions, contact the Kodak Alaris Australia & New Zealand Team at Email: service-anz@kodakslaris.com or Dial Toll Free: 1300 252 747

Judo Bank and REX caught in data breach

Two new Australian companies have announced potential exposure in the data breach by law firm HBL Ebsworth which has already compromised more than 40 government agencies.

Regional Express (Rex) airline announced that one of its subsidiaries has been a victim of the cyber-attack.

"The incident resulted in the theft of data relating to confidential exchanges between Rex's subsidiary and its client. As far as Rex is aware, Rex Airlines is not affected, and no passenger details have been compromised," the firm said in a statement.

"Rex is now requesting for evaluation of the documents that have been stolen from HWLE's servers to determine the extent of potential damages to Rex's interests.

"Rex has put both HWLE and the client on notice of the potential damage to Rex's interests and has reserved all its rights."

Rex is Australia's largest independent regional and domestic airline.

Judo Bank has also announced it is affected, having used HWL Ebsworth Lawyers (HWLE) as a legal service provider for a short period.

"Judo Bank's systems were not impacted and remain secure," the bank stated.

"Judo Bank has provisionally, and where required, contacted our customers and employees who we understand may have been impacted by this incident.

"Judo Bank is continuing to work with HWLE to ensure affected individuals are formally notified under the Notifiable Data Breaches scheme."

Organisations previously going public as victims include the government of Tasmania, the Fair Work Ombudsman, and the NDIA.

Air Marshal Darren Goldie - Australia's new National Cyber Security Coordinator - has confirmed multiple government departments and agencies have been affected by the attack on HWL Ebsworth in May.

There must be a better way?

Scanner Rentals
POWERED BY ezescan.

✓ The Right Scanner
✓ Expert Advice
✓ Quick Deployment
✓ EzeScan Software
✓ Pay As You Go
✓ No Warranty Hassles

Call: 1300 EZESCAN (1300 393 722)
www.ezescan.com.au

Digital Transformation? How about Information Transformation

By Sean Burgess, EncompaaS

Digital transformation is still one of the buzz phrases of the IT industry. An umbrella term with so many nuances that it makes it difficult to start a constructive conversation, particularly when it comes to information governance and data protection. Where do you start?

Having been part of the content services, information management and governance community for over 10 years now, I come across many organisations who are experiencing the challenge of balancing old with new, decommissioning the old, or giving the old a makeover. Essentially, they're trying to transform…digitally.

In fact, keeping the legacy around for a while might be a good thing. In 2022, vinyl records outsold CDs for the first time in decades, showing that sometimes the old can be cool and useful.

Music, clothing, films, content repositories… It's a big decision to turn your back on a parka coat when you might need it at some point in the future when you see Liam Gallagher in concert. You have to be sure that when you replace it, you've got something ready to transition over to that suits your needs.

The challenge that many of my clients face is the ever-accelerating growth of a demanding customer base and the requirements to change to align with that demand. Partner this with a plethora of legacy platforms, full of information (often critical and personal) that already have complex integrations that now need to communicate with newer age technologies that need access to that key information.

Organisations are now juggling M365 alongside the non-M365, with content spread across many silos. Spinning those plates when it comes to information management becomes very difficult.

With an estimate that 80% of information is unstructured and that volume continues to grow, as managers of information it comes with a requirement to go on a journey of information transformation.

The growing digital heap brings both challenges and opportunity, as there are great insights locked within documents that can bring value to your organisation if you have your information visible and under control.

Take Microsoft Teams as an example, with 270 million daily active users of Teams in 2022 and a huge number of documents being shared across the platform, it creates a necessity to manage and govern the information that's being shared.

Multiply that across your information architecture and it creates a productivity, cost, and risk headache. It's already difficult enough to manage and govern the information that you do know…but what about the unknown?

Before embarking upon information transformation, you first need to understand what you have and where it is – only then can you really know what can go in the rubbish bin (securely), what you can apply retention to and what strategic decisions can be made around your information.

When a lot of data is unknown, there may be critical documents or data that are tucked away in the wild that make achieving these impossible. With knowledge being key, having a holistic visualisation of all your information sources before making important, strategic decisions is paramount; and by having all this intel in the same place, you no longer have to be afraid of the dark…data.

I refer to this as "the blueprint" – know what is stored and understand your information value and risk together, showing your SharePoint Online footprint and Teams information alongside your legacy content and network drives.

Doing this in an automated way, without user input, takes away a lot of discovery and operational costs. By having content policies and classification in place centrally, you are then able to report back within your organisation findings and strategy to help with compliance and governance, whether it be regulatory or internally driven.

Not to mention peace of mind in knowing that you can centralise policy management from one screen, whilst keeping the content in place, taking away change management from end users and increasing productivity.

Creating that blueprint presents endless possibilities – a rich, visible landscape that enables you to derive value from your information, whether that be looking at things from a governance angle (retention, defensible disposal or relocation) through to beginning to actually use the value within your documents to drive processes (faster data access for SARs, FOIs, eDiscovery).

Now, is this information transformation I speak of an easy task? Absolutely not, however the great part of it is that it has a clear, structured approach that enables you to bite off one piece at a time when negotiating the challenging roads that will appear. However, the long-term benefits in productivity, cost, and risk that this transformation can bring are significant.

At a high level, I see four key pillars to achieve this:

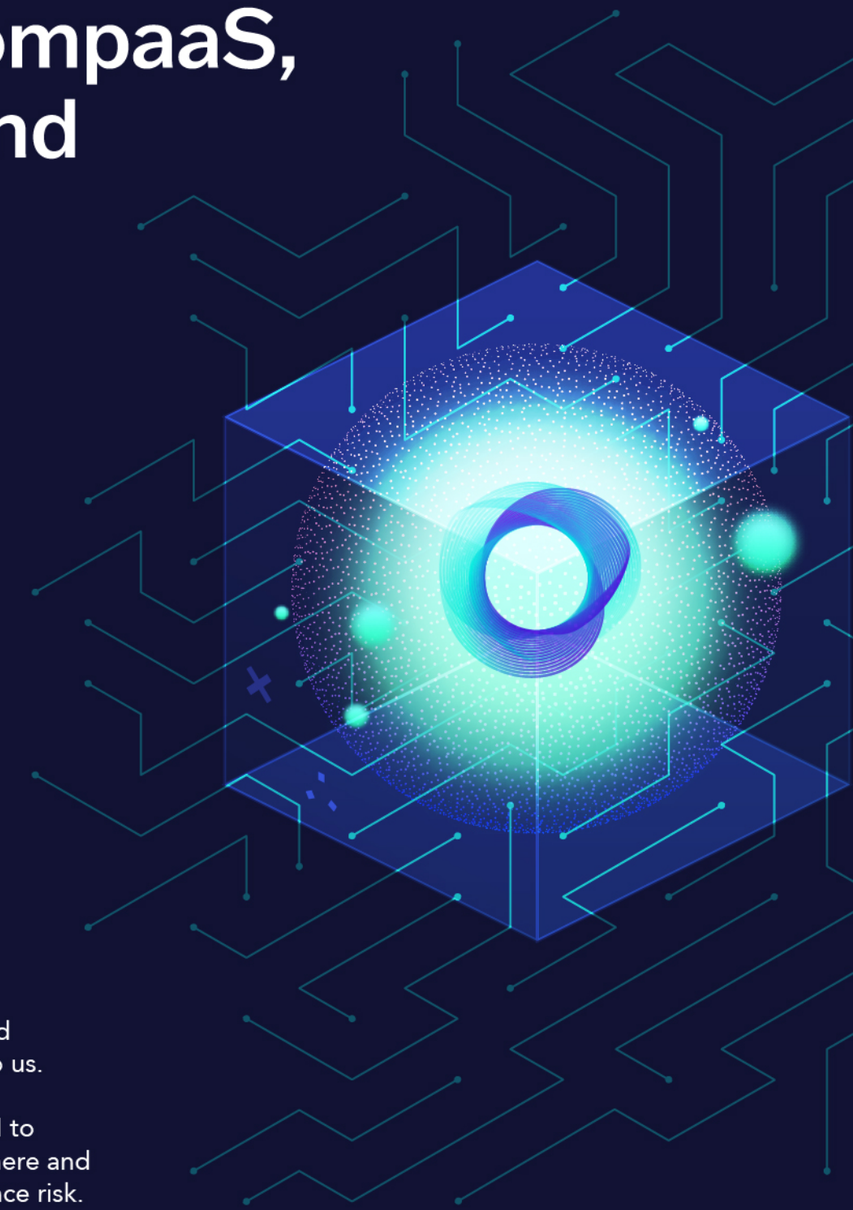
- **Discovery:** Having visibility of your information across all sources, in real time.
- **Understanding:** Identifying and classifying at-risk personal data.
- **Governance:** Automating retention, disposition, and relocation.
- **Utilisation:** Empowering end users with the right information at the right time.

Elements 1 and 2 are the most important, as well as the blueprint that I mentioned, to achieving a strong foundation to progress with. From there, the fun begins!

Sean Burgess is Sales Lead at EncompaaS. Send an email to sean.burgess@encompaas.cloud for more information.

For information management, AI is a trendy topic.

For EncompaaS, it's second nature.



We transcend buzzwords and hype because AI isn't new to us. Our customers are already benefitting from next gen-AI to harness information everywhere and reduce privacy and compliance risk.

Unlock the latent potential of information with EncompaaS.

encompaas.cloud

Australian Federal Police Modernise Record Keeping with $A3.6M Deal

Two years after a scathing report from the Australian National Audit Office (ANA), the Australian Federal Police (AFP) has issued two contracts worth over $A3.6 million dollars to implement records management systems from solution provider iCognition and local AI developer CastlePoint.

In 2021 the ANAO published a report critical of the AFP's record-keeping processes and practices, including its extensive use of file shares, and recommended the implementation of an Electronic Document and Records Management System (ERDMS)

It found that "The AFP's poor digital record-keeping is a risk to the integrity of its operations."

Despite a project that commenced in 2015 to migrate to an EDRMS, it found that the AFP still stored the bulk of its information on shared drives, a web-based collaboration tool and the PROMIS Case Management system.

The ANAO stated that "As a matter of urgency, the Australian Federal Police should implement an Electronic Data and Records Management System (EDRMS) to allow it to store records so that they are secure and readily accessible.

"... [it] keeps more than 90 per cent of its digital operational records in network drives which are not considered by the National Archives of Australia (NAA) to be appropriate for that purpose.

"Records in network drives are not secure from unauthorised access, alteration or deletion.

"The AFP does not have the capacity to identify all digital records that it holds on any individual or entity.

" ... the AFP does not have an EDRMS and by its own reckoning, 'has digital records in approximately 700 business systems'.

"The AFP has a number of network drives but the main drive is known as the S drive. The AFP advised in October 2020 that the S drive contained approximately 680 TB of data. There are no mandated naming conventions for the S drive and officers are free to create folders as and when they choose.

"There are a total of 137,111 folders in the S drive. Some of these folders bear simply a Christian name or surname, and others had names such as Ideas 'n stuff, Old stuff, Misc, Junk, My music and Footy tips 2002."

Police Commissioner Reece Kershaw responded that while "the AFP accepts that the distributed nature of information holdings within the AFP posed challenges for the ANAO's independent verification of material. Pleasingly, the AFP is unaware of any instance where it could not produce a document requested by the ANAO with the exception of one original affidavit retained by the issuing officer.

"Further, when drawing conclusions on record-keeping, it should be acknowledged that policing and court processes remain heavily dependent on paper-based records. For example, paper-based warrants remain a necessary feature of policing."

Kershaw promised the AFP would establish a "dedicated implementation team" to respond to the findings of the ANAO report, which cost $A532,000 to produce.

The AFP has 6,834 staff of which more than 4000 are either police officers or protective service officers.

iCognition has been issued a contract worth $A2.7 million running over three years from August 2023. The firm is a specialist reseller and integrator of OpenText Content Manager, and has overseen over 500 enterprise information and governance implementations in the last two decades.

It also offers as a range of add-on solutions for Content Manager that enhance workflow, collaboration and connections to other line of business systems.

iCognition will be working together with Castlepoint which has been issued a contract worth $918,218 over the same period.

Castlepoint offers an AI platform to manage retention and disposal across shared drives, legacy EDRMS, Office 365, business systems, cloud-hosted systems, and other business systems. It claims that two thirds of Australian federal government portfolios have implemented its AI-driven platform.

INGRESS
by iCognition
The next generation Content Services Platform has arrived!

Find the right information at the right time.

UPGRADE TODAY

Fast track your information, securely!

- Build and deliver your own content services within corporate apps.
- Find, secure and protect your vital and sensitive records, regardless of where they live.
- Supercharge your digital transformation and prevent risks.
- Ensure your vital information is always safely managed in the latest software.

iCognition's trusted service offers:

- Secure to government Protective Security Policy Framework standards.
- ISO27001 Information Security Management Infrastructure.
- IRAP security assessed to the level of PROTECTED.
- Support team available 24/7.

DISCOVER | PROTECT | SECURE | USE

1300 426 400
icognition.com.au

iCognition MICRO FOCUS is now opentext Azure ISO 27001 INFORMATION SECURITY

The First 6 Months of a Data Governance Initiative

By Nicola Askham

If you're considering starting a Data Governance initiative, you may be wondering what the first six months of work might look like – and that is a very good question because it is challenging... and even though I have done it many times before, sometimes it still surprises me exactly how involved and challenging those first few months can be!

Here I am going to set out roughly what you should expect when on your Data Governance journey – but please remember, this is just a guide based on my many years of experience, every organisation and therefore every Data Governance initiative is different. The first thing I was you to remember is that data governance is all about cultural change and therefore you're probably not going to get things within your organisation moving very quickly and one of the very first things you need to do is manage the expectations of whomever you're reporting to and what you're trying to do. Six months down the line you're not going to have a fully embedded data governance framework, but you will have designed and begun the implementation process.

Early Days

It's important they understand why your company is doing Data Governance, and why your role is being created, because once you understand those drivers it makes it much easier to engage with and sell your Data Governance initiative to senior stakeholders. This is what you will spend some of the first month of your journey doing – establishing and selling your 'why'. What we're talking about is speaking to senior people within your organisation and talking to each individual to understand what their challenges are, what their views on data at your company, what challenges have they got.

Use their feedback to build your framework and work out which bits of Data Governance you need in place and establish which parts you are going to focus on first. So, once you've designed something, the next stage is to start socialising it with the senior stakeholders and get them to really buy into it and let them think that they've helped shape it and their input into it, because it's going to address the issues they've brought to your attention around data.

Once you've done that then you need to try and get them engaged and explain to them that it's not going to be quick - you've not got a magic wand that you're going to wave... but you're going to be able to try and put in place some frameworks and processes and roles and responsibilities that should ease the pains of some of those challenges.

Next Steps

In the next stages of your Data Governance journey, you are going to start fleshing out some of those roles and responsibilities and perhaps even start working on a data glossary. This is another great way to ensure team members and senior stakeholders feel engaged in the process, as you'll need their input to flesh out these things to ensure everyone within the organisation is singing from the same hymn-sheet.

Appointing the wrong people to key roles can cause the wheels to come off any well thought out initiative pretty quickly. So, getting the basics right and the most effective and suitable team in place from the outset will stand you in good stead for successful data governance implementation. In order to appoint the most appropriate people to these roles, it is important to understand what they involve and what their responsibilities will be.

From the top to the bottom of an organisation, it is crucial to your data governance initiative that you identify fit and proper people to take on each of these important roles and that they also understand what role each other plays in the big picture. Again, getting the basics right and the most effective and suitable team in place from the outset will stand you in good stead for successful data governance implementation.

Now, this article is titled 'What to Expect in the first SIX months of your Data Governance initiative' and you are probably wondering why the creation of these things would take up such a large chunk of time and it is understandable that people look for ways to quicken this process up. One of the ways I am often asked if this can be done is by fast-tracking the creation of items like a data glossary by using standard definitions.

However, it's not a part of the process that can be skipped or glossed over, so to speak. Part of the reason for this is that organisations, even those within the same industry, very rarely use the same terminologies in exactly the same way. This means there is no bank of standard definitions to pick and choose from; what works for one will very rarely work for the next. Only by creating your own data glossary can you be sure that everyone fully understands the definitions within it.

Moving On

The next step may possibly be to implement a data quality issue resolution process because whilst you're doing the initial engagement, maybe creating conceptual data models, people will be starting to tell you anecdotes - their data quality horror stories - and this is a great time to start identifying where some of your biggest quality issues lie and begin logging which of them need investigating and fixing. You're not going to solve everything in six months, but at the very least, I would start logging issue and once I've designed my process for investigating and resolving them, I would roll the process out on a phased basis for key consumers of data first.

Full Circle

You may not feel like this is very much to have achieved in six months, but trust me, from my years of experience I can assure you it is. And to bring you full circle, please remember – you MUST manage both you and your organisations expectations when it comes to the early phases of implementing your Data Governance initiative.

You're dealing with people and organisational change. It's going to take time and don't underestimate the amount of energy and effort it will take. I think a lot of people just assume that they can sit at their desk, design a framework, send it out and people will start doing things.

It takes a huge amount of effort and energy and preparation. It's a standing joke that my husband believes that what I do is go to meetings! In reality what I'm doing is meeting people and trying to influence them to change their behaviours - and I'm not going to do that sitting at my desk sending out emails.

At the end of six months, if you can have designed your data governance framework perhaps created a some conceptual data models and use that to identify and agree data owners, you'll be doing really well.

Originally published on www.nicolaaskham.com

opentext™

Australia & New Zealand

CONTENT MANAGER

Customer Innovation Showcase 2023

Register Now

Wednesday, 22 November
1:00 PM AEDT Virtual

OpenText Content Manager Customer Innovation Showcase recognises and celebrates users, practitioners and implementers of Content Manager in their organisations to manage and govern information — those that harness and exploit OpenText technology to advance information management for the digital transformation age.

Join this virtual annual showcase event to discover OpenText's expanded portfolio for information management and governance and gain insights into how others are successfully managing and governing their data.

Smarter Information Management with OpenText.

The Robodebt Aftermath:
Reflections on the Royal Commission and the Future of AI in Government

The Robodebt Royal Commission, conducted in the wake of Australia's controversial automated debt recovery system, unveiled a troubling saga of governmental overreach and systemic failures. Like other public sector information and records management professionals, Alyssa Blackburn keenly followed the lengthy proceedings of the Commission and what it exposed in terms of inadequate practices. Alyssa, who has worked in senior roles in state and federal government agencies, is currently Director, Information Management at AvePoint. She spoke with IDM publisher and editor, Bill Dawes.

IDM: Alyssa, The Commission's findings exposed a flawed algorithmic approach that wrongfully targeted thousands of citizens, causing undue stress and financial hardship. It revealed that the system lacked proper human oversight and was built upon shaky legal foundations, ultimately leading to the government's decision to repay over $A1.2 billion in unlawfully collected debts. You've looked closely into what led to the downfall of the Robodebt scheme. What have you found were the principal flaws in information and data management?

AB: I've thoroughly immersed myself in this topic by reading the report, listening to numerous podcasts, and I'm just three YouTube videos away from watching all the actual transcripts. As an ex-public servant, I can confidently say that it represents a massive failure in government administration. If organizations, especially government ones, fail to learn from this, it would be an even bigger tragedy.

One significant failing is the refusal of many senior public servants to create any records. Catherine Holmes, the Commissioner, highlighted this issue in both her report and the video evidence. She even expressed disbelief, wondering why there was such a reluctance to put anything in writing. She mentioned that it doesn't even have to be pen to paper; simply putting fingers to a keyboard would suffice. The absence of documentary evidence leads to situations where conflicting claims are made without any means of verification. The Commissioner often pointed this out when questioning witnesses, emphasizing that supporting documentation was not available to back up claims being made. This raises questions about information management and how it impacts the integrity of government processes and decision-making. When organizations adamantly resist creating records, information managers face the challenge of reconciling this conflict, as there's no information to manage in the first place. There was a refusal to write anything down or as, as the Commissioner says, put a finger to keyboard. How do we prove integrity of process or decisions without appropriate evidence?

