idm.
information & data manager
AUGUST-SEPTEMBER 2023

Archives under threat from 'Digital Deluge'

Why Microsoft Teams Archiving is More than Capturing Chat

The role of AI in information management

Six ChatGPT Risks Legal and Compliance Leaders Must Evaluate

Robodebt report highlights automation risk

Australia Races to Battle Identity Crime by 2030

Liverpool City Cloud records transformation

Liverpool City Council in Western Sydney has signed a 5-year contract with Kapish to transform the delivery of Records Compliance, moving to Kapish Content Manager Cloud. Kapish has been a long-term Content Manager partner with Liverpool, providing value adding services such integration with the Property & Ratings System (Pathway), business system integrations, Kapish Commercial off the Shelf (COTS) Products as well as Content Manager Upgrades.

As part of a broader transformation initiative, Council is Transitioning to cloud for many of its corporate systems to ensure a secure, interoperable suite of business systems.

The move to Kapish Content Manager Cloud ensures that Council can capitalise on significant regulatory, and costs benefits when compared to the legacy on-premise model. The Kapish cloud platform also minimises the change impacts to the business while ensuring many of the business customisations will continue to function.

Liverpool City Council is now the sixth Australian local government entity that is undertaking the cloud records transformation journey (joining Campbelltown, Waverley, Monash, Whitehorse & Brisbane) with Kapish Content Manager Cloud.

UpFlow takes on Ephesoft IDP in APAC

Australian solution provider UpFlow has obtained the distribution rights for Ephesoft in the Asia Pacific region. Ephesoft, a Kofax company, provides a range of Intelligent Document Processing (IDP) solutions offered in the cloud, hybrid or on-premise.

Ephesoft provides businesses with the tools to streamline and automate their document workflows effectively. These include AI and machine learning capture technologies that can easily connect to any existing application.

UpFlow, a subsidiary of Ellby Group, offers a range of advanced document capture and data analytics solutions.

"We are thrilled to announce that we have secured the distribution rights for Ephesoft in the Asia Pacific region," said Lee Green, Sales Director at UpFlow.

"By partnering with Ephesoft, a global leader in IDP, we are poised to revolutionise the way businesses across Asia Pacific handle their document-centric processes."

Ephesoft has more than 1,000 existing customers in 53 countries. Its leading IDP platform, Ephesoft Transact, 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.

"Together, we will unlock new levels of efficiency, accuracy, and insight, enabling our clients to stay ahead in today's rapidly evolving digital landscape," said Steven Chenery, CEO at UpFlow.

"We look forward to delivering unparalleled value and driving transformative outcomes for our customers."

According to recent study by Research Nester, the intelligent document processing market size is anticipated to surpass $US122 billion by 2035 and is projected to expand at CAGR of over 40.5% from 2023 to 2035.

"Organizations that continue to embrace digital transformation projects in the coming years will position themselves for tremendous growth. We're excited to support businesses alongside Steven and his team throughout the Asia Pacific region ready to adopt new technologies and achieve greater efficiencies," said Gaetan Spake, Vice President, Channel Sales at Kofax.

https://upflow.solutions

ZircoDATA buys Shred It

ZircoDATA is acquiring Shred-it, one of Australia and Singapore's preeminent providers of secure document shredding, secure bin services and IT Asset disposal.

This acquisition will integrate shred services, a core part of records management, with ZircoDATA's existing offerings.

"This acquisition will be a significant turning point for our businesses and a strategic advantage in the competitive and ever-evolving records and information management industry we operate in," said ZircoDATA Chief Executive Officer, Jacqueline Leeds.

As part of the transition, the Shred-it brand will be phased out in Australia and Singapore in favour of the ZircoDATA brand. The acquisition will also extend ZircoDATA's service locations to include Rydalmere (Sydney), Banyo (Brisbane), Footscray (Melbourne), South Australia, Canberra and Singapore.

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

eVoting not on the agenda for AEC

Voting for the Australian Senate will remain a pencil and paper process for some years to come, according to a call for tender just issued by the Australian Electoral Commission (AEC).

A tender for the Digitisation of Senate Ballot Papers for the 2027/2028 federal election estimates that 17.2 million will need to be scanned and captured. This figure closely matches the size of the Australian electoral roll as listed on the AEC Web site (17,446,467).

FUJIFILM Data Management Solutions has been the AEC's data capture provider since 2016 and will complete data capture from Senate ballot papers for the next federal election in 2024/2025 after the AEC exercised an option on the existing work order.

Senate ballot papers are scanned and OCR is used to capture voter preferences. Once captured, these preferences are then verified by a human operator.

However, votes in the lower house are still counted manually.

"The AEC have never conducted data capture for House of Representatives ballot papers," said a spokesperson.

One area where the AEC has been moving towards digital processes is in the capture of electronic certified lists (ECL) that record the identities of voters that show up to vote. These have traditionally been paper lists that are marked off with pencil by polling booth officers and subsequently scanned and OCRd. For the 2022 Federal Election more than 5 million voters were marked off on ECLs, including the growing number casting prepoll votes ahead of election day.

Paper certified lists were not deployed to pre-poll voting centres or mobile teams for the 2022 federal election, and voters were marked off using an electronic certified list at those locations. The AEC deployed 5,800 electronic certified lists (ECLs) for the 2022 federal election, an increase compared with the 2019 federal election, where more than 4500 ECLs and more than 2700 printers were deployed.

There were 7,587 polling day and pre-poll voting locations across Australia for the 2022 election, with 657 polling places and mobile teams used Electronic Certified Lists (ECLs). For the 2024/25 federal election the AEC expects to deploy up to 10,000 ECLs.

In 2020 the AEC issued a request for information investigating the possibility of operating its electronic certified list (ECL) system at "100 percent of polling places" in the future.

An AEC spokesperson said no decision has been made yet whether to proceed with this option.

"The AEC is currently looking at innovative solutions with the capability to scale up significantly beyond 2024/25. Given the scale of a federal election, this is a significant task and the steps taken to this point are iterative advancements."

AYR and CiGen Bring Advanced IDP to APAC

AYR is extending the reach of its flagship IDP platform, SingularityAI, across Australia, New Zealand (ANZ) and Southeast Asia in partnership with Australian AI Automation consulting firm CiGen.

CiGen will serve as a Strategic Platinum Reseller of SingularityAI, which utilizes proprietary computer vision, natural language processing, OCR and machine learning to streamline document processing, automate data extraction, and improve overall operational efficiency.

"We are thrilled to partner with CiGen to expand the availability of SingularityAI in ANZ and Southeast Asia," said Scott Lee, CRO of AYR.

"CiGen's expertise in AI-driven intelligent automation and their commitment to delivering innovative solutions align perfectly with our mission to revolutionize document processing by solving unstructured data. Together, we will enable businesses in the region to harness the power of advanced IDP technology and accelerate their digital transformation initiatives."

Leigh Pullen, CEO of CiGen, said, "This partnership strengthens our commitment to providing transformative technology solutions that drive efficiency and enable organizations to unlock the true potential of their data."

Desktop Imaging teams up with ABBYY

New Zealand digitisation and workflow systems provider Desktop Imaging has announced a partnership with ABBYY. The collaboration aims to redefine document management and enhance the efficiency of business in Aotearoa New Zealand.