The next issue I noticed, is something that resonates deeply with those of us who have worked in information management in the public service. The Commissioner highlights it right at the beginning of the Robodebt report and again towards the end – the extreme difficulty the Commission faced in obtaining information from the department. While the Commissioner attributes this to a deliberate attempt to withhold information, my perspective is slightly different. I believe it's more a consequence of information being scattered across various systems, saved in obscure email folders, buried in file shares, or even left unorganized on individual desktops. It's possible that even when the information is in the right system, it's poorly labelled or organized, making it hard to locate. There may also be limitations in the systems' export capabilities.

As an information manager, I don't interpret this as a deliberate act of concealment. Instead, it seems to stem from the inherent challenges within their information management systems. These difficulties raise significant concerns for government organizations, given the increasing frequency of royal commissions or other investigations or legal cases. For government departments, it's only a matter of time before you have to produce evidence for such a commission or similar process. Ensuring easy and efficient access to information for these purposes is critical.

Additional issues with accessing information was a situation involving Kathryn Campbell, the former Deputy Secretary of the Department of Human Services, who struggled to access information from her electronic calendar. In this scenario, an attempt was made to export the calendar into an Excel spreadsheet, but it only provided basic information like meeting titles and dates. Crucial details such as the attendees or references to specific documents were missing. This inability to retrieve vital information raises questions about technical obsolescence and inadequate information management practices.

Further to that, there was a situation where a time zone difference led to misunderstandings. A witness was asked to produce information and this person was based in Western Australia. This meant the timestamps on emails were different, and concerns were raised as to why they were receiving emails at 3:00 in the morning? It turned out it wasn't 3:00am, they were just in Perth. This highlighted the importance of metadata and how it was examined in the Commission.

Lastly, the Commission extensively discussed the suicides associated with Robodebt. While it's challenging to attribute all of these directly to Robodebt, there's a clear link between the system and some individuals' deteriorating mental health. One case in particular stood out, where the individual ultimately did not owe any debt. This person had provided an employment separation certificate showing their employment end date, but the system couldn't process that information due to the unstructured nature of the data. The system's limitations, inability to access unstructured data, and lack of proper data utilization resulted in a series of failings. These failures, as the Royal Commission rightly pointed out, contributed at least in part to the tragic death of this individual. It's nothing short of a heartbreaking tragedy. The department had the information to make better decisions but either chose not to use it or didn't design the systems to utilize it effectively. Organizations must have access to the correct information to make good decisions and this clearly was not the case in this scenario.

IDM: The Royal Commission struggled in following decision-making across the agencies involved in Robodebt, does this surprise you considering the technology platforms you would expect they would have had available to them?

AB: Indeed, the technology is readily available, and it has never been more accessible. As someone who's always on the go, I find myself constantly juggling tasks. (To demonstrate the insanity of this, I'm going away this Friday, and I have an enormous cabbage I have grown, that I must use up. If I don't turn it into several jars of sauerkraut, I can't go on holidays). So, however crazy that is, I'm accustomed to multitasking and staying organized.

One of the technologies I find immensely helpful is voice notes. I can easily record voice memos and email them to

Alyssa Blackburn, Director, Information Management at AvePoint

myself as reminders or for documentation purposes. This approach is far from reverting to traditional file notes, a concept well-known to public servants. Instead, it's about leveraging the technology at our disposal to streamline our processes. After a meeting or conversation, I can quickly record a voice note summarizing what occurred, which can then be emailed and stored in the appropriate location.

I work with a colleague who has dyslexia, and note-taking during meetings is a significant challenge for them. To accommodate those needs, we utilize technology during our meetings. For instance, we enable the transcript feature in Teams, which provides a clear record of what transpired in the meeting, including action items. This approach allows everyone to engage effectively. The technology is here, it's accessible, and it's more user-friendly than ever before. However, it appears that many organizations aren't taking advantage of it as they as they could be.

IDM: The Royal Commission made recommendations about the management of information, or lack thereof, in this case. What do you see as the most important of the recommendations they made?

AB: I believe the most crucial aspect to consider, although these specific words may not have been used in the Robodebt inquiry, is to respect the integrity of our information. It's essential to demonstrate that our information is accurate, correct, and appropriate. This extends to the integrity of our decision-making processes, using the available information as evidence of our sound decision-making.

Some of the recommendations made by the Royal Commission emphasize the importance of organizations taking the creation of records documenting business evidence, decisions, actions, and transactions more seriously. I think this is particularly vital for government organizations, as they serve the community and owe it to the people to demonstrate that they operate in the most appropriate manner. The only way to achieve this is through the integrity of their information, allowing them to confidently present evidence and decisions made.

Government organisations are essentially service providers. They serve people of the nation, and they owe it to the people of that community to prove that they're doing things in the most appropriate way. The only way that they can do that is to stand up and 'hand on heart' say we've got this. Here's the evidence. Here's the reason the decision was made.

(Continued Over)

The Robodebt Aftermath:

(From Previous Page)

In the case of Robodebt, the lack of transparency and the discouragement of record-keeping created a significant credibility issue. There was a noticeable absence of integrity across various areas, making it impossible for anyone to have confidence in the proceedings. Therefore, the most critical takeaway from this situation is the absolute necessity of maintaining the integrity of our information, which directly influences the integrity of our decision-making processes.

IDM: Tools that prove for AI-assisted workflows are becoming widely available in 2023. Should the Robodebt scandal provide people with a reason to pause and think before rolling them out?

AB: I'm all for technology when it genuinely enhances **pro**cesses. That's where technology shines. However, I also firmly believe that technology must always be accompanied by human oversight. The idea that 'machines will take care of it all' is a misguided.

What we often miss, and this isn't exclusive to government organizations but applies to most organizations, is a clear understanding of the desired outcome when implementing automation. It's not enough to just jump on the bandwagon because something is new and exciting. We need to pause and ask ourselves, 'What does success look like? What should be the ultimate goal?' Without defining these objectives, we end up with subpar systems.

In the context of Robodebt, although it involved automation, it's essential to note that there was no artificial intelligence (AI) involved. However, if they had integrated some AI capabilities, even though it might have been early in the technology's evolution (around 2015/2016), it could have been beneficial. AI excels at processing unstructured data and extracting meaningful information, such as interpreting an employee cessation certificate date. However, AI is most effective when we have a clear understanding of our desired outcomes and continuously monitor and improve it. At this point in time, I don't see AI replacing jobs; if anything, it creates more jobs related to defining desired outcomes, success criteria, and continuous improvement over time.

IDM: That there should have been a human in the loop was a key message from the Robodebt Royal Commission report. Does that mean that that decisions like information classification, retention and disposal made through AI must always be reviewed by a human?

AB: No, I don't believe that every task necessitates human intervention. We should approach this by considering the balance between risk and value.

For example, when we're dealing with situations like potentially charging people with debts that could go back seven years, I would say this is a high-risk activity. In cases like this, human oversight and judgment is essential. On the other hand, if we're using AI for information lifecycle classification, applying classification terms to content that will ultimately be reviewed by a human before disposal, there's a lower risk involved. In such cases, the value of being able to carry out these tasks at scale is significant.

So, it truly depends on the scenario. Not every task requires human intervention, as long as a careful analysis has been conducted to assess the risk and value associated with it.

IDM: Is there a risk in utilizing AI-based classification to classify and destroy data that could one day be requested by a Royal Commission for instance?

AB: If you've followed the proper procedures, including authorized disposal schedules, there's a clear framework for ensuring the defensibility of actions taken. Even if some information requested by the Royal Commission was potentially destroyed, it should not pose an issue if the disposal followed the guidelines set by entities like the National Archives. This of course, must take into account respecting disposal holds or freezes, but there is defence of the disposal activity because you have followed the appropriate processes.

It comes back to understanding and upholding the integrity of these processes. It's about being able to assert, with confidence, that you no longer possess certain information. You can provide a well-documented process, the relevant policies governing it, and adherence to established retention schedules. In such cases, there should be no reason to worry about future scrutiny or the need to hold onto information indefinitely.

If someone feels the need to hold onto information for fear of a future Royal Commission, it's a sign that they may not be following the correct procedures from the start, and that's something that should be addressed immediately.

IDM: One of one of the key recommendations of the report was a national body to monitor and audit automated decision making. How do you see that working on?

AB: I understand the perspective behind this, but I see it as part of a broader issue. While I hold Commissioner Holmes in high regard and believe she conducted the Commission exceptionally, I don't think it's sustainable to have a single entity solely responsible for overseeing automated decision-making processes. Instead, we should consider whether this oversight belongs elsewhere within the government structure.

Maybe it's the Office of the Information Commissioner or the Digital Transformation Agency? The exact placement isn't for me to decide, but should there be policy? Should there be guidance? Should there potentially even be legislation to define whether or not a decision made by a computer is actually a decision versus a decision made by a person?

I think that there's absolutely value in having more guidance for the public sector on what this could entail. Whether it should be a standalone agency, I'm not sure. That's something for the federal government to consider. However, I definitely agree that guidance, policy, and principles are absolutely required.

IDM: Lastly, what are the lessons the private and public sectors can learn from the Robodebt scandal?

AB: Information is vital. Therefore, regardless of the industry, whether it's the commercial sector or the public sector, the management of that information is vital. Good information allows you to make good decisions. The absence of good information can lead to situations like Robodebt, which, as I mentioned earlier, represents a massive failure in public administration in Australia.

Information stands as the most valuable asset within any organization. It's high time that organizations, be it public or private, wake up and recognize this fact.

Content Everywhere - A Scalable Plan Leveraging the Best of Purview

By Shimron Shimla, EncompaaS

In one sentence, Records Management in Place (RMIP) is traditionally described as Records Management systems that can connect to other Systems of Engagement, to keep your content compliantly managed as mandated, and close any risks or gaps in an integrated and seamless manner for end-users.

Customers adopting RMIP are most commonly seeking to achieve the following:

- Gain visibility into records and manage retention, transfers, holds, and disposition from virtually any system in the business from ONE central place and get a complete and contextual view of all information assets.
- Be able to leverage new tools released to market, without worrying about their native recordkeeping compliance, as mandated by the legislative bodies of the sector or region.
- Decommission systems no longer used, without having to manually copy items into the records corpus for compliance purposes.

Sounds perfect, right?

There are, however, some threats that are emerging in the industry of recordkeeping that are easy to overlook when you first venture into RMIP.

There are also many hidden benefits you have yet to consider or encounter.

If you're ready to dive in, then let's start with an example of a fictitious, yet remarkably common scenario:

The Customer invested in an Electronic Document and Records Management System (EDRMS) 10-15 years ago and users were trained to save their content inside. It was a better experience than using file shares which was the other alternative at the time.

It had version control, metadata, search, etc., but file shares were still occasionally used for saving content, including documents.

Over the years, new systems were introduced by the Customer to solve a certain business challenge (CRM systems, ERP systems, HR Information system, several custom-built web applications for both internal and external use, etc.).

Gradually, users started treating the EDRMS as a "final resting ground" for the content they created in other systems. Some documents were converted to PDF and uploaded to the EDRMS by staff members that acknowledge the importance of proper recordkeeping compliance... typically by records managers or members of the Legal team...

Recently, the Customer has procured Microsoft 365, offering more advanced document management and collaboration capabilities (co-authoring, offline access, enterprise search, etc.).

In addition, The Customer now also has access to Purview, allowing them to manage records in place inside M365, classify them, label them, and ultimately dispose of them.

Now, the Customer is looking into a new System of Record to work with Purview, and after spending substantial budgets on maintaining the EDRMS system, decides to take up an evergreen cloud based RMIP system as part of their new IT transformation project! (...sounds familiar??)

(Continued Over)

Content Everywhere

(From Previous Page)

So, by now, the Customer's application portfolio includes at least the following information systems:

- 1 x Traditional EDRM
- 1 x Online SaaS CRM
- 1 x Legacy CRM
- 1 x Online SaaS ERP
- 1 x Legacy ERP
- 3 x Network File Shares (commonly referred to as the "Home" or "H:" drive)
- 2 x Legal Case Management Systems
- 1 x Human Resources Information System
- 3 x Custom / Legacy Web Applications, some with external users' access
- 1 x Microsoft Office 365 tenant, including:
    - 2,000 SharePoint sites
    - 10TB in OneDrive for Business storage
    - 5,000 Microsoft Teams
    - 200 Planner plans

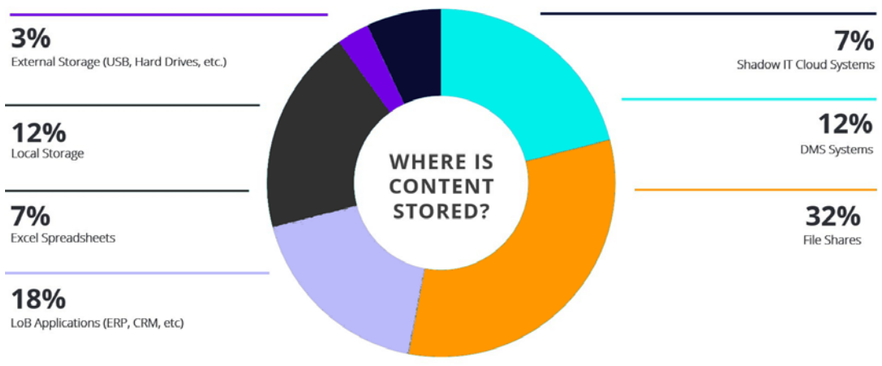
The question is…

WHICH of these systems should The Customer have managed by the new RMIP system?

We know the ideal answer is **ALL OF THEM**, but priorities, time, and budget stand in the Customer's way…

So, let's continue by first understanding where the Customer's content is.

The following chart is a representation of average content distribution across the customer corpus:



Now, let's continue by identifying the benefits **the Customer** wants to realise by using any system/repository:

1. Compliance Levels

Compliance levels can be measured by how information in this system is classified, retained, disposed, and managed compliantly in a way that conforms with legislation and governing bodies regulations.

Your compliance levels are only as high as your least compliant system, as during an audit or an investigation, these will be the systems dragging your overall compliance levels down, despite how compliant all other systems are.

M365 and the EDRMS lead the charge here, but some of the traditional storage systems and line of business systems fall behind.

2. Business Analysis Benefit

Business Analysis benefits can be measured by how easy it is to use data from the system for the purpose of reporting and analytics, based on facts and figures that can be extracted from the content that this system stores.

Your ability to extract insights from your information systems for the purpose of supporting your decision-making process depends on all facts and figures being available, and not providing a skewed or partial view.

3. Discoverability

Discoverability levels are measured by how easy it is to search and find information from this source system, can it be searched by data fields? Or free text? Or both?

The quality of your discovery processes, especially legislation driven ones, is dependent on having access to all information, ideally from one central search interface.

4. Productivity

Productivity gains can be measured by how complementary this system is to the business processes currently followed by the customer.

At times, you might inevitably be forced to pick systems based on the other criteria listed here, at the expense of compromising on business processes alignment and as a result, reducing potential productivity benefits.

5. Cost Efficiency

Cost efficiency is measured by how quickly you can turn up/down your cost of this system, based on its usage at a moment in time.

For example, can it be decommissioned as soon as it is no longer used? Can you remove content from it that is no longer required to maintain or exceed the productivity measures? Can license costs scale up/down based on the tangible benefits this system offers when in use?

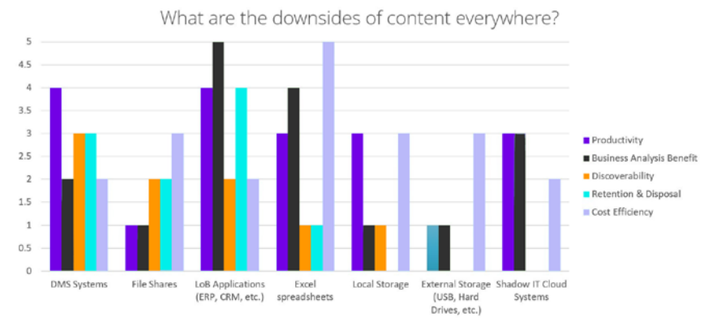
Your maximum potential of cost efficiency is only limited by the systems you cannot decommission quickly and without risk.

Keeping such systems for no other benefit other than retention, discovery or business insights is a sunk cost when this information can be used in other ways.

Migration costs to transfer content out of those systems is also considered a sunk cost, as the act of migration does not add any business benefit other than retention, which can be achieved more efficiently.

It is imperative to note that security is intentionally not listed here, as it is the criterion you will not compromise on, for obvious reasons.

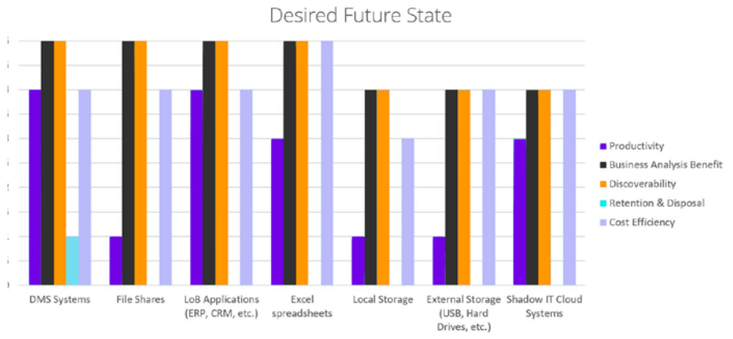
So now, let's have a look at the systems listed above and their respective performance against the measures listed above, in a "Downsides of Content Everywhere" chart:



The difficulty involved in assessing solutions based on the five measures listed above (six when you factor in security) is high, so there needs to be a way to leverage RMIP solutions to address the compliance levels, business analysis benefit, cost efficiency and discoverability in solutions that do not natively do.

When the Customer succeeds in doing that, their only criterion for selecting products or solutions (other than security of course), is their alignment with their business processes as it pertains to the Customer's overall productivity benefits.

The chart below helps to visualise that comparison:



Before:

Other than security, all 5 areas form the criteria that currently informs the Customer's products / solutions selection.

After:

Other than security, productivity is now the only criterion to inform the Customer's products / solutions selection.

Now let's think about the potential of a RMIP system helping the Customer achieve this, a few benefits are listed below, but there are many more to consider:

- Your RMIP system enriches your content on a regular basis, whatever format and wherever it is stored, with metadata values from your business taxonomy, using Machine Learning, Document Cognition, and OpenAI working together.
- Your search experience now covers all your content, including the metadata fields enriched by your RMIP system, metadata that is native to the source system, and free text.
    - You can now challenge this new data to provide better business insights and support your decision-making processes.
    - Compliance levels for retention and disposal are defined in one place and address content from any system.
    - Discovery is comprehensive and identifies sources of truth and natively handles redundant duplicates from multiple systems, ideally by grouping duplicate records stored in various systems together.
- There are immediate cost benefits associated with decommissioning systems that are no longer actively used by the business (or have their footprint significantly reduced), because all content is retained compliantly in your RMIP system.
- There is no longer a need for costly migrations for content that is not active or needed for day-to-day operations, your RMIP can not only retain it, but it can also relocate it to another active system as part of a BAU policy.
- "Right tool for the right job" experience, leveraging the best of Purview while not leaving items not designed for M365 behind, still seeing it all centrally from one place.
    - You can free up business users time when there is no longer a need to have them take on the responsibility of system administration, only to ensure content is properly retained.

Sounds tempting?

How can you make all this happen for myself and my business?

The EncompaaS platform connects to hundreds of system types, including bespoke ones, without writing a single line of code.

It provides intelligent enrichment using Machine Learning, Large Language Models (including Azure OpenAI, PII Scanners, Document Cognition metadata extraction models, etc. with minimal training and flexible trust thresholds.

It contextually correlates related items from various systems (including duplicate copies) into a collection that can be managed as a single series, without needing to relocate items to the same folder.

It uses all this to help meet various compliance regulations and guidelines more easily, while providing a comprehensive search and discovery experience for all content and its enriched insights.

I am interested in your thoughts on the above, as well as how far down the path your business is in achieving these goals and any other goals you see as relevant.

Reach out to shimron.shimla@encompaas.cloud for more information.

Australian WWII records digitised

Over 1 million Second World War service records have now been digitised as part of a large-scale digitisation effort by the National Archives of Australia. These records are now progressively being made available online free-of-charge.

Records digitised include all of Royal Australian Navy series A6769 and A6770, Army series B883 and B884, and Royal Australian Air Force series A9300. A significant portion of Royal Australian Air Force series A9301 has also been completed.

National Archives of Australia Director-General Mr Simon Froude explains that these service records are a valuable resource, not just for those interested in the military, but for family history researchers and anyone interested in the involvement of Australians in our wartime history.

'These records will help the nation to better understand, remember and reflect on the service and sacrifice of each man and woman who served.' said Mr Froude.

'Each record documents a service person's enlistment, movements, transfers, promotions and ultimate fate, offering a fascinating glimpse into the lives of WWII veterans.'

Access to these records continues to be one of the most popular requests made to National Archives, as more Australians seek to discover the untold stories of their own relatives and their role in defending the nation.

'Our priority first and foremost was to preserve these iconic at-risk paper records. The next step is to make sure every one of these records is available to anyone in the world for free.'

National Archives funds digitisation through a combination of an annual budget allocation, project-specific funding received from Government, partnership arrangements and through the generosity of our members and benefactors.

In 2019, the Australian Government provided $A10 million in funding to help National Archives digitise the remaining 852,000 Second World War service records. At the time, 200,000 had already been preserved and made available through annual budget allocations.

As of 30 June, there are approximately 45,000 Second World War service records awaiting digitisation, which will be prioritised over the next 12 months and ultimately made available to view online.

In addition to government funding, $A1 million was donated by long-time supporter and philanthropist Ms Barbara Mason. This donation is being used to digitise the photographic portraits stored on the Second World War service files, helping National Archives to put a face to the name.

Digitisation Project Manager Rebecca Penna said 'digitising these fragile negatives alongside the paper records ensures that more faces can be put to the names of those who served during the Second World War.

'This has been an enormous effort over a number of years. Reaching a milestone of 1 million records digitised is something our teams are incredibly proud of.' said Ms Penna.

Once digitised, records are progressively made available free-of-charge via National Archives' website.

To learn more about the World War II Digitisation Project, visit: Digitising World War II service records.

For more information on war records in the national archival collection, visit: Defence and war service records.

NCA moves into the Cloud with iCognition

The National Capital Authority (NCA) has selected a secure cloud service from solution provider iCognition to handle document and records management under a 3-year contract. On behalf of the Australian Government, the NCA is responsible for overseeing the development and preservation of Canberra and the Australian Capital Territory. Originally formed in 1921 as the Federal Capital Advisory Committee (FCAC) to oversee the construction of Canberra, its functions are now managed by the NCA which was established in 1989 when the Australian Capital Territory was granted self-government.

iCognition will provide NCA with its Content Manager-as-a-Service, EDRMSaaS, which empowers organisations to effectively manage records through a combination of manage-in-place and central records models.

Compliance and security are paramount when handling sensitive government information, and iCognition's cloud-based solution adheres to global records management standards, including ISO15489 and ISO16175, as well as security standards like ISO27001 and government IRAP assessment to the level of PROTECTED. This ensures that the NCA's information is not only efficiently managed but also handled securely, meeting all compliance and governance requirements.

The NCA's decision to choose iCognition builds upon the successful transitions of other Federal Government clients who have benefited from the enhanced compliance and content services offered by Content Manager Cloud. Notable Federal Government clients already utilizing iCognition's services include the Department of the Treasury, Australian Office of Financial Management, and the Australian Digital Health Agency.

According to Nigel Carruthers-Taylor, Principal at iCognition, clients are increasingly turning to cloud services not just to reduce costs but also to embrace future innovation. The cloud-based approach facilitates regular updates and new enhancements, providing the NCA with the opportunity to extend a standard Content Manager solution to iCognition's Ingress Content Services Platform.

Ingress extends a standard Content Manager system with technologies such as Enterprise Search, Artificial Intelligence, and content functions that can be accessed directly from corporate applications and Microsoft 365.

"iCognition is proud to partner with the National Capital Authority in their journey towards efficient document and records management. By leveraging our industry-leading solutions, the NCA will experience greater efficiency, enhanced compliance, and a seamless path to future innovation," said Nigel Carruthers-Taylor.

www.icognition.com.au

Automate ministerials, correspondence, approvals, purchases, FOIs and more.

Easily engage staff in digital business processes using RM Workflow.

Engage them effortlessly in Outlook and web browsers to streamline your business processes, just like Tasmanian Government, Tyson Foods, and NSW Property has.

RM Workflow controls your records in Content Manager to ensure information security, audit and compliance while delivering ease of access and use.

Easily build new processes to supercharge your digital transformation using RM Workflow.

Request a demo
1300 426 400 | icognition.com.au

iCognition · MICRO FOCUS is now opentext · Azure · ISO 27001 INFORMATION SECURITY

OAIC wields data breach powers

Australian Government

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (OAIC) has shown how it will use its new information gathering powers provided under new legislation in 2022 to target organisations that fail to report data breaches within 30 days.

According to the latest six-monthly Notifiable Data Breaches (NDB) Report that covers from January to June 2023, more than a quarter of organisations notifying of data breaches failed to do so within 30 days, with some taking between four and six months.

"In the event of an incident such as a cyber-attack, organisations must also be able to adequately assess whether a data breach has occurred, how it has occurred and what information has been affected," said commissioner Angelene Falk.

"Prompt notification ensures individuals are informed and can take further steps to protect themselves, such as being more alert to scams.

"The longer organisations delay notification, the more the chance of harm increases."

The January to June 2023 period saw 409 data breaches reported to the OAIC. While that was a 16% decrease in the number of notifications compared to the previous period, there was one breach that affected more than 10 million Australians. This is the first breach of this scale for Australians since the scheme began in 2018.

In one case the OAIC became aware of a ransomware incident that ccompromised the information of 20 health service provider clients of an IT service provider, including their patients' treatment information.

"The entity notified the impacted health service providers of the breach, presuming they would notify affected individuals if required. The entity declined to provide the health service providers' details to the OAIC, claiming it did not have consent to disclose the information.

"In the circumstances, the Commissioner exercised her power under s 26WU(3) (*The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*) to issue a written notice, requiring the entity to provide a list of the health service providers impacted by the data breach. Following receipt of the notice, the entity provided the information required. This information enabled the Commissioner to ensure the affected individuals were notified and that all entities involved in the data breach complied with the NDB scheme."

Cyber security incidents were the source of 42% of all breaches (172 notifications) in the first six months of 2023. The top three cyber-attack methods were ransomware (53 notifications), compromised or stolen credentials for which the method was unknown (50 notifications) and phishing (33 notifications).

Contact, identity and financial information remained the most common kinds of personal information involved in breaches.

The full report is available HERE

Data breaches seen as Number 1 privacy concern: OAIC

There has been a sharp increase in the number of Australians who feel data breaches are the biggest privacy risk they face today, according to a survey released by the Office of the Australian Information Commissioner (OAIC).

The Australian Community Attitudes to Privacy Survey (ACAPS) 2023 provides a comprehensive view of Australians' privacy attitudes and experiences and how recent events have impacted them.

The survey tested attitudes on topics such as data practices, privacy legislation, data breaches, biometrics, artificial intelligence and children's privacy.

"Our survey shows privacy is a significant concern for Australians, especially in areas that have seen recent developments like artificial intelligence and biometrics," said Australian Information Commissioner and Privacy Commissioner Angelene Falk.

"Australians see data breaches as the biggest privacy risk today, which is not surprising with almost half of those surveyed saying they were affected by a data breach in the prior year.

"There is a strong desire for organisations to do more to advance privacy rights, including minimising the amount of information they collect, taking extra steps to protect it and deleting it when no longer required."

Among the key themes of the survey are:

■ **Australians care about their privacy**. Nine in 10 Australians have a clear understanding of why they should protect their personal information, and 62% see the protection of their personal information as a major concern in their life.

■ **Australians don't feel in control of their privacy and don't know what to do about it.** Only 32% feel in control of their privacy, and half believe if they want to use a service, they have no choice but to accept what the service does with their data. Three in five care about their data privacy, but don't know what to do about it.

■ **Most Australians have had a negative privacy experience.** Forty-seven per cent were told by an organisation that their personal information was involved in a data breach in the year prior, and three-quarters said they experienced harm because of a data breach.

■ **Australians have strong feelings about certain data practices.** Nine in 10 are concerned about organisations sending customers' information overseas. Ninetysix per cent want conditions in place before artificial intelligence is used to make decisions that might affect them.

■ **There are high levels of distrust.** Only four sectors (health, federal government, finance and education) are more trusted than not by Australians to handle their personal information. Less than half of people trust organisations to only collect the information they need, use and share information as they say they will, store information securely, give individuals access to their information and delete information when no longer needed.

■ **Australians want more to be done to protect privacy.** Eightyfour per cent want more control and choice over the collection and use of their information. Around nine in 10 Australians would like businesses and government agencies to do more to protect their personal information.

Commissioner Falk said the survey has important signposts for organisations.

"The findings point to several areas where organisations can do more to build trust in the community," she said.

"Not only is good privacy practice the right thing to do and what the community expects, it's a precondition for the success of innovations that rely on personal information."

The survey findings also show there is strong support for privacy law reform.

"We are at a pivotal moment for privacy in Australia, where we can seize the opportunity to ensure laws and practices uphold our fundamental human right to privacy," Commissioner Falk said.

"This is an opportunity to ensure the protections the community expects are reflected in the law.

"The OAIC will use the findings to inform our ongoing input into the review of the Privacy Act and to target our activities at areas of high concern among the community."

The OAIC commissioned Lonergan Research to undertake ACAPS 2023. The survey was conducted in March 2023 with a nationally representative sample of 1,916 unique respondents aged 18 and older.

To read the full report, visit oaic.gov.au/acaps

It’s time to rethink your scanning operation

Scott Maurer, President of OPEX International, explains how the newest technologies can help to reduce document prep and labour costs, while improve the efficiency of your scan environment.

Traditional high-speed document scanning requires extensive prep, lots of labour, and often involves considerable scanner downtime while waiting for documents to be prepped. The latest evolution of document scanners faces these challenges head-on and delivers substantial improvement in productivity. Here's what you need to know to scale up your scanning performance.

When was the last time you examined your scanning operations? If you haven't done so in a while, you may be surprised by what you would discover about improving your speed, efficiency, and ultimately your profitability with the right combination of workflow changes matched with the right scanning equipment. New technology innovations are opening the door to new levels of efficiency that overturn traditional models of process productivity. Here are three key areas you should audit on a regular basis: your document prep workflow, labour costs, and scanner runtime efficiency.

DOCUMENT PREP

Let's first look at common practice utilised in many scanning workflows. One cannot overemphasise the importance of the proper preparation of documents and financial records to facilitate quick and accurate capture of digital documents. This time-consuming and monotonous process - commonly known as "document prep" - has been widely accepted in the banking, mortgage, revenue, and insurance industries as a necessary cost of doing business.

Paper documents from mortgage, insurance or legal files are quite diverse in size, format and condition, requiring lots of extra handling and slow operational throughput. Examples include letter- and legal-sized documents paper clipped and stapled, envelopes of varying sizes, business cards, Post-it notes, torn and tattered sheets, carbon copies, NCR forms, historic documents printed on onion skin-type paper, and critical original documents like cheques, deeds, titles and surveys, many of which have been tri-folded to be sent through the post.

These odd-sized, unusual-formatted, and critical documents cannot automatically be passed through a scanner without significant manipulation, making manual pre-scanning document prep a time-consuming necessity.

The document-prep process involves removing staples and paper-clips, taping torn documents, photocopying delicate and important papers, securing small or odd-shaped notes and papers onto larger sheets for photocopying, opening envelopes, unfolding, and removing creases from pages, inserting document separators, and whatever additional actions are needed to make these documents capable of being fed through a scanner in the right order. Sometimes it is even necessary to capture the image on a remote device such as a multifunction device (MFD) or flat-bed scanner and later, successfully reunite those images into the right documents.

The most difficult part of prep and scan is balancing the talent to work on prepping documents with varying levels of complexity and getting jobs perfected at consistent quality levels. Good training is a constant battle when temporary or transitory labour enters the equation. The benefits of good technology working with good people is lost in standalone prep processes.

LABOUR NEEDS

The document prep stage requires an enormous amount of labour but finding quality employees today cannot be assumed. When your intensive prepping process requires that you always must have enough employees on hand, it raises the stakes and expense of your recruiting efforts, which often means increased overhead costs in HR. Companies of all types, including scanning operations, are facing the fact in a post-pandemic world that the old method of relying on a readily available pool of low-cost labour is a thing of the past.

(Continued over)

INTRODUCING RIGHT-SPEED™ SCANNING

Traditional high-speed scanning requires extensive prep and lots of labour, especially as jobs get messier and messier. High-speed scanners sometimes require multiple operators to keep them in continuous operation. This leads to additional labour hours driving up cost per image and driving down profitability.

The OPEX® Gemini™ scanner is designed for maximum versatility and configurability and handles documents at the right speed while requiring minimal prep and controlling costs.

DM DOCUMENT MANAGER AWARDS 2022
WINNER
Imaging Product of the Year: High Volume
OPEX
OPEX Gemini

Visit digitiseyourdocuments.com.au to learn more or contact info@opex.com to schedule a demo today.

OPEX®

Time to rethink your scanning operation

(From previous page)

Even if you can find quality employees, you must deal with the ever-increasing expense of onboarding and training. And many companies find themselves spending more and more resources to retain the employees due to increasing turnover rates. The costs to management in interviewing, training and integrating new people into teams has its own impact on disrupted efficiency of day-to-day operations.

Now, in the face of higher-cost and often less reliable or less productive labour, companies are looking at every means necessary to change their operations models wherever possible to reduce their dependence on staff in general, but especially in roles that require little talent. Bundled with the constant pressure to meet service level commitments, the shifting economics of staffing have made the ROI on automated solutions coupled with a core of quality operators, a lot more attractive.

TIME & EFFICIENCY

In many ways, throughput efficiency is dictated by the amount of manual prep work your employees invest to clean up the media so it can be scanned. Business process outsourcers are continually looking for faster and more cost-efficient ways to convert paper documents to digitised files. But often there is mismatch when the capacity of a document prep system is not able to keep up with the rate at which a scanner can receive and scan documents.

In the processing of documents, the throughput capability of a scanner should not be focused solely on how fast a scanner can scan pages, but rather on the scanning speed combined with the scanner downtime while waiting for documents to be prepped, especially for complex prepping processes. A very fast mortgage or insurance document prepper can handle 750 to 1,000 documents per hour, but this is no match for high-speed scanners operating at 6,000 to 12,000 DPH.

For most scanning work, a prepper generally handles less than 600 documents per hour. Therefore, a more accurate estimate of scanning throughput would need to also include the prep time involved with preparing the documents for scanning. Only in this way can companies realistically assess the true performance of their document scanning operation.

When the scanner must stop and wait for the document prep to catch up, it results in expensive equipment often sitting idle while the employees you hired to run it are also underutilised. This start-stop sequence occurs frequently in the scanning of mortgage, financial, insurance and legal documents.

To improve efficiency, prepping documents simultaneous with scanning would not only increase throughput but would optimise labour utilisation resulting in reduced operational costs. An ideal workflow would involve systems that adapt to the complexity of the documents themselves.

Although automated options do exist to reduce the high labour expense and excessive time associated with the document scanning process, until now there has not been a one-source solution for efficiently handling both clean documents at high speeds and messy documents requiring excessive prep work.

Some scanning equipment manufacturers have embraced aspects of this concept, integrating varying levels of document prep into their scanners. The latest evolution in systems providing integration of document prep and scanning represents a significant game changer for document processors.

A NEW PARADIGM IN SCANNING TECH

Such a system has been introduced by OPEX Corporation, a manufacturer of high-speed automated sortation and scanning systems for mail and document handling.

Its recently released OPEX Gemini scanner not only streamlines prepping of the widest range of document types, sizes, and conditions, but also provides a level of system speed flexibility beyond any prior system's capability. This latest revolutionary OPEX Gemini scanner has indeed ushered in a new paradigm in document scanning technology.

The workflow has changed. Documents bypass traditional prep stations, and go directly to the scanner, where the operator performs minimal prep using Gemini's CertainScan software combined with unique feeding mechanisms that adapt to document conditions including stacks and individual sheets.

Within CertainScan image clean-up, page recognition, indexing, and quality control can be done at scan time or in post scanning, providing options for balancing an organisation's staff of the highest quality operators.

Where a conventional document prepping then scanning cycle might take four-and-a-half hours (for example), now mixed speed scanning while prepping with a single operator could yield a 200-300 percent increase in productivity.

The OPEX Gemini scanner can handle both clean documents requiring little or no prep at high speeds, as well as messy documents at speeds optimised to a drop and feed method for items like folders or envelopes. The scanner seamlessly transitions speeds to handle workloads with different document types, adjusting to the right speed for scanning at maximum throughput.

For example, operators can run clean stacks at high-speed rates up to 240 pages per minute intermixed with difficult to prep, damaged or delicate documents at slower speeds. OPEX's dual-feeder capability and fully-configurable output bins permits operators to continuously stack-feed documents at high speeds up to three stacks deep, while drop-feeding messy single sheets without the scanner ever stopping.

READY FOR THE CHALLENGE

Document scanning is a crucial part of most company's business strategy of going digital. Taking time to make the assessment of your scanning processes against workflow, labour needs, management complexities, and efficiency are critical to improving productivity in your business.

The latest evolution of document scanners has ushered in a new paradigm in scanning technology, one that presents an opportunity to optimise your document processing operations in the most robust ways possible for the challenges ahead.

More info: www.opex.com

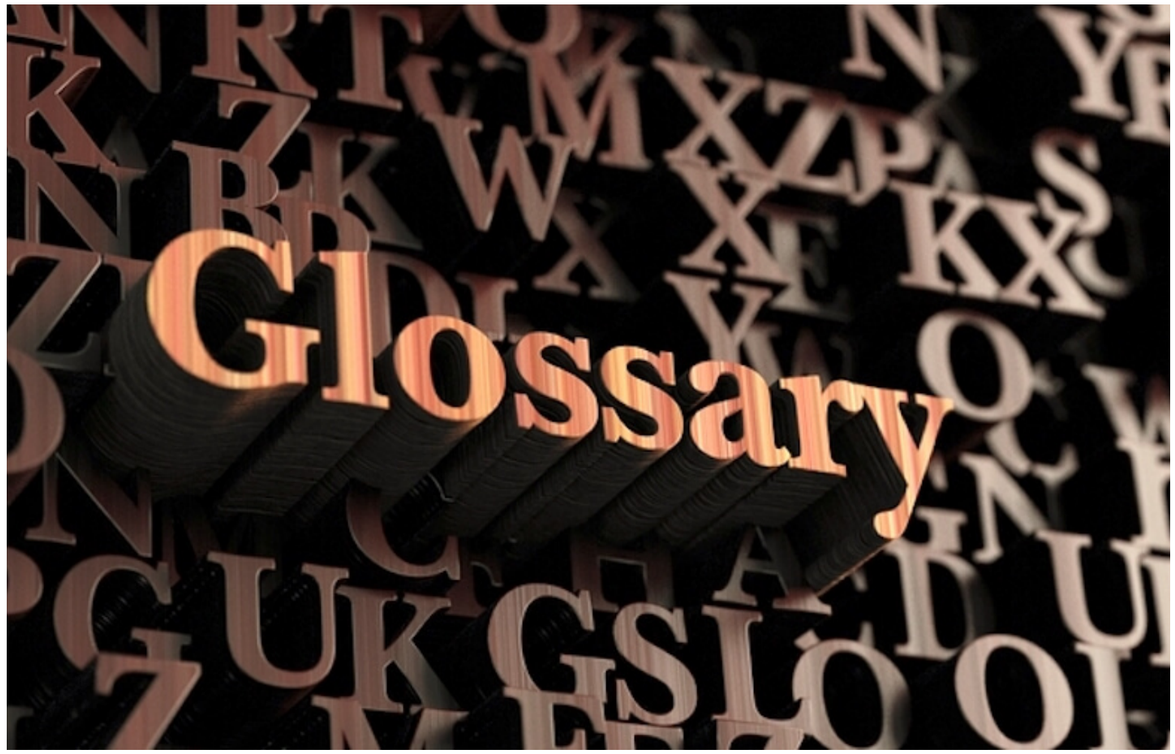
Kapish

Empowering Secure Technology Solutions

Talk to us today to find out how our suite of products and services can help you get the most out of Content Manager.