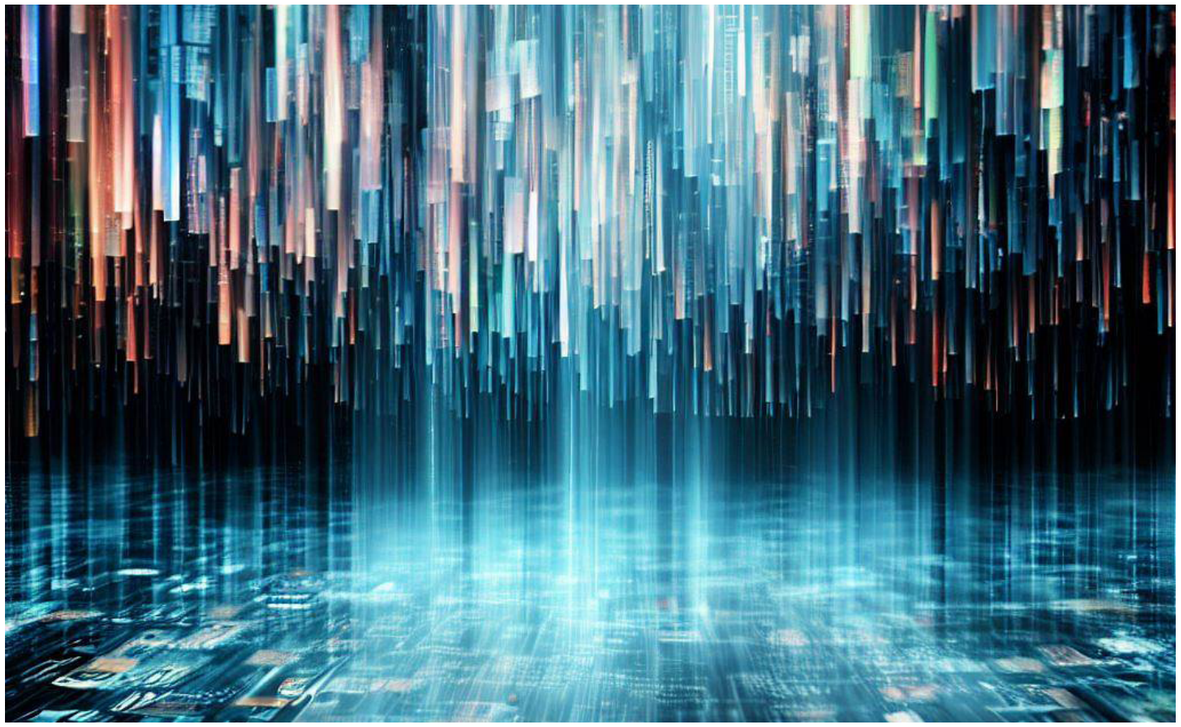
By combining their respective expertise and technologies, ABBYY and Desktop Imaging intend to simplify document-centric processes, automate data extraction, and streamline information management.

The partnership also signified a shared commitment to unlocking the potential of unstructured data.

"We are thrilled to partner with ABBYY in our quest to revolutionise document management solutions," Malcolm Davidson, general manager of desktop imaging told New Zealand Reseller News.

"We aim to empower organisations to achieve unprecedented levels of automation, productivity, and data accuracy. Together, we are poised to reshape the way businesses capture, process, and leverage information."

ABBYY offers artificial intelligence technologies including optical character recognition, natural language processing and machine learning, Intelligent Document Processing (IDP) and process discovery & mining.



National Archives under threat from 'Digital Deluge'

Australia's national strategy to identify and retain essential government records is buckling under the complexity and cost of dealing with an exponential growth in data, according to a new report from the Australian National Audit Office (ANAO).

This audit examined the effectiveness of the National Archives of Australia's implementation of the 2022 Building Trust policy as well as management of information assets (records, information and data) at two selected agencies, the Department of Prime Minister and Cabinet (PM&C) and Australian National Maritime Museum (ANMM).

It gave the NAA and PM&C a scorecard of "partly effective" while the ANMM was found to have ineffective management of information systems and a lack of appropriate governance.

Before a record can be transferred to the NAA, federal agencies must first appraise the record against the relevant records authority to decide if it should be transferred or destroyed. This process is known as 'sentencing'.

The ANAO Report found that "Check-up survey data indicates a rapid increase in digital information and records held in entities awaiting sentencing, known as the 'digital deluge'."

"Over time, this trend may represent a risk to the comprehensiveness of the National Archives."

" - the volume of digital records held by federal agencies has grown on average by 328 per cent a year, from 51 Terabytes in 2013, to over 314,000 Terabytes in 2022; and

"- the proportion of records held by entities reported as 'unsentenced' rose from 69 percent in 2019 to around 93 per cent in 2022."

The ANAO found that while this trend may represent a risk to the comprehensiveness of the National Archives, the National Archives' risk register "does not identify a risk for the lack of sentencing of records by entities."

The NAA's CheckUp Surveys are submitted annually by federal government agencies and rely on data these agencies have chosen to volunteer.

The ANAO report found that "Assurance and verification arrangements over the accuracy of entity reporting have not been changed since the National Archives agreed to the previous Auditor-General recommendation to do so and remain a risk."

The report found deficiencies in the NAA's efforts to oversee the management of information and records at federal government agencies, using information obtained by volunteered reports.

"There is little verification of entity reports and the audit found errors in these reports. This reduces the reliability of the National Archives' assessment of progress and reporting to Australian Government ministers and other stakeholders.