Call 1300 KAPISH |info@kapish.com.au | kapish.com.au

The 7 Potential Benefits of Having a Data Glossary or Data Catalogue



By Nicola Askham

Is harnessing the power of a Data Glossary or Data Catalogue the key to unlocking the true potential of your data endeavours?

In today's data-driven world, businesses and organisations are constantly generating and dealing with vast amounts of data. This deluge of information can be overwhelming, making it challenging for employees to understand and utilise the data effectively, often leading to confusion and inefficiency.

While it may feel like a bit of a time and monetary investment, the implementation of a Data Glossary or Data Catalogue can significantly enhance an organisation's data management capabilities, leading to improved efficiency, better decision-making, and enhanced collaboration, allowing the true potential of the data to be unlocked.

Sadly, a lot of organisations implement a Data Glossary or Data Catalogue as “best practice” as part of a Data Governance initiative without really understanding the value you can get from having one. So, what are these benefits you can achieve?

Listed below are those that I have seen my clients achieve over the years:

1. Enhanced Communication and Efficiency

One of the key advantages of having a Data Glossary or Data Catalogue is the ease of communication it brings. Everyday actions like responding to enquiries become straightforward, with a simple reference to the glossary or catalogue to make sure that you use the correct data. This saves time and effort, as employees no longer have to spend significant portions of their work hours searching for data.

By providing a centralised repository of all available datasets with detailed descriptions, users can quickly identify the data they need without wasting time searching through various sources, leading to increased productivity and reduced operational costs.

2. Clarity and Consistency in Data Terminology

In the modern business landscape, confusion around data terminology is a common issue. Different departments might use varying terms for the same data elements, leading to misunderstandings and inconsistencies. With a Data Glossary or Catalogue, everyone within the organisation can adhere to uniform data definitions and understand the context in which specific terms are used. This promotes a data-literate culture, wherein employees are better equipped to comprehend data, ask meaningful questions, and draw accurate insights.

3. Improved Data Quality

A Data Glossary or Data Catalogue also acts as a repository for metadata, providing essential information about each dataset, including its source and quality metrics. By maintaining a comprehensive record of data lineage and quality assessments, data users can assess the reliability of the data they are working with. This, in turn, helps improve data quality as potential issues are identified and addressed promptly.

4. Enhanced Compliance

Data governance is crucial for ensuring compliance with many regulatory requirements. A well-organised Data Glossary or Data Catalogue can help meet regulatory requirements. It enables data stewards and administrators to monitor and ensure that sensitive data is appropriately handled and regulations are adhered to.

While Data Governance and Data Protection are not the same thing, with increasing data privacy regulations, such as GDPR and CCPA, organisations must respond to Subject Access Requests (SARs) promptly and accurately. SARs involve providing individuals with information about the personal data the organisation holds about them and how it is being processed.

A Data Catalogue simplifies this process by providing a comprehensive inventory of data assets and their locations. Identifying the data relevant to a specific request becomes much easier and faster, saving time and avoiding potential legal complications.

5. Empowering Data-Driven Decision Making

Data is a valuable asset, and understanding its value is essential for making informed business decisions. Data Glossaries and Data Catalogues support data analysts by providing a detailed understanding of available datasets and their context. This knowledge enables analysts to perform more accurate and meaningful data analysis, leading to better-informed decision-making.

6. Facilitating Data Collaboration and Knowledge Sharing

In organisations with diverse teams and departments, data collaboration is vital for achieving meaningful insights. A Data Glossary or Data Catalogue encourages knowledge sharing by facilitating communication and collaboration among data users. The tool becomes a hub for exchanging ideas, insights, and best practices related to data analysis, fostering a data-driven culture throughout the organisation.

7. Streamlined Onboarding and Training

In all organisations, data plays a crucial role, but new employees often face a steep learning curve when it comes to understanding the complex data landscape. A well-maintained Data Glossary or Data Catalogue simplifies the onboarding process by offering a comprehensive overview of data assets, reducing the time required for new hires to get up to speed and start contributing effectively.

The benefits of implementing a Data Glossary or Data Catalogue are clear: enhanced data understanding, communication and efficiency, data quality, and decision-making.

As data continues to grow in volume and complexity, having a robust data governance strategy that includes a Data Glossary or Data Catalogue becomes more critical than ever. By investing in these tools, businesses can harness the full potential of their data, gaining a competitive advantage in today's fast-paced and data-centric landscape.

What do you think? Are you already benefitting from a Data Glossary or Data Catalogue, or do you think your organisation should think about implementing one? Let me know.

Don't forget if you have any questions you’d like covered in future articles please email me - questions@nicolaaskham.com

Originally published on www.nicolaaskham.com

Australian businesses at risk due to poor information governance

- **65%** say that employees use **7 or more applications** to create information **each day**
- **34%** say that **more than 10 applications** are used

A new survey undertaken by Swinburne University of Technology and Astral Consulting Services has found that Australian businesses are at risk due to the overwhelming increase in data that organisations create daily.

More than a third of those surveyed said their organisation's current progress towards implementing information governance was poor overall, despite 89 per cent of participating organisations recognising the importance of a formal approach to information.

"The last decade has generated more documents and records than any previous decade of human activity," says co-leader of the project, Swinburne researcher Dr Paul Scifleet.

"Yet, at the same time, these records are seen as less reliable, retrievable and accessible than ever before. The volume of information and the rate of growth is simply too large and rapid to rely on traditional methods of information management."

Other key findings include:

- 61 per cent of employees are not confident managing the breadth and depth of information available to them

- Nearly two-thirds of employees use seven or more applications every day to create and store information, with more than one-third reporting the use of 10 applications or more.

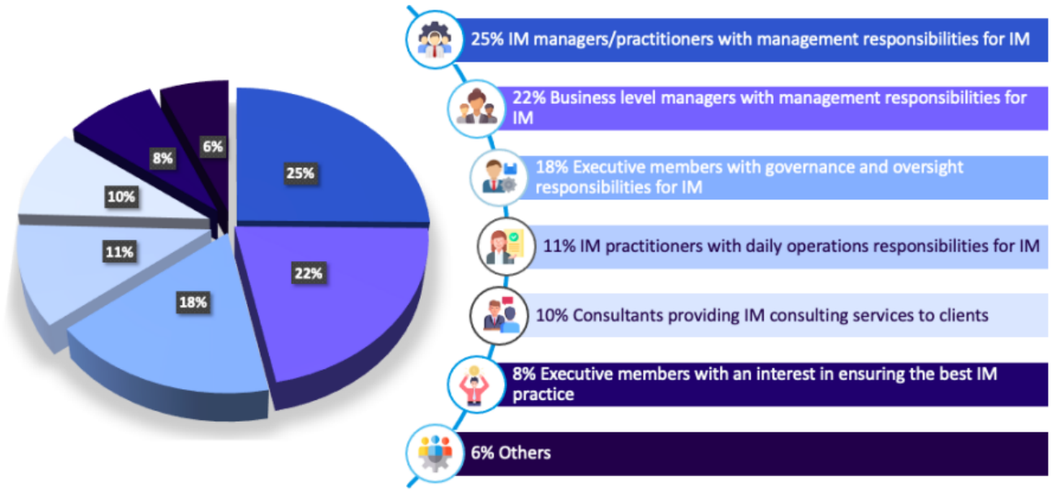
- 44% of respondent's organisations are working globally, in environments requiring management of international information flows across borders and across jurisdictions, with 49% working in organisations with more than 1000 employees.

- 35% rated their organisations current progress towards implementing Information Governance as poor.

The survey of over 100 information management professionals is part of a research project to explore how changes to enterprise information management practice can lead change in information governance to meet current and future challenges.

The collaborative research project, supported by a Department of Industry, Science and Resources, Innovations Connection Grant, aims to better understand the changing role of information governance and develop new information management cloud technologies and services for businesses.

Almost half of the respondents from either proprietary or public listed companies and 39% percent of respondents from the public sector. The remaining 13% of respondents represent a mix of not-for-profit and 'other'organisations, including an independent research institute, a trade union, independent information management consultants and information management consultancies.



Information Management role of respondents.

The survey found discrepancies between Enterprise Information Management (EIM) goal setting and requirements for successful implementation.

- Most respondents rate their organisations as being good and very good in managing vital business information, achieving strategic alignment, and meeting the requirements of assurance and compliance.

- But this is contradicted by responses that rate organisations as being poor and very poor in applying the policies, processes and mechanisms for information capture, control, retention, and use, that are the backbone of EIM and vital business Information Management.

In terms of data management priorities, the survey demonstrates that organisations continue to focus first on managing structured transactional and operational data, records, and information.

82% of respondents rank structured data management for transaction processing systems and operational databases as their greatest priority (either as important or very important), business process management including controlled document management (templates and metadata) was prioritised by 70% of respondents.

Unstructured data management is seen as less important with 52% of respondents rating it as their least important concern.

"The challenges faced in managing and disseminating the ever-increasing volume and complexity of information have never been greater than in today's highly paced business environments," says Astral Managing Director Marie Felsbourg.

56% of respondents indicate that the most common approach to integrating IM in office productivity suites is to license and add-on standard features available in their office suite to support information management (Figure 3.28). 50% of respondents are integrating their office productivity suite with their document, record, and content management systems.

Less common is the application of information architecture for improving the control of vital business information, including applying metadata and classification schemes, automating business rules and workflows for document control, applying functionality to automate classification and action documents created.

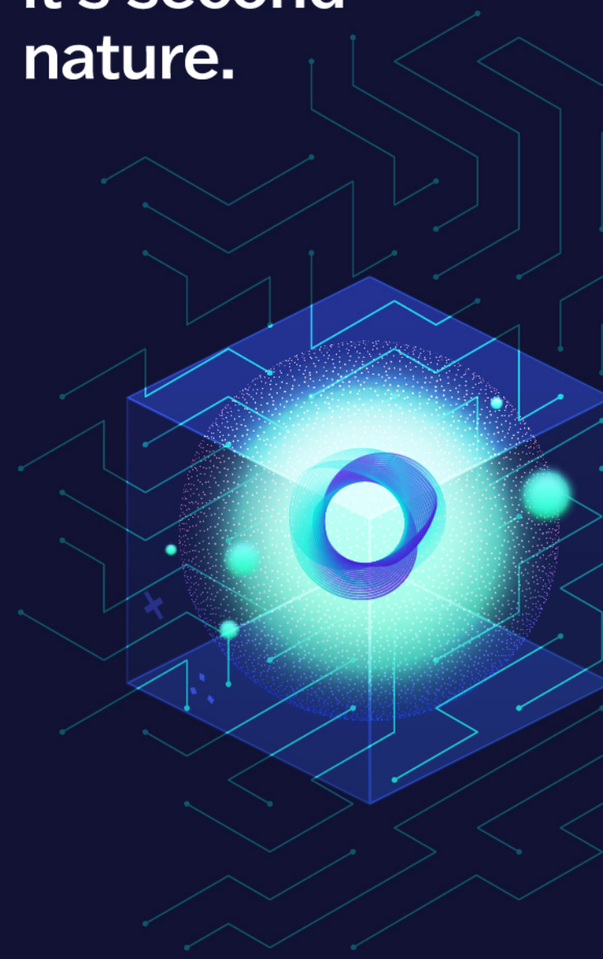
"Every business is now a distributed workplace, dependent on information sharing. The communication of data and information is a critical asset, which urgently requires improved management to reduce vulnerabilities, limit exposure to cyber security attacks and ensure business continuity," Dr Scifleet says.

"It is time to ask new questions about the values, rules and parameters under which information will be managed, and to shift the focus from assurance and compliance to greater accountability, trust and responsibility,"

Download the full report HERE

For information management, AI is a trendy topic.

For EncompaaS, it's second nature.



We transcend buzzwords and hype because AI isn't new to us. Our customers are already benefitting from next gen-AI to harness information everywhere and reduce privacy and compliance risk.

Unlock the latent potential of information with EncompaaS.

encompaas.cloud

Wall Street Firms Hit with Massive Recordkeeping Penalties

The use of "off-channel" messaging apps such as iMessage, WhatsApp, and Signal has landed 11 Wall Street firms in hot water, with the industry regulator, the US Securities and Exchange Commission (SEC), issuing combined penalties of $US289 million.

The firms which include Wells Fargo Securities, LLC and BNP Paribas Securities Corp have admitted to violating recordkeeping provisions of US federal securities laws and agreed to pay the penalties. Meanwhile, the Commodity Futures Trading Commission has issued orders for four financial institutions to pay $US260 million for "Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods."

The four financial institutions are: BNP Paribas $US75 million, Société Générale $US75 million, Wells Fargo $US75 million and Bank of Montreal $US35 million.

The use of consumer messaging apps in the workplace, a form of shadow IT, is making it increasingly difficult for enterprises to protect their data and ensure compliance. These concerns have been raised in other countries, such as the UK, where the Information Commissioner's Office (ICO) has warned against government officials using WhatsApp and personal email.

The SEC has criticised the widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications.

"Compliance with the books and records requirements of the federal securities laws is essential to investor protection and well-functioning markets. To date, the Commission has brought 30 enforcement actions and ordered over $US1.5 billion in penalties to drive this foundational message home.

"And while some broker-dealers and investment advisers have heeded this message, self-reported violations, or improved internal policies and procedures, today's actions remind us that many still have not," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

"So here are three takeaways for those firms who haven't yet done so: self-report, cooperate and remediate. If you adopt that playbook, you'll have a better outcome than if you wait for us to come calling."

The SEC's investigation uncovered pervasive and longstanding "off-channel" communications at all 11 firms. As described in the SEC's orders, the firms admitted that from at least 2019, their employees often communicated through various messaging platforms on their personal devices, including iMessage, WhatsApp, and Signal, about the business of their employers.

The firms did not maintain or preserve the substantial majority of these off-channel communications, in violation of the federal securities laws.

By failing to maintain and preserve required records, certain of the firms likely deprived the Commission of these off-channel communications in various SEC investigations. senior executives.

"Today's actions stem from our continuing sweep to ensure that regulated entities, including broker-dealers and investment advisers, comply with their recordkeeping requirements, which are essential for us to monitor and enforce compliance with the federal securities laws. Recordkeeping failures such as those here undermine our ability to exercise effective regulatory oversight, often at the expense of investors," said Sanjay Wadhwa, Deputy Director of Enforcement.

"The 11 firms settling today have acknowledged that their conduct violated the law regarding these crucial requirements, and are implementing measures to prevent future similar violations. However, we know that other SEC-regulated entities have committed similar violations, and so our work to enforce industry-wide compliance continues."

In addition to the significant financial penalties, each of the firms was ordered to cease and desist from future violations of the relevant recordkeeping provisions and was censured.

The firms also agreed to retain independent compliance consultants to, among other things, conduct comprehensive reviews of their policies and procedures relating to the retention of electronic communications found on personal devices and their respective frameworks for addressing non-compliance by their employees with those policies and procedures.

CFTC Director of Enforcement Ian McGinley, said, "The Commission's message could not be more clear – record-keeping and supervision requirements are fundamental, and registrants that fail to comply with these core regulatory obligations do so at their own peril."

Each order finds the swap dealer and/or FCM in question, for a period of years, failed to stop its employees, including those at senior levels, from communicating both internally and externally using unapproved communication methods, including messages sent via personal text or WhatsApp.

The firms were required to keep certain of these written communications because they related to the firms' businesses as CFTC registrants.

These written communications generally were not maintained and preserved by the firms, and the firms generally would not have been able to provide them promptly to the CFTC when requested.

newgen
UNLOCK SIMPLE

Government Organisations

...

Automate End-to-end at Scale with the Power of ***One – NewgenONE***

What NewgenONE Does that Others Can't?

Learn More

About Newgen

Newgen is the leading provider of a unified digital transformation platform with native process automation, content services, communication management, and AI/ML capabilities. Globally, successful enterprises rely on Newgen's industry-recognized low code application platform to develop and deploy complex, content-driven, and customer-engaging business applications on the cloud. From onboarding to service requests, lending to underwriting, and for many more use cases across industries, Newgen unlocks simple with speed and agility.

For SALES Query

AMERICAS: +1 (202) 800 77 83
CANADA: +1 (202) 800 77 83
AUSTRALIA: +61 290 537174
INDIA: +91 11 407 73769
APAC: +65 3157 6189
MEA: +973 1 619 8002, +971 445 41365
EUROPE: +44 (0) 2036 514805

info@newgensoft.com
www.newgensoft.com

newgen

Is Business Serious about Generative AI?

By Bill Dawes

So i is it just a glorified autocomplete or the most significant development in human history since the release of the graphical user interface or the iPhone? The inaugural Generative AI Summit 2023 held in Sydney last month heard from different points of view on business uptake including input from entities such as NAB, Optus and the Australian Stock Exchange (ASX).

A recent survey of global executives in data, IT, AI, security and marketing conducted by VentureBeat found more than half (54.6%) of organizations are experimenting with generative artificial intelligence (generative AI), while a few (18.2%) are already implementing it into their operations, but only a few (18.2%) expect to spend more on the technology in the year ahead.

Kicking off the conference, Dr Michael Kollo from AI consulting firm Evolved Reasoning set the scene by looking at the economic and industry impacts of Generative AI. The fastest growing app in the world ever since its launch in November 2022, ChatGPT is developing fast but can only infer truth from semantic relationships.

"Language Models can learn to reason through replication of language, but they are poor at analytical tasks unless assisted by other systems. They are optimised for engagement not truth," he said.

Kollo sees ChatGPT's potential as a business augmentation tool which can reduce time spent on writing tasks by 37%.

"Impact is primarily in the drafting stage and brainstorming. Overall quality of output and job satisfaction are raised," he said.

The key areas of impact in the BackOffice are expected to be in staff training, Knowledge Management, Compliance and HR Policies and Training.

"ChatGPT can be programmed with the latest regulatory standards and requirements and can then be used as a tool to ensure compliance. It can provide reminders of important deadlines, assist with the preparation of compliance reports, and help to answer questions about complex regulations."

A new report says Australia's professional and financial services sector could unlock billions of dollars in value by 2030 if it accelerates the responsible adoption of generative artificial intelligence (GAI). The report, Australia's Generative AI Opportunity, is a collaboration between Microsoft and the Tech Council of Australia. It shows that GAI could contribute between $45 billion and $115 billion a year to Australia's economy by 2030 through two major channels: improving existing industries and enabling the creation of new products and services.

Professional and financial services are identified as one of the four key sectors of the Australian economy that are poised to benefit from GAI. The report demonstrates that the technology could contribute between $5 billion and $13 billion annually to the sector in Australia by 2030.

A recent survey undertaken in 2023 by the University of Queensland and KPMG found Trust in AI systems in Australia was extremely low in comparison to other countries around the world. In fact, Australia was ranked lowest in terms of perception of the trustworthiness and perceived benefits of AI systems.

Howard Silby, Chief Innovation Officer, National Australia Bank expects the release of Microsoft Copilot tools in Office365, scheduled to happen by the end of 2023, will show up as a large change for the general workforce.

Although he expressed significant reservations about the use of generative AI in interactions with bank customers.

"We can't afford to be wrong one in 10,000 times or even one in 50,000 times."

He also pointed out that new skills will be required, as for instance prompt engineering, the ability to design queries that deliver the optimal answer from ChatGPT, is very different to undertaking an effective Google search.

"It is a skill we will need to learn to get the best result," said Silby.

Optus has deployed Google AI on its own private data in a partnership with Google Cloud to enhance its call centres with the Contact Centre AI (CCAI) solution.

Dan Chesterman, ASX Group Executive Technology and Data and Chief Information Officer, was asked about the potential for business use of Generative AI.

He admitted that while pretty much every aspect of share trading today is touched by AI, he considered tools such as ChatGPT only showed potential as a research assistant.

"Our analysts receive 15,000 announcements from listed companies each year and must make a quick assessment whether it is significant enough to put a halt to trading. Our analysts are experts and tools like Copilot may be a help in comparing these with previous announcements made by the same company, but won't replace them."

On average, an AI project brings $A361k incremental revenue to an organisation, according to Stela Solar, Director – National Artificial Intelligence Centre, CSIRO's Data61.

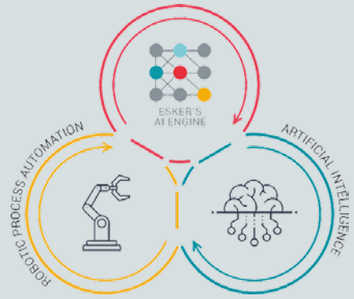
Sola was quoting from Australia's AI ecosystem momentum report, commissioned earlier this year.

It concluded that Australian businesses have access to the foundations to start taking advantage of AI but the partner and support ecosystem in Australia needs to mature.

BUSINESS BENEFITS OF RPA

Robotic Process Automation (RPA) refers to software that can be easily programmed to do routine, repetitive human tasks quickly, accurately and tirelessly. Relying on structured data, RPA automates workflows or clerical processes by emulating human interaction within a graphical user interface (GUI) — helping businesses:

- Reduce overall costs & process redundancies
- Facilitate business security & scalability
- Improve speed & quality in data management
- Free up staff time to perform more strategic, value-added activities
- Ease the replication of tasks & processes across multiple locations & business units
- Empower employees to be more productive & professionally fulfilled



GOING BEYOND RPA WITH ESKER'S AI ENGINE

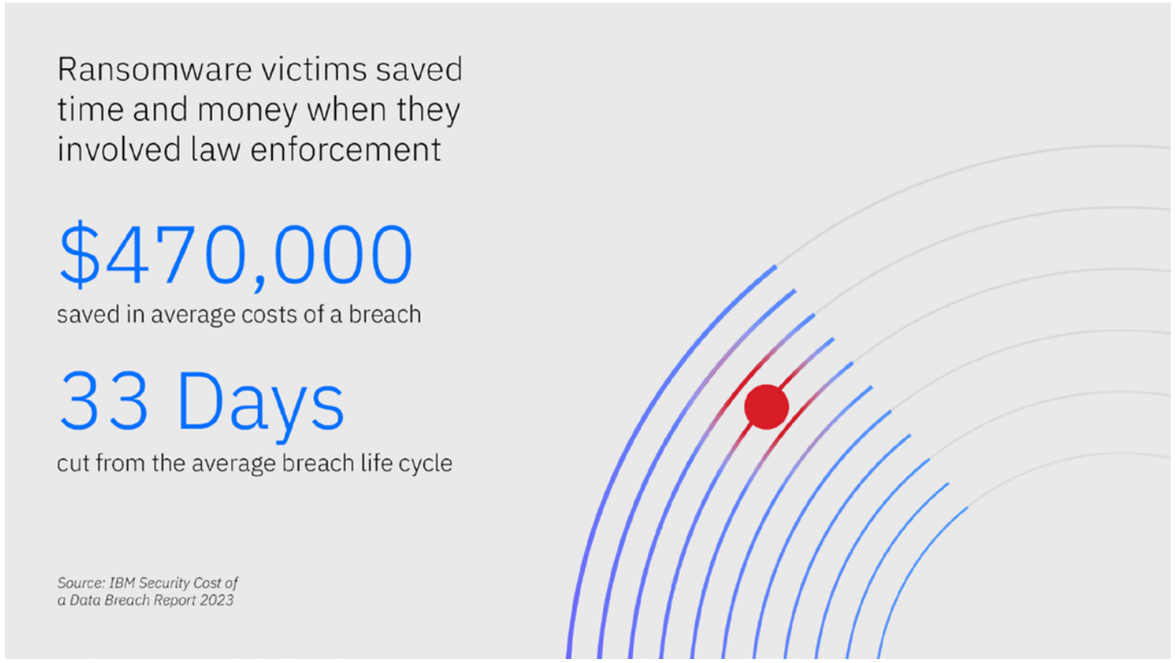
Although both deal with automation, RPA and AI are not one and the same. RPA doesn't "learn" on its own and only works with structured data, whereas the AI technologies built into Esker's AI Engine can automatically adapt based on user's behaviour.

Combined with RPA, machine learning and deep learning help bring automation to a whole new level!

Learn about benefits of Esker's RPA and AI-driven solutions and how leading organisations are using the technology to increase customer, supplier and employee satisfaction.

ESKER®
www.esker.com.au

Half of Breached Organizations Unwilling to Increase Security Spend



IBM Security has released its annual Cost of a Data Breach Report, showing the global average cost of a data breach reached $US4.45 million in 2023 – an all-time high for the report and a 15% increase over the last 3 years. Detection and escalation costs jumped 42% over this same time frame, representing the highest portion of breach costs, and indicating a shift towards more complex breach investigations.

According to the 2023 IBM report, businesses are divided in how they plan to handle the increasing cost and frequency of data breaches.

The study found that while 95% of studied organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%).

The 2023 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 553 organizations globally between March 2022 and March 2023. The research, sponsored and analyzed by IBM Security, was conducted by Ponemon Institute and has been published for 18 consecutive years.

Some key findings in the 2023 IBM report include:

■AI Picks Up Speed – AI and automation had the biggest impact on speed of breach identification and containment for studied organizations. Organizations with extensive use of both AI and automation experienced a data breach lifecycle that was 108 days shorter compared to studied organizations that have not deployed these technologies (214 days versus 322 days).

■The Cost of Silence – Ransomware victims in the study that involved law enforcement saved $US470,000 in average costs of a breach compared to those that chose not to involve law enforcement. Despite these potential savings, 37% of ransomware victims studied did not involve law enforcement in a ransomware attack.

■Detection Gaps – Only one third of studied breaches were detected by an organization's own security team, compared to 27% that were disclosed by an attacker. Data breaches disclosed by the attacker cost nearly $US1 million more on average compared to studied organizations that identified the breach themselves.

"Time is the new currency in cybersecurity both for the defenders and the attackers. As the report shows, early detection and fast response can significantly reduce the impact of a breach," said Chris McCurdy, General Manager, Worldwide IBM Security Services.

"Security teams must focus on where adversaries are the most successful and concentrate their efforts on stopping them before they achieve their goals. Investments in threat detection and response approaches that accelerate defenders speed and efficiency – such as AI and automation – are crucial to shifting this balance

Every Second Costs

According to the 2023 report, studied organizations that fully deploy security AI and automation saw 108-day shorter breach lifecycles on average compared to organizations not deploying these technologies – and experienced significantly lower incident costs.

In fact, studied organizations that deployed security AI and automation extensively saw, on average, nearly $US1.8 million lower data breach costs than organizations that didn't deploy these technologies – the biggest cost saver identified in the report.

At the same time, adversaries have reduced the average time to complete a ransomware attack. And with nearly 40% of studied organizations not yet deploying security AI and automation, there is still considerable opportunity for organizations to boost detection and response speeds.

Ransomware 'Discount Code'

Some studied organizations remain apprehensive to engage law enforcement during a ransomware attack due to the perception that it will only complicate the situation. For the first time this year, the IBM report looked closer at this issue and found evidence to the contrary.

Participating organizations that did not involve law enforcement experienced breach lifecycles that were 33-days longer on average than those that did involve law enforcement – and that silence came with a price. Ransomware victims studied that didn't bring in law enforcement paid on average $US470,000 higher breach costs than those that did.

Despite ongoing efforts by law enforcement to collaborate with ransomware victims, 37% of respondents still opted not to bring them in. Add to that, nearly half (47%) of studied ransomware victims reportedly paid the ransom. It's clear that organizations should abandon these misconceptions around ransomware.

Paying a ransom, and avoiding law enforcement, may only drive-up incident costs, and slow the response.

Security Teams Rarely Discover Breaches Themselves
Threat detection and response has seen some progress. According to IBM's 2023 Threat Intelligence Index, defenders were able to halt a higher proportion of ransomware attacks last year. However, adversaries are still finding ways to slip through the cracks of defence.

The report found that only one in three studied breaches were detected by the organization's own security teams or tools, while 27% of such breaches were disclosed by an attacker, and 40% were disclosed by a neutral third party such as law enforcement.

Responding organizations that discovered the breach themselves experienced nearly $US1 million less in breach costs than those disclosed by an attacker ($US5.23 million vs. $US4.3 million).

Breaches disclosed by an attacker also had a lifecycle nearly 80 days longer (320 vs. 241) compared to those who identified the breach internally. The significant cost and time savings that come with early detection show that investing in these strategies can pay off in the long run.

Additional findings in the 2023 IBM report include:

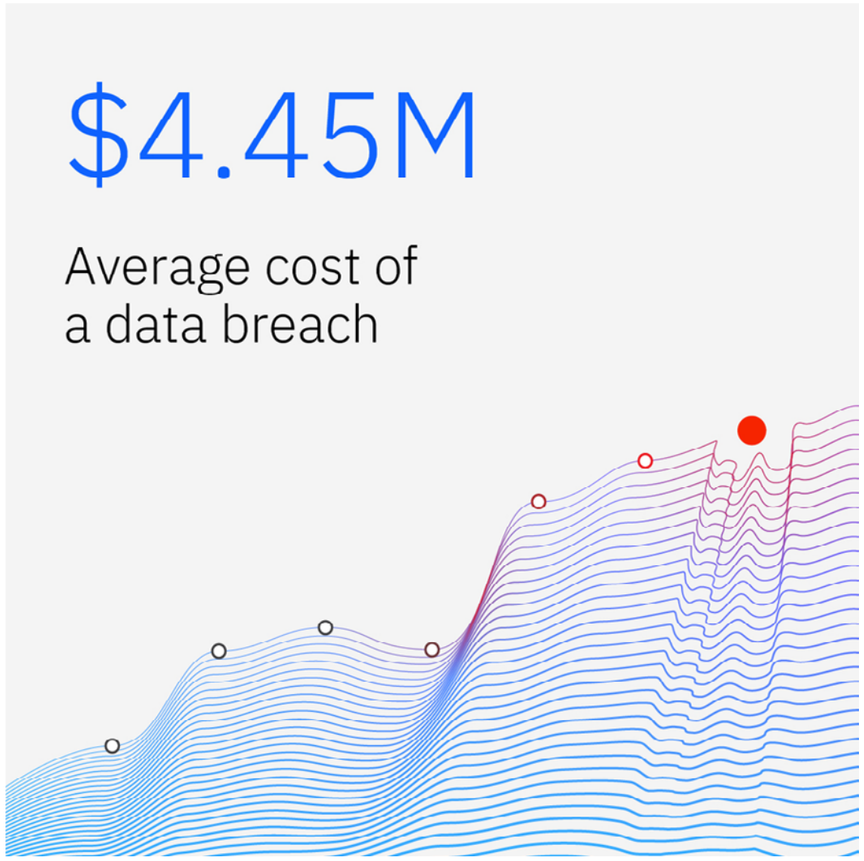
■Breaching Data Across Environments – Nearly 40% of data breaches studied resulted in the loss of data across multiple environments including public cloud, private cloud, and on-prem - showing that attackers were able to compromise multiple environments while avoiding detection. Data breaches studied that impacted multiple environments also led to higher breach costs ($US4.75 million on average).

■Costs of Healthcare Breaches Continue to Soar – The average costs of a studied breach in healthcare reached nearly $US11 million in 2023 – a 53% price increase since 2020. Cybercriminals have started making stolen data more accessible to downstream victims, according to the 2023 X-Force Threat Intelligence Report. With medical records as leverage, threat actors amplify pressure on breached organizations to pay a ransom. In fact, across all industries studied, customer personally identifiable information was the most commonly breached record type and the costliest.

■The DevSecOps Advantage – Studied organizations across all industries with a high level of DevSecOps saw a global average cost of a data breach nearly $US1.7 million lower than those studied with a low level/no use of a DevSecOps approach.

■Critical Infrastructure Breach Costs Break $5 Million – Critical infrastructure organizations studied experienced a 4.5% jump in the average costs of a breach compared to last year – increasing from $US4.82 million to $US5.04 million – $590K higher than the global average.

Download a copy of the 2023 Cost of a Data Breach Report at: https://www.ibm.com/security/data-breach.



Global call to end social data scraping

A group of 12 nations, including Canada, Australia, the UK and New Zealand, have issued a joint call on social media companies (SMCs) to protect personal information on their platforms from unlawful data scraping.

A statement issued week by the national regulatory bodies, including the Office of the Australian Information Commissioner, Australia, and Office of the Privacy Commissioner, New Zealand, included a series of "recommendations" to prevent data scraping.

Although it was pointed out that many of these recommendations are explicit statutory requirements in particular jurisdictions "or may be interpreted as such by courts and data protection authorities."

"Social media companies and the operators of websites that host publicly accessible personal data have obligations under data protection and privacy laws to protect personal information on their platforms from unlawful data scraping," the group said in a joint letter.

The statement has also been simultaneously delivered to Alphabet Inc. (YouTube), ByteDance Ltd (TikTok), Meta Platforms, Inc. (Instagram, Facebook and Threads), Microsoft Corporation (LinkedIn), Sina Corp (Weibo), and X Corp. (X, previously Twitter).

It states SMCs and other websites should implement multi-layered technical and procedural controls to mitigate the risks from unlawful data scraping.

A series of controls were suggested including:

- "Rate limiting" the number of visits per hour or day by one account to other account profiles, and limiting access if unusual activity is detected.
- Monitoring how quickly and aggressively a new account starts looking for other users. If abnormally high activity is detected, this could be indicative of unacceptable usage.
- Taking steps to detect scrapers by identifying patterns in "bot" activity. For example, a group of suspicious IP addresses can be detected by monitoring from where a platform is being accessed by using the same credentials from multiple locations. This would be suspicious where these accesses are occurring within a short period of time.
- Taking steps to detect bots, such as by using CAPTCHAs, and blocking the IP address where data scraping activity is identified.
- Where data scraping is suspected and/or confirmed, taking appropriate legal action such as the sending of "cease and desist" letters, requiring the deletion of scraped information, obtaining confirmation of the deletion, and other legal action to enforce terms and conditions prohibiting data scraping
- In jurisdictions where the data scraping may constitute a data breach, notifying affected individuals and privacy regulators as required.

The statement concludes by requesting that the SMCs respond with feedback within a month demonstrating how they will meet regulators' expectations. Although there is no specific information on what action will be taken if this request is not met.

NZ merges cyber security agencies

New Zealand's Computer Emergency Response Team (CERT NZ) has joined with the country's National Cyber Security Centre (NCSC), the first step in creating a lead operational cyber security agency, similar to those in Australia, the UK, and Canada.

"The key thing for our customers to know is that our existing core services continue," said Lisa Fong, head of the NCSC.

"This initial shift has been designed to minimise disruption to customers, with the move simply transferring CERT NZ's operations and staff from the Ministry of Business, Innovation and Employment to the NCSC."

"We will shortly begin work to design a new integrated operating model that uses our enhanced scale and capability to provide a stronger cyber security system and improved customer service for New Zealanders," said Ms Fong.

In the meantime, CERT NZ and NCSC will continue to deliver existing functions. The full merger will be phased in over several years.

CERT NZ, established in 2017, reported $NZ5.8 million of direct financial losses from cyber incidents in the first quarter of 2023.

"While it will take significant time to complete the integration, we hope to find opportunities along the way to leverage the expertise of both CERT NZ and NCSC in the services we provide."

"Both CERT NZ and NCSC have ambitious programmes of delivery underway, and will continue that work," CERT NZ Director Rob Pope said. "We look forward to providing a more integrated range of products and services to New Zealanders."

AI adoption is racing ahead ungoverned

Almost three-quarters (72%) of Australian businesses are using some form of AI, however only half of respondents (52%) have staff policies in place for its use, according to a report commissioned by solution provider datacom.

Most businesses are expecting AI to bring significant changes to their organisation – with 86% of business leaders believing the integration of AI within Australian businesses will impact operations and workplace structures. This has raised concerns for 1/5 (20%) that do not feel educated on the risks AI poses, as well as 60% expressing security and safety concerns over AI causing a loss of control.

Among the 21% of businesses that were not currently using AI, just over two thirds (67%) expected to be using some form of AI within 1-2 years and a further 13% expected to be using it within three years. Employee use of widely available AI tools, such as ChatGPT, to help them perform their work tasks was also strongly supported by 86% of respondents.

Despite the high level of AI adoption – and predicted use of AI in the near future – a much lower proportion of Australian businesses have implemented policies and legal guidelines to govern the use of AI. In addition, 58% of organisations lack targets around the use of AI, making its success difficult to measure.

Just 52% of respondents had staff policies in place around AI usage, while only 40% had legal guidelines in place for use of AI and 39% had audit assurance and governance frameworks.

Datacom Group CISO Karl Wright says organisations need to be proactive about setting policies to manage associated risks around business data, IP and copyright issues, especially given 86% of respondents said they support their employees using AI tools to carry out their work tasks.

"The use of AI needs to be carefully considered, monitored and governed with clear policies and guidelines in placed to ensure the risks to businesses are minimised," says Wright.

The lack of governance of AI at an organisational level could be a contributing factor to the high number of businesses calling for government legislation and the suggestion from almost two-thirds of survey respondents that the implementation of AI should be management by specialists.

Of the more than 300 respondents, 89% felt there should be legislation for AI use in the public sector and (63%) believed AI implementation should be managed by specialists.

The survey also highlighted security and ethical concerns relating to the use of AI.

The key issues that respondents identified around AI usage were security concerns (60%), a fear of loss of control (60%), ethical concerns around AI use in wider society (45%) and the potential for a reduction in job opportunities for Australians (41%). A fifth of respondents also felt they were not educated about the associated AI security risks that exist.

Respondents were also asked to identify which industries stood to deliver the greatest gains for society from AU usage and which ones posed the greatest risks from the adoption of AI.

Financial services were identified as posing both the greatest risk (30%) and offering the biggest potential gains (22%). Healthcare and the use of AI in areas such as diagnostics were again seen as posing significant risk (28%) and opportunity for improvements (21%). The use of AI in legal services was seen as risky by 28% of respondents, while the use of AI in advertising and marketing was seen as a positive by 22% of business leaders surveyed.

Backlash mounts over UK Voter Data Breach

The UK Electoral Commission is grappling with severe criticism over its belated acknowledgment of a sweeping cyber intrusion that laid bare confidential information linked to 40 million voters.