"There is no performance measure in place to monitor entity compliance with a key, mandatory policy and legislative requirement for entities to transfer 'retain

(Continued Over)

as national archives' information assets as soon as practicable, or within 15 years of creation, to the care of the National Archives and there is evidence that this requirement is not being met."

From 2019 to 2021, the NAA developed a policy known as *Building trust in the public record: managing information and data for government and community*.

As part of developing the Building Trust policy the NAA identified a series of risks. However, the ANAO report points out "The risk register does not include a risk that entities' reporting may be inaccurate."

It criticised the unwillingness of the NAA to utilise information that would enable it to identify agencies that were potentially not complying with obligations under the Archives Act.

"The National Archives has no process to engage and follow up entities that are not transferring RNA records in accordance with the requirements of the Archives Act and the actions and requirements of the Building Trust policy.

"There is a risk that RNA records may be inadvertently destroyed, corrupted or lost in the absence of actions on the part of entities, with the support of the National Archives"

(RNA records are categories of records that have been identified in a records authority and are no longer used on a regular basis.)

The NAA responded that it will look at "better ways to systematically collate and analyse information to efficiently indicate in an entity is at-risk to ensure early engagement."

PM&C

Check Up reports provided by the Department of Prime Minister and Cabinet (PM&C) were found to include inaccuracies and the department had no electronic management systems for documents classified above 'protected'.

"Shared drives remain in use with some controls. The effectiveness of the controls is not monitored or assessed. The main record-keeping system (ShareHub) has recently been upgraded to enable better appraisal and sentencing of records."

"In January 2023, PM&C implemented a new record-keeping solution, 'Records365'. As at April 2023 over 430,000 ShareHub records and files had been ingested into R365 and 200,000 of these had been sentenced using the system. Approximately 2.6 million records are currently held in ShareHub which are planned to be progressively ingested and sentenced during 2023.

"PM&C policy on managing digitally ... requires that any records classified as confidential, Secret and Top Secret must be retained in hard-copy form. This is because 'there are currently no electronic [information management] systems available within PM&C to manage material classified above Protected.'

"Partly due to its inability to sentence ShareHub records, PM&C has transferred only one digital asset to the National Archives since 2019. PM&C considers the lack of transfers is mainly due to National Archives using an unclassified network to manage the transfers and as a result only unclassified files being available for transfer; and that a transfer 'freeze' was in place.

Nine instances of paper files and one of '3 Dimensional records' have also been transferred from PM&C to the National Archives over this time period."

Australian National Maritime Museum

The ANAO report found that "The Australian National Maritime Museum's (ANMM's) management of information systems is not effective, lacking appropriate governance and support for staff. It has not transferred any records to the National Archives since the ANMM's establishment in 1991, and in this regard is non-compliant with the Archives Act 1983 (Archives Act).

"The ANMM does not have enterprise-wide structures, committees, or accountabilities for information management. Risks to information assets are not identified and key policy documents are in draft or absent. There is insufficient guidance and support for ANMM staff in the use of the document management system.

"Training and guidance in the use of the ANMM's electronic document management system is insufficient. The sentencing, disposal and transfer of information to the National Archives is not compliant with the requirements of the Archives Act. There is frequent use of shared drives to hold records. The ANMM became aware that no records had ever been transferred in July 2022 when the records manager contacted the National Archives and asked for details of past transfers. The National Archives advised that 'there have been no transfers of any format to the National Archives from the Australian National Maritime Museum'.

The ANMM's most recent records manager commenced in June 2022 and left in December 2022

"The ANMM's Check-up survey response accurately reported that it had not transferred records to the National Archives. Several other parts of the ANMM's response regarding information governance risk management were not accurate."

The ANMM responded "it is aware that it has not been able to prioritise information management in the last few years" and effectively blamed this on limited funding.

"We note the report identified our Collection Management System as well managed. Maintaining this system and ensuring the veracity of the information stored in this system remains a key focus for the Museum. Policies and procedures are being updated and system upgrades are planned as resources allow. The ANMM is committed to improving its information management systems and has taken actions to improve information management practice within available resourcing."

The agency has committed to "continue working to improve governance and reporting arrangements for information management and will endeavour to improve documentation of its Check-up survey response."

ELO, the ANMM's document management system, had not been updated since 2018 and there was no support agreement in place with the service provider.

"The absence of such an agreement limited the ability of ANMM staff to receive training in ELO or manage the system. Staff were unable to delete records or containers created in error potentially affecting data reliability and accessibility. In November 2022, the ANMM and the service provider established a support agreement. "

The ANMM has committed to upgrading both the ELO EDRMS and its collection management system (TMS).

The full report is available HERE

Australia Races to Battle Identity Crime by 2030

Guidelines will be updated, annual reports written, and detailed plans definitely developed under a new National Strategy for Identity Resilience signed off by the Minister for Finance and Australia's state and territory Data and Digital Ministers.

The 2023 National Strategy for Identity Resilience, which replaces the 2012 National Identity Security Strategy, promises to "help to make Australia the most cyber secure nation by 2030".

In pursuit of this seven-year timetable to protect the nation against Identity theft, described as a key enabler of terrorism and of serious and organised crime, the latter of which costs the Australian economy over $A60 billion annually, a series of initiatives will be attempted over the next 5 years.

In the first 12 months the strategy aims to roll out education and awareness programs, standardise Proofing Guidelines across Commonwealth, state and territory digital ID systems, and establish a national Centre of Excellence for data breaches.

Over the next 3 years, the Labor government will seek to improve the Credential Protection Register it established in October 2022 to prevent Identity Matching Services verifying a compromised credential that has already been listed on the Register.

"When a credential is discovered to have been compromised it can take a long time to remediate. During this time, criminals can continue to misuse the credential."

The aim is by 2026 to eventually allow individuals to have better control of their credentials, and also to improve the sophistication of the Register.

There are also plans to develop a mobile phone trust score system to mitigate the use of multifactor authentication for fraud.

"A 'Mobile phone trust score' system would allow telecommunication providers to assign trust scores to mobile phone numbers based on risk factors such as recent sim swaps, tenure of phone plan and virtual private numbers."

The Mobile phone trust score system could possibly be in place before 2027.

A series of longer-term initiatives have also been announced, estimated to take 3-5 years to implement), although this will require the re-election of the current Labor government.

These include:

- Enabling Digital Credentials (for example Working with Children Checks or mobile driver licences) to be issued through Digital wallets;
- Allowing Australians the ability to contact to one government organisation to recover their identity; and
- Improving links between identity records such as birth certificates/ immigration records with change of identity (e.g. change of name) processes in other jurisdictions.

According to the National Strategy for Identity Resilience, "In implementing this strategy, effectiveness will be assessed by progress made towards implementation of the initiatives, and the effectiveness of these outcomes.

"An annual report will be provided to the Data and Digital Ministers Meetings on the effectiveness of the Strategy, associated policy and legislation, and follow-on actions required to ensure that Australians' identities are resilient."

Unmasking Business Email Compromise: Understanding, Identification, and Prevention

Business Email Compromise (BEC) represents one of the most insidious threats in the modern digital landscape, causing billions of dollars in losses worldwide. Instead of relying on brute force or sophisticated hacking techniques, cybercriminals conducting BEC attacks relies on deception, manipulation, and exploiting human vulnerabilities.

In many cases, companies that conduct wire transfers with foreign suppliers or businesses that regularly perform online transactions are a good target for this type of attack. BEC attacks are gaining traction.

In 2022 BEC increased by more than 81%, according to Abnormal Security, resulting in significant financial losses for organizations across different industries.

At its core, BEC involves these entities, the cybercriminals, and the impersonating of company executives, employees, or business partners. Typically this attack is executed through email when the victim is tricked into sharing sensitive information, IP, or wire money with the attacker without noticing that the person on the other side of the mail is not who he thinks it is.

BEC is a form of phishing attack where the attacker seeks to gain trust by masquerading as a legitimate entity. These scams are particularly effective as they exploit human psychology and organizational processes rather than depending on technological vulnerabilities (This is a subject for a different article).

As such, hackers bypass traditional security measures and catch businesses off-guard, resulting in potentially significant reputational and financial damage.

Business Email Compromise Scenarios

To understand the workings of BEC better, we put together this made-up scenario:

An established organization, XYZ Corp, deals with multiple suppliers globally, including raw materials suppliers, financial suppliers, marketing, and business partners.

One of the organization's accounting department team members receives an email from what seems to be one of their suppliers.