The Commission identified the breach in October 2022 but delayed announcing it publicly until August 2023. During the period of the breach, which extended back to August 2021, the attackers had access to the Commission's email servers, control systems, and copies of the electoral registers.

The breach was reported within 72 hours to the UK Information Commissioner's Office (ICO), as well as the National Crime Agency. However, the Commisssion chose to withhold this information from the public for 0 months, sparking doubts about transparency, data integrity, and the entity's capacity to manage such incidents effectively.

News about the breach finally emerged through a public notice posted on the Commission's official Web site. According to the notice, the incident was initially identified in October of the previous year when the agency's internal systems flagged unusual activities. It subsequently transpired that unauthorized parties had illicitly accessed the systems as early as August of the year prior.

"The registers held at the time of the cyber-attack include the name and address of anyone in Great Britain who was registered to vote between 2014 and 2022, the names of those registered as overseas voters during the same period, and the names and addresses of anyone registered in Northern Ireland in 2018. "

The breach included full names, email addresses, residential locations, contact telephone numbers, content from web forms, and conceivably personal images submitted to the authority.

Although the Commission stated that "The electoral register data held by the Commission has not been amended or changed in anyway as a result of the attack and remains in the form in which we received it. The data contained in the registers is limited, and much of it is already in the public domain."

"The personal data held on the Commission's email servers is also unlikely to present a high risk to individuals unless someone has sent us sensitive or personal information in the body of an email, as an attachment or via a form on our website, such information may include medical conditions, gender, sexuality, or personal financial details. Information related to donations and/or loans to registered political parties and non-party campaigners is held in a system not affected by this incident."

While the electoral register is able to be inspected by the public this can only be done via electoral registration officers, and only handwritten notes are permitted. The data is not allowed to be used for commercial or marketing purposes.

The tardy revelation of the breach has sparked widespread concern. The digital advocacy group Open Rights Coalition (ORC) vented its displeasure on social media, contending that the undisclosed breach had exposed individuals to the perils of fraud, identity theft, and the potential targeting of homes.

Commission Chair John Pullinger voiced support for withholding information for 10 months, highlighting the potential hazards associated with untimely disclosure prior to addressing security vulnerabilities.

The revelation of the data breach comes as the UK considers replacing traditional paper ballots with an e-voting system. Shaun McNally, Chief Executive of the Commission, claims that maintaining traditional methods will make it harder for cyber-attacks to influence election outcomes.

IRS Under fire for Mismanaged Records

The US Internal Revenue Service is unable to locate thousands of microfilm cartridges storing millions of sensitive business and individual tax account records, a new investigation has found. The IRS is required to create and store microfilm backups of both business and individual tax records and keep them for 75 years and 30 years respectively before destroying them.

Documentation obtained from the IRS's Office of Information Technology show an average of 42 million business tax records were stored on microfilm in Fiscal Years (FY) 2021 and 2022 with an average of 190 million individual tax records stored during this same period.

A review by the US Treasury Inspector General For Tax Administration has "identified significant deficiencies in the IRS's safeguarding, accounting for, and physical storage of its microfilm backup cartridges.

"For example, our physical inspection found empty boxes labeled as including microfilm backup cartridges with no explanation as to the location of the missing cartridges. In addition, our discussions with responsible officials at the current three Tax Processing Centers that house microfilm backup cartridges identified that required annual inventories have not been performed.

The lack of adequate inventory controls also includes no reconciliation of the microfilm backup cartridges noted as being sent from closed Tax Processing Centers to what was physically shipped and received.

"As a result of the lack of adequate inventory controls, the IRS cannot account for thousands of microfilm cartridges containing millions of sensitive business and individual tax account records. The personal taxpayer and tax information included on these backup cartridges is key information that can be used to commit tax refund fraud identity theft."

The report also found the IRS is not in compliance with records management requirements nor is it in compliance with microfilm destruction time frames.

Ken Corbin, the agency's wage and investment commissioner, responded that the report highlights the challenges the IRS has experienced over the last decade due to reduced funding and the attrition of experienced staff. As a result, the agency has had to shift workers to high-priority tasks and this affected its ability to update microfilm inventory records in a timely manner.

While the report notes that the IRS is slowly phasing out its use of such microfilm records, it is likely that their secure storage will remain an ongoing challenge for the IRS for years to come. As such, the report urges IRS officials to address these shortcomings with urgency and to ensure that microfilm records remain an asset for the agency and not a liability.

Kodak alaris
Makes Sense

Want to learn more?
Contact the Kodak Alaris Australia Team
Email : Service-Anz@KodakAlaris.com
Dial Toll Free No : 13002 52747

Services from Kodak alaris

Australian enterprises need to trim their data to minimize risk

Imperva has warned Australian enterprises need to swiftly grasp their data footprint and work towards reducing it in response to the Privacy Act Review Report.

A series of high-profile breaches in the second half of 2022, affecting millions of Australian citizens, prompted government authorities to review the Privacy Act of 1988 and increase the maximum penalties for data breaches from AU$2m to AU$50m. Implementing all 116 transformative proposals would mark the most significant overhaul of the country's privacy and data protection landscape since the inception of the Australian Privacy Principles.

"Companies that start eliminating unnecessary data from their environments now will gain a distinct advantage in responding promptly once all changes are finalized," says Reinhart Hansen, Director of Technology, Office of the CTO at Imperva.

Previous research from Imperva found that the predominant data type that cybercriminals are stealing is Personally Identifiable Information (PII), which comprised 42.7% of data taken.

"In the context of data breaches, leaked information frequently dates back decades and lacks any valid reason for organizational retention. As data privacy regulations become more stringent and data storage costs rise, reducing data footprint has taken precedence in many organizations. Proactively identifying and eliminating unnecessary data reduces operational security and business risk by minimizing organizational exposure to breaches. In addition, it also reduces costs, financial penalties, and strengthens data security."

Yet, navigating this path to streamlined data presents a challenge for many. The expansive data landscape in modern enterprise environments makes it difficult to determine where to begin and what to prioritize. In many cases, valuable data originates from an organization's customers (service consumers) and begins its journey as structured data within a database. It is at this early stage in the data lifecycle that organizations must intensify their efforts in securing and monitoring data. However, attention often redirects only after data shifts from controlled realms to unstructured formats, rapidly permeating the enterprise.

A prime challenge that organizations confront in their privacy initiatives is safeguarding unstructured data – emails, messages, and conversation transcripts. A recent Gartner survey found that half of the respondents witnessed a 25% increase in the volume of unstructured data between January 2022 to January 2023.

"There's a shift in focus towards unstructured data, as businesses often have little insight into what risk exposure this type of data presents. If an organization cannot manage this data type today, the problem will grow exponentially. By connecting unstructured data sources, businesses can gain a credible inventory and discover hidden data that could put their organization at risk."

Here are some specific steps organizations can take to have a more comprehensive and effective data-centric security ecosystem.

Data discovery and classification: Many organizations are undertaking large-scale data classification projects to ensure valuable information stored in shadow databases is maintained. By categorizing data on its sensitivity, business criticality, and relevance, initiatives can be undertaken to identify and tag data for deletion or offloading. Doing so has the net outcome of reducing the overall data risk footprint and driving down the cost associated with data storage and retention of data that no longer serves a purpose.

Data masking: In pursuit of efficiency and innovation, development teams testing applications often cause the spread of sensitive production data to non-production and staging environments. This significantly increases non-compliance with data privacy responsibilities and data breach risks. Organizations can mitigate these risks by replacing production data sets with masked and tokenized sensitive data that retains the original semantics and is equally helpful for development teams in non-production environments. This process involves creating a realistic but fake version of organizational data to protect sensitive information while providing a functional alternative when real data is unnecessary.

Unified data environment: A centralized data protection environment will streamline data management processes, enhance security and privacy measures, and ensure the application of policies to data regardless of its type (structured or unstructured) or location (on-premise and/or cloud). This ultimately leads to improved efficiency and reduced total cost of ownership.

Forensics experts release Australian Scam Culture Report

Traffic and trading on the dark Web continues to rise, with approximately 2.7 million daily users in 2023, up from 2.5 million in 2022, according to BDO's inaugural Australian Scam Culture Report.

"Surprisingly, illegal trading or associated activity by criminals only makes up half of dark Web activity. Of that, 67 per cent is forums, chat rooms and data hosts, followed by narcotics trading (8 per cent), the sale of firearms (6 per cent) and financing services (6 per cent).

"The remaining 19 per cent includes such things as stolen data, services for hire, malicious software and content from extremist groups," said Michael Cassidy, BDO's National Leader of Forensics.

The new report from BDO – which will be released quarterly into the future - shows that over the June quarter the top traded items on the dark Web were fraud and counterfeit products (such as passports, credit ratings and credit cards, and Facebook accounts) and corporate data (such as user IDs, passwords and intellectual property).

"Many people are surprised to learn that about half of the activity on the dark Web is entirely legal. In addition to some traditional business entity presence, there are also other groups such as anti-vaccination, anti-government, conspiracy theorists and information disseminators looking for a place that is not easily accessible or searchable by traditional means," Michael said.

Costs continue to fluctuate on the dark Web with the June quarter showing COVID-19 vaccination certificates trading for $A119, false passports trading for $A2,255 and Australian drivers' licences for $A526.

The cost of hacked cryptocurrency accounts has varied significantly, with an average drop of 72 per cent in the last 12 months. Cloned SIM cards fell by 33 per cent in the last quarter down to $A399 from $A599.

The data for 2023 to date shows an increase in hacked social media accounts for sale, up by 32 per cent from 2021, with Facebook, WhatsApp, Instagram and Telegram accounts all trading for around $A119 each.

The dark Web currently has over 10,000 ChatGPT accounts available for sale.

"Anyone can sign up for a free ChatGPT account, but people are looking for paid ChatGPT accounts on the dark Web to get enhanced accuracy and response time, plus priority access during peak times.

"Faster response times and enhanced accuracy make for a more authentic and conversational experience, which is the type of content people want the AI to generate.

"We expect these accounts to become more valuable as usage continues to increase," Michael said.

Michael commented that interestingly there is increased negotiation activity on the dark Web, with traders and buyers communicating to negotiate their own terms.

"Like any marketplace, trust is crucial to make a transaction. But this is heightened on the dark Web, because if an illegal transaction doesn't go to plan, there is no recourse. To address this, we are seeing market operators mediating with buyers and sellers to negotiate a solution" Michael said.

From a consumer point of view, despite common belief that identity theft and romance scams are the most popular of the moment, these two make up only nine per cent of scam activity in 2022, with investment scams making up for 70 per cent of scams last year.

In 2023, text message has overtaken phone call as the leading delivery method scammers are using.

"Up until 2021, a phone call was the most common way that scammers were reaching people, but in 2023 the text message has overtaken the phone call and is now the mode of choice. One of the reasons scammers have changed tact is due to society's reluctance to answer phone calls from unknown numbers and the increased use of screening apps that assist people to identify scam calls," Michael said.

"Text messages are working for scammers because people have their phone on them all the time, and we're accustomed to taking a quick glance and actioning something without really thinking," he said.

"Of course, scammers these days are skilled at posing as trusted brands, organisations and human contacts – known as spoofing – which makes it harder to detect a scam over a legitimate communication."

"This really is a golden era for scammers – people are using their phones to do their day-to-day admin, business systems are connected to people's personal devices, and AI is ramping up and giving scammers an opportunity to automate and tailor their approach, meaning they will reach more people with more ease," Michael said. "One thing people may need to be aware of in the future is scammers using AI generated voice activity to bolster their attacks. This might involve using a sample of someone's voice to make seemingly human conversation with their targets.

"In essence, it could be an extension of the Hi Mom scam, where a fake child asks their mum for money to help them get out of trouble, but instead of a text, it'll be a call that sounds just like their son or daughter. Of course, these tactics could be used to scam businesses as well."

Download REPORT

COMPANIES WITH ANSWERS AND SOLUTIONS FOR YOUR DIGITAL TRANSFORMATION INITIATIVES

EzeScan is one of Australia's most popular production capture applications and software of choice for many Records and Information Managers. This award winning technology has been developed by Outback Imaging, an Australian Research and Development company operating since 2002. Solutions range from centralised records capture, highly automated forms and invoice processing to decentralised enterprise digitisation platforms which uniquely align business processes with digitisation standards, compliance and governance requirements. With advanced indexing functionality and native integration with many ECM/EDRMS, EzeScan delivers a fast, cost effective method to transform your manual business processes into intelligent digital workflows.

EzeScan benefits include: initiate intelligent automated processes; accelerate document delivery; minimise manual document handling; capture critical information on-the-fly; and ensure standards compliance.

www.ezescan.com.au | info@ezescan.com.au | 1300 393 722

Newgen offers a unified digital transformation platform that includes native process automation, content services, and communication management capabilities. Globally, many successful enterprises across various industries rely on the NewgenONE digital transformation platform—a comprehensive and unified cloud-based platform with low code capability for rapid development of content-driven, customer-engaging business applications. The platform can transform and simplify complex business processes. Equipped with cutting-edge technologies, including mobility, social listening/sensing, analytics, cloud, artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA), the NewgenONE platform helps enterprises stay ahead of the curve. From grass-root citizen experience management, dynamic case management to electronic documents and records management, lending to underwriting, the platform solves multiple use cases across various industries, including government, banking, insurance, and others. Furthermore, Newgen has a robust partner ecosystem, including global system integrators, consulting and advisory partners, value-added resellers, and technology partners.

newgensoft.com/home-anz/ | info@newgensoft.com | +61 2 80466880

INFORMOTION is an innovative professional services organisation specialising in the design and implementation of modern information management, collaboration and governance solutions – on-premises, in the cloud or hybrid. INFORMOTION's workflow tools, custom user interfaces and utilities seamlessly combine to deliver compliance, collaboration, capture and automation solutions that provide greater business value and security for all stakeholders. We can help you map and successfully execute your digital transformation strategy. Boasting the largest specialist IM&G consulting teams in Australia with experience that spans over twenty years, INFORMOTION consultants have a deep understanding of business and government processes and the regulatory frameworks that constrain major enterprises. Our compliance experience is second-to-none. INFORMOTION is a certified Micro Focus Platinum Partner and global Content Manager implementation leader. We are also an accredited Microsoft Enterprise Business Partner, Ephesoft Platinum Partner and EncompaaS Diamond Partner.

informotion.com.au | info@informotion.com.au | 1300 474 288

UpSol are experts in Digital Transformation and Business Process Re-engineering with strong domain expertise in Data Capture, Document Management, Organisational Workflow, Electronic Forms, Data Integration

upsol.co.nz | sales@upsol.co.nz| 0800 003 115

Kapish is a member of the Citadel Group (ASX:CGL).Citadel solve complex problems and lower risk to our clients through our tailored advisory, implementation and managed services capabilities. With over 250 staff nationwide and an ability to 'reach back' and draw on the expertise of over 1,500 people, we are specialists at integrating knowhow, systems and people to provide information securely on an anywhere-anytime-any device basis. Servicing both large and small, public and private sector organisations across all industries, our team of highly qualified staff have global experience working with all versions of Micro Focus Content Manager (CM). It is this experience coupled with our extensive range of software solutions that enable our customers and their projects to be delivered faster, more cost-effectively and with more success. At Kapish we are passionate about all things Content Manager. As a Tier 1, Micro Focus Platinum Business Partner, we aim to provide our customers with the best software, services and support for all versions of the Electronic Document and Records Management System, Content Manager. Quite simply, our products for CM make record-keeping a breeze.

kapish.com.au | info@kapish.com.au | 03 9017 4943

Esker is a global leader in cloud-based document process automation solutions. Esker's solutions are compatible with all geographic, regulatory and technology environments, helping over 11,000 companies around the world improve efficiency, visibility, and cost-savings associated with the processing and exchange of information. Founded in 1985, Esker operates in North America, Latin America, Europe and Asia Pacific with global headquarters in Lyon,

France and U.S. headquarters in Madison, Wisconsin and AUS/NZ headquarters in Sydney, Australia since 1997. Esker's solutions span the order-to-cash and purchase-to-pay cycles — allowing organisations to automate virtually any business process:

- Order Processing: automated entry and routing of incoming customer orders
- Accounts Receivable: automated sending and archiving of paper and e-invoices
- Collections Management: streamlined post-sale collection interactions
- Accounts Payable: automated entry and routing of incoming supplier invoices
- Purchasing: electronic processing and delivery of supply chain documents.

www.esker.com.au | info@esker.com.au | 02 8596 5100

FileBound Solutions offers cloud-native, work automation and document management solutions that can be used to underpin any organisation's digital transformation program. These solutions are based around the FileBound software platform and are able to be deployed in organisations of all sizes. The solutions can include capture, document management, workflow, electronic forms, analytics, mobile access, advanced business system integration capabilities and much more. Solutions from FileBound Solutions deliver organisational efficiencies, drive out manual paper-based processes to decrease costs, increase productivity and support compliance with internal and external mandates. FileBound Solutions customers have the flexibility to create a variety of solutions from complex A/P automations to simple document archival and retrieval processes.

www.filebound.solutions | www.filebound.solutions/contact | 1300 375 565

Collaborate with confidence. AvePoint is the largest Microsoft 365 data management solutions provider, offering a full suite of SaaS solutions to migrate, manage and protect data. More than 8 million cloud users rely on our solutions to make their organisations more productive, compliant and secure. Founded in 2001, AvePoint is a five-time Global Microsoft Partner of the Year and headquartered in Jersey City, New Jersey.

AvePoint Cloud Records is a SaaS based, IRAP certified and VERS compliant solution used to manage the information lifecycle including content classification; retention and disposal; comprehensive auditing; reporting; and physical records. The Public Office Record of Victoria (PROV) has certified that government agencies and enterprise customers alike can leverage AvePoint Cloud Records to overcome physical and electronic records management challenges around authenticity, reliability, and ensuring content is maintained in a compliant format long-term.

www.avepoint.com| sales@avepoint.com | (03) 8535 3200

UPFLOW

UpFlow is a provider of Document Capture, RPA, Document Management, Workflow, Electronic Forms and Integration software products and services throughout APAC region.

UpFlow distributes and resells products such as:

- **Ephesoft Transact**, which can accept images from a variety of input sources, and can output the extracted data in all major file formats for easy integration into RPA, BPM, ECM, iPaaS platforms or any workflow app or other repository.

- **PSIcapture**, an innovative document capture platform that provides unmatched integration with just about any ECM or ERP platform [e.g. SharePoint, Xero, Trim, Objective etc.] and allows the utmost in flexibility for deployment in large or small organisations.

- **FileBound** is a Document Management and Workflow solution platform that delivers process automation that increases efficiency and improves control by enforcing business workflows and corporate policies.

- **Integration and Robotic Process Automation solutions** that provide fully featured Integration, attended or unattended Bots for the automaton of enterprise work.

- **Kofax Power PDF**, easily edit, create, markup, collaborate real-time, secure, redact, share, or eSign PDF files. Convert PDFs to or from virtually any document.