The email contains an invoice for a recent delivery but notes that their banking details have changed due to internal restructuring, and future payments should be sent to the new account.

The email appears legitimate: the sender's email ID closely resembles the supplier's, the email content maintains the supplier's typical tone, the invoice looks just like previous ones, and the request seems reasonable.

Any organization's CEO or CFO would expect that employee to open the email and complete the work to maintain a good relationship with the supplier and do their job.

The employee, therefore, processes the payment to the new bank account.

A few weeks later, the real supplier contacts XYZ Corp for payment, at which point they discover that they've been a victim of a Business Email Compromise.

The email had been sent by a cybercriminal who had carefully studied the organization and its suppliers, then convincingly impersonated the supplier to redirect the payment to his account.

At this point, only a few post-mortem actions can be done to learn and analyze what happened. But it's most likely that the money wired to the hacker will not be paid back to XYZ Corp.

This case is 100% fiction, but dozens of similar topics are happening daily around the globe.

So, what you can and should do to prevent things like this from happening to you?

Securing Your Organization from Business Email Compromise

Preventing BEC, particularly in the context of supply chain management, requires a mix of technical, organizational, and procedural safeguards. Here are five key steps an organization should take with its suppliers to prevent these types of cybersecurity issues:

- **Supplier Verification Process:** Establish a robust process for verifying changes in the payment details of suppliers, for example. This could include out-of-band communication, like a phone call to a pre-established number, rather than relying solely on email confirmation. In sensitive cases that deal with money wiring or other sharing of sensitive information, have another layer of authentication to be sure you are speaking with the right person.
- **Employee Training and Awareness:** Regularly educate employees about the threat of BEC and how to spot suspicious emails. This should cover aspects like scrutinizing email addresses for subtle changes, checking for poor grammar or unusual language, and understanding that unusual requests for payment changes could be signs of a scam.
- **Email Security Measures:** Implement advanced email security measures, including flagging emails from outside the organization that appears similar to internal email addresses and setting up system alerts for emails with extensions similar to company email. Here is a list of Email Security Tools that should detect messages with malicious content and steal confidential data.
- **Frequent Communication with Suppliers:** Regular communication with suppliers can help build a familiarity that makes it easier to detect when something is off. Additionally, inform suppliers about your organization's policies, such as not making payment changes based solely on email communication.
- **Incident Response Plan:** Have a detailed incident response plan in place and ensure your suppliers are aware of it. In the event of a suspected BEC attempt, clear steps should be taken to isolate the threat, prevent damage, and report the issue to the necessary parties.

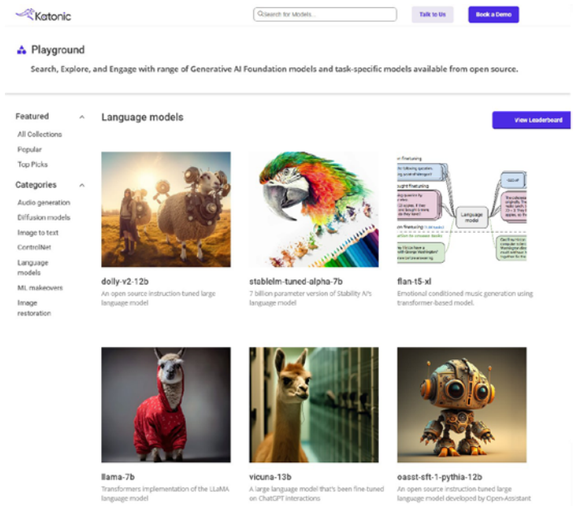
Business Email Compromise (BEC) is a cybercrime that capitalizes heavily on human vulnerabilities, also known as the 'human element'. It manipulates the psychological tendencies of trust, authority, and the natural inclination to act promptly when tasks are assigned, especially in a business setting.

Here's how its done in some cases:

- **Trust and Familiarity:** BEC commonly involves cybercriminals impersonating colleagues, superiors, or known business contacts. By appearing to be someone the victim knows and believes, the scam is more likely to succeed.
- **Authority:** BEC scams often exploit the power dynamics in a company. When a request appears to come from a high-ranking executive or a crucial business partner, employees might feel pressure to comply quickly without questioning the request's legitimacy. This is particularly the case if the request seems urgent or the executive is known to be strict or demanding.
- **Urgency and Fear:** Many BEC scams create a sense of urgency or impending consequences. For instance, a false email from a CEO might insist on immediate payment to secure a vital business deal. Fear of missing out on an opportunity or causing a business problem can lead to impulsive actions.
- **Social Engineering:** BEC cybercriminals often perform good research on the organization before executing the attack. The use of phishing to gather information about the victim, the organizational structure, and the relationships between different parties. This information enables them to craft convincing emails that mirror the style, tone, and typical requests the victim expects to see, making the scam hard to spot. With the increasing use of machine learning tools and AI like ChatGPT, crafting a convincing email becomes very simple.
- **Confirmation Bias**: Once trust has been established, people tend to interpret subsequent information in a way that confirms their preconceptions. For example, once employees believe they're interacting with their CEO or supplier, they will likely interpret all further communication with that assumption, making it harder to spot inconsistencies.

Originally published HERE by Rescana, an Israeli company that has developed a new personalized artificial intelligence tool to help its clients detect cybersecurity risks. It uses AI and natural language processing (NLP) to let users create dashboards, reports, and alerts that are tailored to their individual needs.

Katonic.ai unveils AI Playground



Australian firm Katonic.ai is looking to capitalise on the surge in interest in Generative AI, offering a range of different options to integrate the technology with corporate applications.

The company has delivered a portal that provides an opportunity to test a large number of open source large language models (LLMs), with more than 50 to choose from at https://playground.katonic.ai/

One of the first free tools it has made available is a chatbot that can be implemented on your own Web site or intranet, although the free version only scrapes the home page, with additional pages able to be added individually.

A Search tool is promised to be next to be released offering the capacity to build a Semantic Search engine powered by LLMs.

Katonics.ai CEO Prem Naraindas said "We predict that most organisations will begin with experimentation, then fine tuning a model and then eventually building their own. We can go with them on that journey."

Naraindas suggests there are a series of options to implement Generative AI, beginning with simply utilising the off-the-shelf tools leveraging available LLMs. There are various levels of customisation that can be applied to these tools by building content restrictions, using database lookups and fine tuning to tailor LLMs to an organisation's needs.

Many companies have banned ChatGPT over concerns that proprietary or sensitive company information given to the AI could be unintentionally shared with other users.

The most expensive and complicated model is to build your own application and train it from scratch with your own data.

Katonic.ai offers a MLOps (Machine Learning Operations) platform that enables the implementation of AI capabilities simar to ChatGPT but based on an organisation's own data.

Although the company warns that this can be a "Very expensive endeavour with high risks [and needs] cross-domain knowledge spanning from NLP/ML, subject matter expertise, software and hardware expertise.

"It is less efficient than the Customise option as this leverages existing LLMs, learning from an entire internet's worth of data and can provide a solid starting point."

Katonic.ai has teamed with solution provider Collabera Digital to establish Generative AI labs in key cities in APAC.

"We are very excited about this partnership with Collabera Digital," said Naraindas. "By combining our expertise in AI and Collabera Digital's network and reach, we can make it easier for businesses to take advantage of generative AI capabilities quickly, securely, and cost-effectively."

The partnership aims to fine-tune Generative AI models and install them directly on the organization's infrastructure.

"Generative AI could automate or augment around 65% of tasks across industries, enhancing efficiency, accuracy, and reducing costs. We are delighted to partner with Katonic.ai to offer these upgrades to our clients in APAC," said Anil Snehi, Executive Vice President & Regional Head of APAC, Collabera Digital.

Cyber attacks double between 2020 and 2022

More than two in 10 Australian businesses experienced a cyber security attack during the 2021-22 financial year, compared to almost one in 10 in 2019-20, according to new data released by the Australian Bureau of Statistics (ABS).

Robert Ewing, head of ABS business statistics, said: "Today's Characteristics of Australian Business data release is important because it gives governments and researchers information about the prevalence, impacts and nature of cyber attacks. This helps them understand who they need to support and what strategies they need to use."

The types of cyber attacks included, scams or fraud (16 per cent), malicious software infecting computers (5 per cent) and unauthorised access or use (3 per cent).

The latest figures also show how cyber attacks impacted businesses. In 2021-22 just over half of those that experienced a cyber attack were negatively impacted, compared to more than 80 per cent of businesses in 2019-20.