If you want to add high quality, profitable, business automation products to your list of products and services then contact UpFlow today.

www.upflow.solutions | info@upflow.com.au | AUS: 1300 790 360 NZ: 0800 003 115

ENCOMPAAS

EncompaaS is a global software company specialising in information management, powered by next-gen AI. Leading corporations, government departments and statutory authorities trust EncompaaS to govern and optimise information that resides within on-premises and multi-cloud environments. Organisations are empowered to solve information complexity, proactively address compliance and privacy risk, and make better use of data to act strategically at pace. EncompaaS is distinguished in the way the platform utilises AI to build a foundation of unparalleled data quality from structured, unstructured and semi-structured data to de-risk every asset. From this foundation of data quality, EncompaaS harnesses AI upstream to unlock knowledge and business value that resides within information. EncompaaS maintains a robust partner ecosystem, including global consulting and advisory firms, technology partners, and resellers to meet the diverse needs of highly regulated organisations.

encompaas.cloud | enquiries@encompaas.cloud | 1300 474 288

iCognition

Information Management and Governance (IMG) specialist, iCognition Pty Ltd, helps our clients to maximise the value of their information assets, while minimising cost and risk. We use an integrated Information Management and Governance approach that combines the disciplines of data, records, and information management to value, manage, control and harness information across the enterprise. iCognition's Electronic Document and Records Management System-as-a-Service (EDRMSaaS) represents 20 years of iCognition experience. It is a proven, secure and trusted Software-as-a-Service offering for Content Manager. It can also include iCognition's award-winning RM Workspace for secure web-based end-user access and collaboration, Office365RMBot for fast and easy information governance of Office 365 information, RM Workflow to deliver easy-to-use Content Manager workflows, and RM Public View for publishing and sharing to non-Content Manager users.

www.icognition.com.au | info@icognition.com.au| 1300 00 4264

Kodak alaris

Kodak Alaris is a leading provider of information capture solutions that simplify business processes. Digital Transformation is the need of the hour for many organisations, and it starts with information and data capture. We exist to help the world make sense of information with smart, connected solutions powered by decades of image science innovation. Alaris drives automation through every business process dependent on document and data capture so that you can get the right information to the right place at the right time. Our award-winning range of scanners, software and services are available worldwide, and through our network of channel partners.

www.alarisworld.com/en-au | Angelo.Krstevski@kodakalaris.com | 0419 559960

Microsoft expands DLP options in Purview

Microsoft has announced new capabilities in Purview Data Loss Prevention, including (OCR) in Exchange Online and Teams.

With this capability, the DLP engine is able to extract text from images, quickly recognize if the image contains sensitive information such as credit card or social security numbers and prevent users from sharing such images. OCR for SharePoint and Endpoint is currently in public preview.

Purview is available for Exchange, SharePoint, and OneDrive as part of the M365 E3 license and DLP for Teams and Endpoint is part of the M365 E5 license (and other E5 variants).

Additionally, Microsoft is bringing document fingerprinting support to SharePoint Online, One Drive, Teams, and Windows Endpoint.

Document fingerprinting is a Microsoft Purview Data Loss Prevention (DLP) feature that converts a standard form into a sensitive information type (SIT), which you can use in the rules of your DLP policies. For example, you can create a document fingerprint based on a blank patent template and then create a DLP policy that detects and blocks all outgoing patent templates with sensitive content filled in.

Purview Data Loss Prevention is also getting a new feature that prevents employees from pasting sensitive information to select websites.

Organizations can now set DLP policies to prevent their users from copying and pasting sensitive information such as personally identifiable information (PII) from organization's internal databases such as SQL server, KUSTO databases, customer relationship management (CRM) tools and more to their personal email accounts, generative AI chatbots, and social media sites on supported browsers, including Microsoft Edge, Chrome, and Firefox.

DLP protection has been extended for sensitive files stored on network shares. With this capability organization's DLP policies to restrict common egress actions such as copy to USB, print, upload to cloud and more can be automatically extended to files containing sensitive information on network file shares as well.

Priva boosts privacy & compliance integration

Microsoft has announced a series of enhancements to Priva, its platform for identifying personal data and critical privacy risks in M365, including closer integration with Purview Compliance Manager.

With this update, admins can take specific actions within Microsoft Priva that achieve points that count toward compliance assessment completion and increase the overall compliance score. Examples of actions that can detect and provide credit include admins setting up a Privacy Risk Management policy or enabling data retention limits for a subject rights request.

Additionally, insights from Compliance Manager will now populate within Priva itself.

Priva Privacy Risk Management now provides administrators with access to data minimisation policy insights 72 hours after starting Priva, with a view of data up to the past 90 days.

"Previously, customers would have waited at least 30 days to catch policy matches," said Kacey Lemieux, director of compliance and privacy marketing at Microsoft in a blog post. "With a better history of data, privacy admins can understand privacy trends better, and use these data points to strategise the best approach for their organisations."

Priva Privacy Risk Management leverages auto-classification technology to identify more than 308 personal data types in the Microsoft 365 environment, with no configuration needed.

Organizations can create policies from pre-configured templates to automate privacy risk mitigation.

Admins can configure Priva to help employees make better data-handling decisions. Microsoft Priva can trigger a system-generated email or Microsoft Teams message to a data owner with recommended actions and privacy best practices.

Priva Subject Rights Requests is another new feature introduced to manage the right to be forgotten, giving people the ability to request the deletion of all the information an organization has collected about them.

"According to Gartner, by the end of 2024, three-quarters of the world's population will have personal data covered by modern privacy regulation," said Lemieux.

The ability to configure delete as a request type is now included in Priva. This will kick off a workflow to streamline deletion and also deliver a summary report.

"For organizations, the process of completing subject rights requests can be a manual, complex, time-consuming, and expensive process, that is also time bound. Microsoft Priva Subject Rights Requests help organizations manage requests at scale and with confidence," said Lemieux.

Automation Hero introduces new fraud prevention capabilities

In an age where document-centric processes are central to business operations, the risk of fraud and manipulation looms large. And, with increased digitization, many changes have been deployed at the front end; however, back-end processes and systems remain untouched, which raises the question: have all changes been assessed for their vulnerability to fraud?

Similarly, return fraud is a growing concern for retailers, accounting for over 10% of total retail returns.

To combat these issues, Automation Hero has introduced new capabilities for its intelligent document processing platform that supports intelligent document forensics.

The AI-powered platform helps determine if documents involved in any process have been potentially manipulated, combating fraud and ensuring authenticity.

Document forgery encompasses a wide range of deceptive practices involving the manipulation of documents to deceive others into believing they are genuine.

Some common types of document forgery include:

Signature forgery: Fraudsters alter or replicate signatures to misrepresent a document's authenticity and authorization.

Altered content: Documents are tampered with to change critical information, such as dates, amounts, or terms.

Counterfeit documents: Criminals create completely fake documents to impersonate legitimate ones.

Photocopy manipulation: Unauthorized alterations are made to photocopies of documents to present false information.

Common strategies in insurance fraud

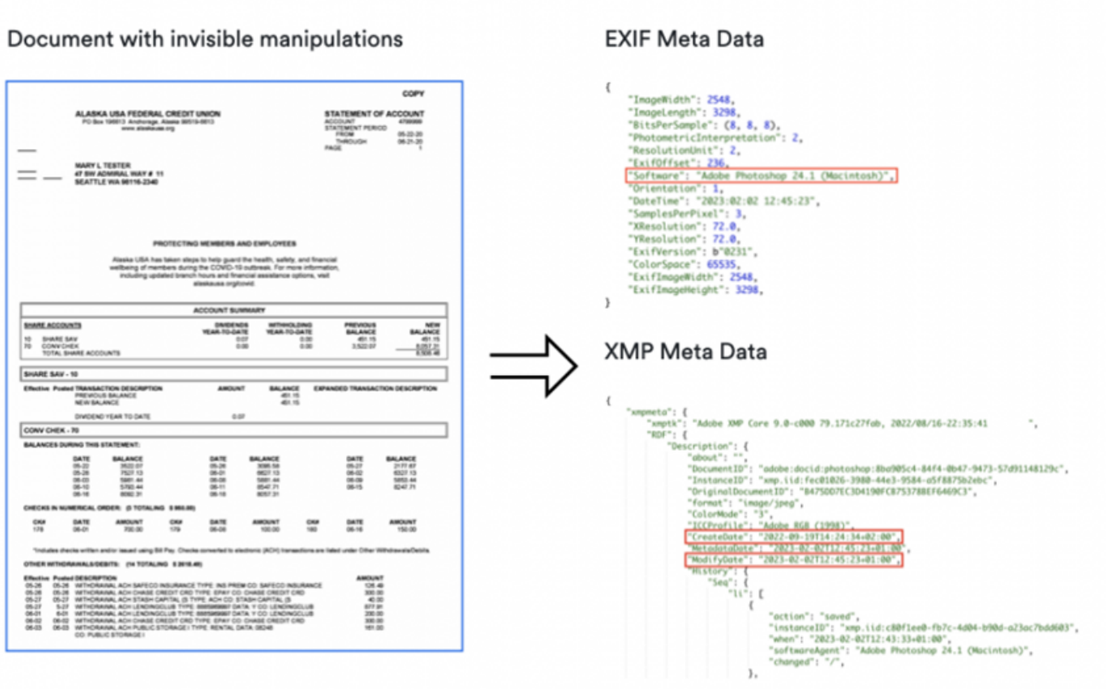
Insurance fraud is a pervasive issue, and fraudsters adopt various strategies to deceive insurers. Some common strategies include:

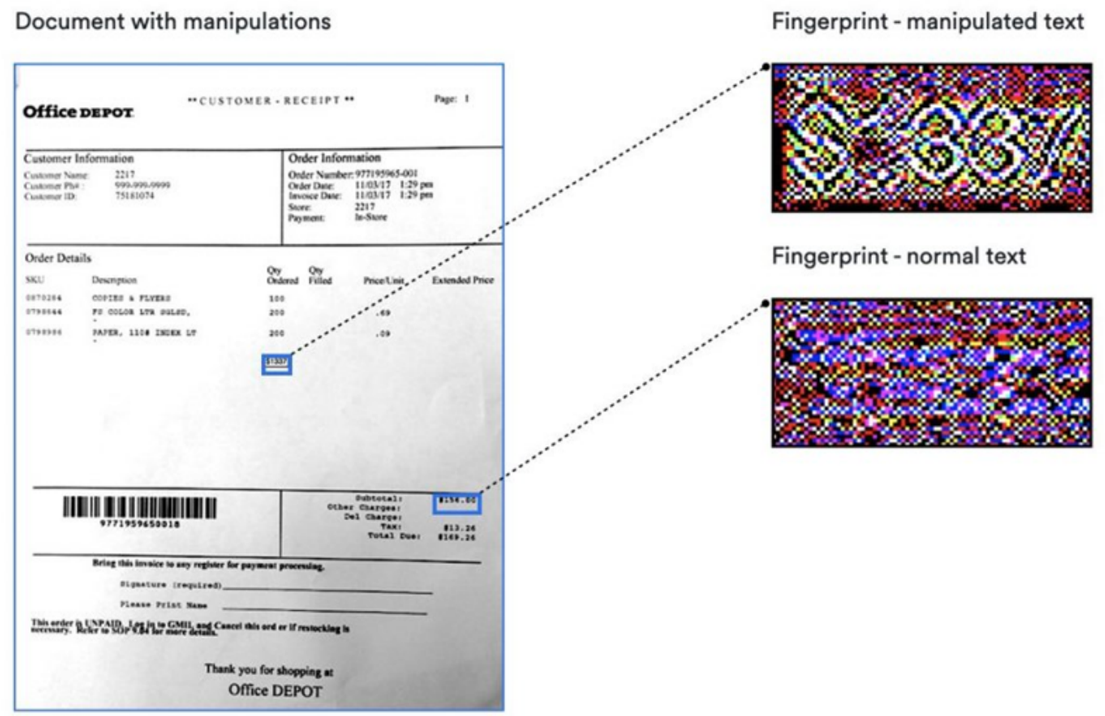
False claims: Policyholders submit claims for damages or losses that never occurred.

Exaggerated claims: Legitimate losses are reported, but the claimant exaggerates the extent of damage or the value of lost items to receive a larger payout.

While many insurers have dedicated fraud mitigation units, their effectiveness is often limited by various challenges:

Problems with data quality: Insurers face data quality issues, including errors, omissions, and inconsistencies across different systems, impacting analytical tools' efficacy.





Limited use of analytical tools: The lack of advanced technology tools like predictive analytics and fraud detection systems hampers proactive and timely fraud detection.

Issues with data protection and privacy: Stringent data protection policies can lead to limited access to crucial data, making fraud risk mitigation a significant challenge.

In the digital era, document forgery has become more sophisticated, making traditional detection methods insufficient. To combat this, leveraging advanced AI capabilities is crucial. Some cutting-edge techniques to detect document forgery include:

Image analysis: AI algorithms can scrutinize document images for irregularities, inconsistencies, and signs of tampering.

Pattern recognition: Advanced AI can identify unique patterns in signatures and handwriting, distinguishing between genuine and forged content.

Metadata examination: Analyzing metadata can unveil clues about a document's origin and potential modifications.

Text analysis: AI-powered algorithms can detect copy-paste or other text alterations that may indicate forgery.

Automation Hero's end-to-end platform integrates document forensics, bolstering fraud risk mitigation. Some of the key methods utilized by the platform include:

EXIF and XMP data analysis: Metadata within document files provides vital information about post-scanning alterations and the software used for modifications.

Scan fingerprint analysis: Subtle patterns in document scans reveal manipulations that are barely visible to the human eye, exposing any anomalies.

Copy-paste detection: This method identifies instances of identical text, exposing fraudulent alterations made by copying and pasting text.

In a world riddled with document forgery and manipulation, Automation Hero's intelligent document processing platform is a game-changer. By leveraging advanced AI capabilities for intelligent document forensics, they enable businesses to detect potential fraud and ensure the authenticity of documents within their processes. This helps combat insurance fraud, reducing its staggering annual costs, and protects retailers from return fraud, enhancing profitability.

You can also check out our video below, which provides a demo.

https://youtu.be/VoFHnjLDXoc

Agiloft puts Contract AI Into the Hands of Non-Technical Users

Agiloft has announced the release of AI Trainer, a new AI model training capability that will empower non-technical users to fully customize the way they review and analyze contracts.

AI Trainer empowers non-technical, subject matter experts to train Agiloft's AI to identify important key terms and clauses, so they can quickly analyze and draw actionable insights from their contracts, then share that business-critical intelligence with the rest of their organization to drive real enterprise value.

Agiloft's AI Trainer also actively accelerates its own training process by continuously learning and then auto-suggesting additional relevant data for users to consider tagging.

"No two contracts are quite alike, nor are any two organizations. That is why relying on pre-trained, generic AI models alone simply does not get the job done," explained Agiloft's Chief Product Officer Andy Wishart.

"We are introducing AI Trainer to ensure more organizations can use our best-of-breed AI to surface, analyze, and report on their contracts effectively.

"This provides legal and contracting teams with an easy-to-use, self-service tool that helps them codify their expertise to enhance the automation of the contracting process.

"AI Trainer empowers the very teams who are closest to the contracting process and gives them a way to train and individualize the systems they use to uncover and categorize key terms and clauses in their contracts."

AI Trainer is designed to put the power of artificial intelligence fully into the hands of non-technical users. In keeping with the entire Agiloft platform, AI Trainer offers users a no-code environment to create their own AI models to better automate the process of reviewing large numbers of contracts.

This will accelerate contract review cycles and help organizations reveal the valuable information that can otherwise be trapped in their contracts.

"CLM should be viewed as an enterprise solution, rather than just legal technology, so a legal department's partners – in sales, procurement, and finance – need to be able to easily find and interact with the invaluable data that is contained within their contracts." adds Eric Laughlin, Agiloft's CEO.

"Using AI to identify party names, dates, and common clauses is necessary but insufficient. The organizations that create competitive advantage will be those who are able to extract and use the information that is uniquely valuable to their environment and unlikely to be covered by pre-trained models – for example legal and commercial terms unique to their industry niche or company. That's why we are so excited for our customers to use AI trainer – it puts that power in their hands."

AI Trainer enables users to easily create custom AI models to examine business-specific elements of their contracts, including clauses, important key terms, and obligations that will help them to monitor risk, performance, and compliance.

The outcome is a rapid, individualized model of an organization's contracts, which enables teams to surface potential risks before they become problems, identify opportunities for competitive advantage, and ensure compliance across a range of regulations.

https://www.agiloft.com/

Sovereign cloud for Local Law Firms

AUCloud has partnered with managed services provider LexVeritas to launch LexCloud, Australia's first dedicated sovereign cloud solution designed for Australian law firms.

The LexCloud solution is designed to address the growing need for enhanced security and data management capabilities across Australia's legal sector.

AUCloud CEO Peter Maloney said the partnership represented a transformative opportunity for the legal sector to become more cyber-resilient and efficient when it comes to storing and managing data.

"Our mission has always been to safeguard Australia's sensitive data and empower businesses with secure cloud and cyber security solutions.

"LexCloud provides the legal sector with a powerful tool that ensures data sovereignty, enables collaboration, and reinforces the industry's cyber resilience."

Key features of LexCloud include:

■Sovereign Cloud Infrastructure: LexCloud is hosted on AUCloud's sovereign infrastructure, ensuring that sensitive legal data remains within Australia's borders, promoting data sovereignty and complying with regulatory requirements.

■Advanced Cyber Security: LexCloud offers multi-layered security measures, safeguarding law firms against potential cyber threats.

■Scalability and Flexibility: The cloud solution is designed to cater to law firms of all sizes, offering scalability and adaptability to accommodate growth and changing requirements.

www.lexveritas.com.au/lexcloud

AIRA launches V2.0 of IDP solution

AIRA has announced Version 2.0 of its Intelligent Document Processing solution which includes three new features: vision-based segmentation, new AI models for text extraction that are trained to understand the nuances of language, and improved OCR so that noisy documents are transcribed correctly.

One of the challenges in document processing lies in dealing with various document formats - from invoices to contracts to legal documents. AIRA 2.0 incorporates vision-based segmentation. This technology uses visual cues to identify different sections within a document, adapting its processing methods accordingly. Whether it's tables, paragraphs, or images, AIRA 2.0's vision-based segmentation ensures precision and context awareness in document processing, regardless of the document's format.

Text extraction forms the core of IDP, as it converts unstructured information into actionable insights. AIRA 2.0 integrates advanced AI models trained to understand the intricacies of language, enabling them to accurately extract relevant information even from complex, context-rich documents.

OCR has been a cornerstone of document processing, converting scanned images into machine-readable text. With AIRA 2.0, improved OCR algorithms ensure that slightly skewed/noisy documents are accurately transcribed, reducing errors and manual intervention. This enhancement directly translates into enhanced data integrity and minimized processing time, enabling organizations to operate at peak efficiency.

The convergence of AI, machine learning, and advanced data analysis is poised to drive continuous innovation in this field:

Cognitive Document Understanding: The future will witness IDP systems understanding not just the text, but the meaning and context behind it. This will enable deeper insights and better decision-making.

Multimodal Document Processing: IDP will evolve to process a variety of document types, including images, expanding its capabilities to handle diverse data sources.

RealTime Document Processing: With the increasing need for agility, real-time document processing will become a standard feature, enabling businesses to respond swiftly to dynamic situations.

https://aira.fr/

Enhancing IDP with Generative AI

Datamatics has announced the integration of Generative AI with Datamatics TruCap+, an AI-powered, template-free Intelligent Document Processing (IDP) solution. Data extracted through TruCap+ integrates well with Robotic Process Automation (RPA) to deliver benefits of true automation

The enhanced solution offers a range of powerful capabilities, including:

TruCap+ uses Generative AI for out of the box extraction with high accuracy.

TruCap+ seamlessly incorporates documents from different channels, formats, and layouts without requiring any setup or configuration time. So, organizations can quickly add new data sources without hassle.

TruCap+ can perform complex checks and validations on the extracted data using prompts that resemble specific business rules or criteria. This makes it easy to extract insights and ensure data quality. TruCap+ provides built-in functionality to query and analyse the extracted data within the same environment or interface. This makes it convenient for organizations to work with the data without switching between different tools.

TruCap+ extracts information from multiple documents or data sources and combines relevant data points to create a more accurate output. This helps resolve inconsistencies, fill in missing information, and validate data against multiple sources, enabling organizations to make confident data-driven decisions.

TruCap+ can accurately extract data from documents written in various Roman script languages such as English, Spanish, French, Italian, German, and many more

https://www.datamatics.com/intelligent-automation/idp-trucap

Generative AI for Content Collaboration

Egnyte has announced several new AI-powered solutions being natively integrated into the Egnyte content collaboration and governance platform. Egnyte customers will now be able to use the latest generative AI models to find and summarize information contained in their company's documents and media files, without having to physically move any of their content, which could violate corporate policies and put their data at risk.

Through a simple, chat-based interface, everyday business users will be able to ask Egnyte's AI to answer questions and perform tasks related to the files they have been granted access to on Egnyte's platform. The AI can perform tasks such as:

- Generating summaries of large complex documents
- Creating text-based transcripts of audio and video files
- Finding photos within your image library containing a particular object

The solution leverages Egnyte's content governance framework and private instances of various AI models to ensure both the source data and AI-generated responses adhere to each company's security and compliance policies.

These new features complement Egnyte's other embedded AI applications, which are used by customers to classify and protect sensitive data, comply with privacy regulations such as GDPR and CCPA, and detect anomalous usage patterns that may be indicative of a data breach or insider threat.

Access to Egnyte's generative AI-powered solutions is currently being offered in limited availability to select customers. A wider roll-out schedule, including additional AI-powered applications, will be announced upon general availability at a later date.

To learn more about how Egnyte's content platform can transform your business, contact the Egnyte team today by visiting egnyte.com.

EPSoft Technologies Unveils Process Co-Pilot

EPSoft Technologies, the creators behind the Intelligent Automation Platform (EZFlow), has announced the launch of its product update EZFlow A² - The Process Co-Pilot driven by Conversational AI and Generative AI.

EZFlow, the Intelligent Automation Platform, offers a comprehensive suite of automation tools for improving business process management. Natively developed, the Intelligent Automation Platform manages the full process automation lifecycle, from process mining to implementation through RPA development and ongoing management through orchestration.

At the heart of EZFlow A² is 'Ezi,' the Generative AI co-pilot, designed to make automation seamless and intuitive. No longer limited by complex interfaces or coding expertise, users can now effortlessly converse with 'Ezi' as it captures and understands their unique business processes.

By leveraging the power of natural language conversations, 'Ezi' eliminates barriers to automation adoption, making it accessible to everyone in the organization.

Among the standout features of 'Ezi' is its ability to analyze, design, and generate Robotic Process Automation (RPA) solutions in a fraction of the time it would traditionally take.

https://www.epsoftinc.com/

Esker automates Virtual Card Processing

Esker and Boost Payment Solutions are teaming up to transform virtual card processing for accounts receivable (AR) departments – eliminating tedious manual efforts and streamlining payment reconciliation.

Sending one-time-use virtual cards to suppliers is an increasingly popular payment method, but processing these card payments by hand can be burdensome for AR departments, requiring substantial manual intervention.

By harnessing Esker's automation technology with Boost Intercept - Boost's straight-through processing (STP) solution - businesses can now seamlessly integrate virtual card payments into their AR workflows, eliminating manual intervention, human errors and improving processing time and costs.

Since 2009, Boost has been reinventing how card payments are initiated, accepted and processed for companies worldwide. This partnership marks a milestone for both Boost and Esker in the AR space by offering organizations an innovative solution to streamline virtual card processing and unlock new levels of financial optimization.

"Virtual card payments are growing at a tremendous speed," said Steve Smith, U.S. Chief Operating Officer at Esker.

"We've seen a huge uptick in card issuance on the AP side and want to be a step ahead as it progresses to the receiving end. We are extremely excited about this new partnership with Boost, as it further solidifies our commitment to progress and meeting our customers' evolving needs for innovative and efficient payment solutions."

https://www.esker.com.au/

https://www.boostb2b.com/

Expert.ai Expands AI Capabilities

Expert.ai has announced enhanced features for its scalable hybrid AI platform, purpose-built to help organizations power business processes and applications relying on language data. The latest version of the platform includes security and infrastructure improvements as well as core technology enhancements designed to provide organizations with even more security and flexibility when creating or enhancing AI-enabled natural language (NL) solutions.

The exponential growth of language data within organizations is driving the need for advanced solutions to analyze business text, optimize manual tasks and accelerate intelligent process automation opportunities.

While large language models (LLMs) have put the spotlight on AI most recently, these are just one tool of many for creating language solutions. The ability to capture and process language data, integrate with third-party and internal applications, automate processes, as well as develop, deploy, manage and monitor your language solution is critical.

The expert.ai Platform combines different AI techniques (machine learning, deep learning, symbolic knowledge-based AI, and LLMs) to accurately understand and process text. As a result, organizations can accelerate decision-making and automate language intensive processes like claims validation, policy reviews, and risk assessment analysis; research drug discovery, clinical trials and regulatory report reviews; enrich news and making content recommendations; review contracts or improve customer experience interactions.

Enhanced expert.ai Platform features include:

Stronger detection for document formats and labels. The new platform release strengthens its Document Understanding capabilities for format detection, font recognition and extraction, and label reading (e.g., "table of contents" labels.)

Import taxonomies enablement. The new platform release streamlines the migration of existing taxonomy-related projects. The new functionality enables users to quickly import SKOS document properties, annotated taxonomies and use them within the platform.

Security Improvements. Continuing to add to the ISO/IEC 27001 and SOC 2 Type 2 compliance and security improvements, the expert.ai Platform updated its Kubernetes (or K8s) hardening procedures.

New analytics filters. By supporting the ability to filter annotation and extraction class data by false positive, false negative and true positive results, the expert.ai Platform accelerates the identification of different result types for a given extraction class, category, taxonomy node or concept.

https://www.expert.ai/

Unstructured Data security via LLMs

Israeli firm Flow Security has designed a data security platform powered by Large Language Models (LLMs). With a focus on unstructured data, this technology can identify over 150 distinct data types with claims of unprecedented accuracy.

In an age in which companies generate data at an unprecedented rate, being able to classify sensitive data automatically has never been more urgent. This challenge is especially critical when dealing with unstructured data (e.g. free text).

Until recently, unstructured data was classified through traditional Named Entity Recognition (NER) algorithms, such as LSTM. Although they got the job done, these algorithms could only recognize a small set of data classes, were limited in accuracy and struggled with context. Now all this is changing with LLMs.

Over the past few months, Large Language Models (LLMs) have taken the digital domain by storm. Powered by vast and diverse datasets, LLMs can mimic and produce text with an uncanny resemblance to humans. What sets these models apart isn't just their scale, but their natural ability to comprehend context, tone, and intent.

Unlike traditional NER algorithms, LLMs recognize a wide range of data types and catch context that other models might miss. In addition, because they are trained on an overwhelming amount of data, their accuracy levels can reach that of humans and beyond.

One of the biggest opportunities for LLMs to shine is unstructured data. Thanks to the capabilities mentioned above, LLMs can classify unstructured data with unmatched accuracy, flexibility, and scalability, leaving traditional methods far behind.

Flow has incorporated LLMs into its classification technology. Its latest offering is bringing about a revolution in the understanding and classification of unstructured data. Designed with a strong emphasis on unstructured formats, Flow's platform dives deep into free text and uncovers sensitive data. The engine identifies over 150 distinct data classes, including out-of-the-box classifications that align with industry benchmarks such as GDPR, HIPAA, CCPA, and PCI-DSS.

These can be further calibrated by users to suit their unique classification needs. Classification can be applied to anything from casual documents and detailed narratives to complex source code, audio files, images and videos (using OCR algorithms).

Flow's use of LLMs in data classification isn't just powerful, it's also extremely secure. The LLM-driven classification mechanism is located in the customer's environment, which means that sensitive data remains entirely on-premises, and is not shared externally.
https://www.flowsecurity.com

Generative AI platform that cuts down on AI hallucinations

Agent Copilot is a new conversational AI solution from Got It AI designed for customer service and sales operations with guard-railed generative AI. Designed to empower agents with quick and accurate answers from complex knowledge sources such as insurance plans, financial products or manufacturer catalogues, Agent Copilot uses TruthChecker AI, a feature designed to catch and avoid inaccuracies in responses generated by Large Language Models (LLMs).

Businesses can customize their Agent Copilot by choosing from a selection of LLMs including ChatGPT, GPT-4, LLaMA2, MosaicML, and FLAN-UL2. The choice of LLM can even be based on the business's specific knowledge base and the measured performance of the LLM against the documents in it.

Agent Copilot can be configured with a variety of data sources including PDFs, web pages, documents, and presentations, enabling support of full multi-turn dialogues against the compiled knowledge base. Finally, for organizations with data privacy concerns, enterprise specific fine-tuned LLMs can be installed on-premises.

Below are hallucination rates for an identical set of questions for the same set of documents for one of Got It AI's customers.

- OpenAI GPT-4, > 175 B, 8.39%
- OpenAI ChatGPT-3.5 Turbo, 175B or less, 13.99%
- Google Flan-UL2, 20B, 14.08%
- MosaicML, 30B, 30.07%
- Meta LLaMA-2, 13B, 36.76%
- Meta LLaMA-2, 70B, 25.45%
- Got It AI LLM, Less than 1B, 8.45%

It is due to become available in September 2023 with the following features:

Knowledge Base connectors to custom data sources and documents (structured and semi-structured) including PDFs, Slide decks and Web pages

Choice of LLMs: FLAN UL-2, LLaMA2, MosaicML, ChatGPT, GPT-4

TruthChecker AI fine-tuned for detecting hallucinations in multi-turn responses

Product UI or Microservice API for customer specific UIs

Fluid conversational dialogue with hallucination detection, mitigation & disambiguation

https://www.got-it.ai

Identify Archetypes for Data Discovery and Protection

Concentric AI, a vendor of intelligent AI-based solutions for autonomous data security posture management (DSPM), has announced archetype functionality for granularity and precision of data discovery and protection. Archetype in the context of data discovery, classification and risk remediation is a specific type of data or file that contains sensitive or confidential information, such as a contract in the legal industry, a tax form in finance services, or a workers' compensation claim in the insurance field.

As a result, updates to Concentric AI's Semantic Intelligence DSPM solution enable security teams to identify archetypes within their organizations and leverage new contextual understanding to identify sensitive data, monitor for risk, and protect data at a new level of granularity and precision that traditional methods simply can't match.

Concentric AI uniquely uses Large Language Models (LLMs) to understand the layers of information within each archetype and categorize them accordingly. This new way to perform data discovery, risk monitoring and protection that identifies the archetype of data instead of just where sensitive data exists significantly enhances organizations' ability to precisely perform risk assessments to identify data at-risk and employ strong data security measures.

By identifying and classifying sensitive information within each archetype, Concentric AI provides organizations with a comprehensive overview of their data landscape, highlighting potential areas of risk and ensuring that appropriate data protection measures can be put in place.

Concentric AI's DSPM solution scans organizations' data, detects sensitive or business critical content, identifies the most appropriate classification category, and automatically tags the data. Concentric AI uses artificial intelligence (AI) to improve discovery and classification accuracy and efficiency to avoid endless regex rules and inaccurate end user labeling.

In addition, Concentric AI can monitor and autonomously identify risk to financial and other data from inappropriate permissioning, wrong entitlements, risky sharing, and unauthorized access. It can automatically remediate permissions and sharing issues or leverage other security solutions and cloud APIs to quickly and continuously protect exposed data.

Concentric AI's Semantic Intelligence automates unstructured and structured data security using deep learning to categorize data, uncover business criticality and reduce risk. Its Risk Distance analysis technology uses the baseline security practices observed for each data category to spot security anomalies in individual files. It compares documents of the same type to identify risk from oversharing, third-party access, wrong location, or misclassification. Organizations benefit from the expertise of content owners without intrusive classification mandates, with no rules, regex, or policy maintenance needed.

http://www.concentric.ai/product

GLASS Studio Delivers Customized Data Discovery

Ground Labs has announced the release of GLASS Studio which simplifies the creation and deployment of custom data patterns for Enterprise Recon, Ground Labs' flagship data discovery and management solution. Using its guided visual builder and no-code interface, GLASS Studio empowers customers and partners to take advantage of Enterprise Recon's proprietary GLASS Technology. GLASS Technology enables the rapid, accurate discovery of custom and non-standard data types across on-premise and cloud-based environments and services.

Requiring no coding knowledge, GLASS Studio users can tailor their own data patterns from scratch or modify them from a library of pattern templates. These can be refined with a variety of context rules, checksum validations, boundary rules and exclude/require rules. With its instant test feature, GLASS Studio ensures accurate and error-free customization.

GLASS Studio unlocks the power of Enterprise Recon's customization features enabling even greater visibility and control of data across the enterprise, whether for compliance, digital transformation or other strategic purpose.

"The release of GLASS Studio marks a new stage for Ground Labs. We are giving customers control of how they search for their own data, allowing them to tailor their data discovery efforts to their own increasingly complex needs," says Don Kaye, COO and CCO of Ground Labs.

https://www.groundlabs.com/

Hyland content services updates

Hyland has launched its latest series of product enhancements and solutions, delivering a key new integration for Workday and a variety of other process-focused features – including for its Alfresco platform – that improve user and administrator experiences.

New innovations within the Hyland product portfolio include:

■**Alfresco platform:** The latest releases across the Alfresco platform equip desktop and mobile users to more rapidly access critical business content and make better business decisions.

Advancements include a more modern search experience platform-wide, as Elasticsearch now provides expanded support for languages, databases and Alfresco modules.

Alfresco Content Services workflow enhancements also make it easier than ever for customers to take advantage of content-centric workflows to act on critical content in the right context.

■**Alfresco Process Automation:** Administrators can streamline operations with key new efficiencies, including: the ability to effortlessly monitor process variables, and to complete process history and track task statuses more efficiently.

Additionally, the latest updates improve security and control over sensitive information with better user access controls, as well as more detailed activity tracking and process initiations.

■**Brainware Foundation 23.1:** In the latest release of Brainware for intelligent capture, administrators and end users have improved functionality for editing PDF documents, enhanced support with licensing and operating systems, and state-of-the-art authentication methods.

■**Hyland for Workday Extend:** Hyland's key new integration for Workday Extend provides comprehensive, in-context content management for core Workday applications.

This includes a more seamless experience with Workday Human Capital Management and Workday Financial Management, for simpler use with Workday Extend.

Additionally, new features allow the ability to link one document to multiple Workday entities and platforms to view it across all areas of the business.

■**Hyland AP Invoice Approval App:** The latest release allows users to find, edit and approve invoices more efficiently all while enjoying a more modern and personalized user experience.

https://www.hyland.com/en

iManage adds new Legal AI Engine

iManage has launched a new AI engine built natively into its knowledge work cloud platform. The core of the new iManage AI solution is a document classification and enrichment engine that improves knowledge search and content workflows on the iManage platform.

iManage AI builds on models trained on tens of thousands of legal-specific documents to automatically analyze documents and extract key data points, such as Jurisdiction, Parties, or Dates, then save that information with the document.

As a result, users are able to pinpoint very specific pieces of information and apply them to their work processes to be more productive and efficient.

iManage has focused its development effort on building tools for curating the content that the AI engine can see, so that responses are relevant, accurate, and built on the best work product available at the organization. The AI engine is trained on high-quality and purpose-built legal content to deliver the level of accuracy and reliability required for legal professionals.

The solution also includes robust governance tools to specifically control the engine's access to content so that the risk of breaching client confidentiality is mitigated. Additionally, the AI engine only analyzes documents located in the customer's own data resource, ensuring complete confidentiality and compliance with ethical and regulatory obligations.

"We believe that AI has tremendous potential to improve the efficiency and productivity of knowledge workers, making the work more satisfying by removing the tasks that humans find mundane and enabling them to focus on higher-value activities that are more interesting to them," said Neil Araujo, CEO, iManage.

"As stewards of our customer's data, we firmly believe that knowledge curation and quality data sets are critical to the effective and ethical us of AI. Achieving business benefits requires the right partner, one with strong experience with AI technologies, deep understanding of the risks involved, and expertise on how to resolve them.

"iManage has been working with this technology for leading global customers for several years to fine-tune its effectiveness across multiple applications, and we are excited to introduce these capabilities to the broader market."

iManage is actively working with customers as part of the company's Early Access Program to validate the results they see with generative AI, and to ensure the approach includes the right security and governance protections.

https://imanage.com/

TotalAgility gains Generative AI

A new Azure OpenAI connector for TotalAgility has been released on the Kofax Marketplace. This Connector uses Azure OpenAI, the Microsoft-hosted version of GPT - the engine behind OpenAI ChatGPT.

TotalAgility workflows can now be extended with several core Generative AI (GAI) capabilities:

■Deep Understanding: Analyze unstructured text to discern meaning, emotion, and purpose.

■Summarization: Efficiently condense vast amounts of content, aiding in quicker decision-making.

■Tailored Responses: Auto creation of impactful replies to user queries and customer touchpoints within a TotalAgility process.

The Generative AI Assistant empowers developers in rapidly generating processes, integrating back-end systems, creating user interfaces, and providing best-practice guidance throughout the development phase.

Fusing TotalAgility with cutting-edge language models, developers will be able to simply prompt for the desired information from a document and watch as the system intelligently retrieves it. This aims to redefine intelligent document processing extraction and provide a faster time to value.

This connector is available at no extra cost to TotalAgility users. For an overview and to download the Azure OpenAI connector for TotalAgility on the Kofax Marketplace, visit HERE

Iron Mountain & telco blockchain alliance

South Korean telecommunications giant KT has entered into a strategic partnership with Iron Mountain to leverage blockchain technology in expanding the certified electronic document ecosystem.

Under this collaboration, KT and Iron Mountain will utilize the Korean telecom firm's blockchain-based electronic document platform to digitize Iron Mountain's physical documents. The partnership extends beyond digitization, with plans to explore diverse business prospects across various markets.

KT has been operating the KT Paperless platform since 2020, providing services such as contract writing, registered document delivery, and document storage. SMEs or small business owners can use electronic document services such as electronic contracts and electronic registration for a fixed monthly fee.

Both companies have identified opportunities in the Asia-Pacific market, a region where conventional paper documentation remains high.

Smart Summaries for Lawyers via AI

Legal technology specialist Litera has announced a new generative AI (GenAI) feature in Kira, Litera's AI-powered contract review and analysis software.

Litera is combining Kira's machine learning, an application of artificial intelligence, with GenAI to further accelerate and improve workflows for the setup, review, analysis, and synthesis phases of due diligence and other contract reviews.

"With products like Kira, Clocktimizer, and Litera Check, Litera has been at the forefront of integrating AI into legal technology for over a decade," said Litera CEO Sheryl Hoskins. "Bringing together Kira's tried and tested, lawyer-trained machine learning assets with the power of generative AI, represents the next step in the evolution of technology-enabled legal services, which will unlock more efficiency and amplify impact for our customers."

While AI has transformed workflows within the legal profession, analyzing AI-extracted information to produce reports, interpret the language, and determine the legal implications remains an intensive manual process. With Kira Smart Summaries, legal teams will see enhanced accuracy and speed in synthesizing content in contracts and other documents, enabling them to deliver recommendations and strategic advice to their clients faster. Kira Smart Summaries will be available to customers later this month.

Over the upcoming year, legal teams will be able to use Kira to instantly get actionable insights from their contracts and other documents using natural language questions and requests, and seamlessly set up projects. Combining Kira's machine learning and world-class workflows with GenAI will make it even easier to collaborate, extract granular data points, and produce work product and client deliverables.

AI-powered machine learning models with over 1,400 smart fields addressing over 40 substantive areas. This legal AI technology automatically identifies and extracts common clauses and data points from contracts and other documents, while providing highly adaptive workflows.

Trained by Litera's in-house Legal Knowledge Engineering team of experienced attorneys on over one million contracts and 500,000 examples, Kira helps the world's largest professional service firms and corporations quickly uncover relevant information from their contracts and documents and contextualize this information to support data-driven decision-making.

With Litera, law firms can provide high-quality work faster, freeing up lawyers to focus on amplifying their impact for clients and leveraging their unique experience. To sign up for early access to Litera's AI beta program, click here.