"In 2021-22, 34 per cent of businesses reported loss of time in managing cyber security attacks, 18 per cent reported downtime of service, while 17 per cent reported a loss of staff productivity," Mr Ewing said.

For the first time, all businesses were asked about the types of cyber security measures they had in place, and seven in 10 (70 per cent) reported some form of protection measure.

"Over 60 per cent of businesses reported regular updates to virus protection software. Around 37 per cent of businesses regularly backed up operations-critical data, while 20 per cent had identity access management and 13 per cent gave staff cyber security awareness training," Mr Ewing said.

Robodebt report highlights automation risk

A national body to monitor and audit automated decision-making in government has been recommended by the Royal Commission into the Robodebt Scheme. The findings of the Royal Commission, which run to over 1000 pages, include major criticisms of the scheme and 57 recommendations for the government and the public sector.

"The Commonwealth should consider legislative reform to introduce a consistent legal framework in which automation in government services can operate," the report concludes.

"The automation used in [Robodebt] at its outset, removing the human element, was a key factor in the harm it did. [Robodebt] serves as an example of what can go wrong when adequate care and skill are not employed in the design of a project; where frameworks for design are missing or not followed; where concerns are suppressed; and where the ramifications of the use of the technology are ignored."

In 2015 the Government introduced automated systems that averaged a person's yearly income and applied it against their fortnightly payments from Centrelink, generating many incorrect debt notices until it was scrapped in May 2020. The scheme led to a class action lawsuit, and subsequent Royal Commission.

"While Robodebt was not technically an AI system, the Chapter 17 recommendations may still be relevant to the Australian government's broader (and ongoing) public consultation into AI regulation," notes Herbert Smith Freehills lawyer Raymond Sun.

"There should have been a human in the loop" was basically the key message from the Report."

The Royal Commission has recommended that "The Commonwealth should consider legislative reform to introduce a consistent legal framework in which automation in government services can operate.

"Where automated decision-making is implemented:

there should be a clear path for those affected by decisions to seek review departmental websites should contain information advising that automated decision-making is used and explaining in plain language how the process works business rules and algorithms should be made available, to enable independent expert scrutiny."

The Robodebt scheme required data to be transferred from the Department of Human Services to the Australian Taxation Office and then back again.

For each year the scheme operated from 2015 to 2019, DHS created a file that contained details of all DHS recipients who, in a specified year, had received a welfare payment, had an outstanding debt to DHS, or were the partner of a recipient that met one of those two criteria.

The file was provided to the ATO, which would then match each DHS recipient with their corresponding PAYG data held by the ATO. The matched records were then returned to DHS.

Dr Elea Wurth, a partner from Deloitte Risk Advisory, was engaged by the Royal Commission to examine the data-matching process.

Dr Wurth reported that there was a lack of proper governance, controls and risk management measures in place under the Scheme.

The ATO argued that its use of the data collected from DHS, the matching and disclosure of matched data back to DHS under the Scheme were all lawful because of general exceptions provided under the Taxation Administration Act.

However, the Royal Commission had doubts as to the correctness of that proposition.

" ... the Commission considers that there is a serious question as to whether information was lawfully disclosed by the ATO to DHS for the purpose of data matching under the Scheme," the report notes.

It recommends that "The Commonwealth should seek legal advice on the end-to-end data exchange processes which are currently operating between Services Australia and the ATO to ensure they are lawful."

Dr Wurth told the Commission that "automation has the potential to increase productivity, efficiency, accuracy, and the cost-effectiveness of service delivery. A trustworthy automated system is a system containing automation that is ethical, lawful and technically robust, coupled with good governance and risk management. To achieve trustworthiness, the system must be designed with human agency at its centre."

The Royal Commission found that "To date, there has been inconsistency in the legal status of automated decision making in Australian government agencies. Numerous Commonwealth laws have been amended to establish a basis for automated decision making, but these amendments have been piecemeal, across a wide body of legislation, and without the necessary further amendments establishing standards for which decisions should be automated and which should not; and appropriately designed systems for transparency, review and appeal."

"Section 23 of New Zealand's Official Information Act 1982 provides a person with a right of access to reasons for a decision made by a public service agency or Minister, including a written statement of the findings on material issues of fact; a reference to the information on which the findings were based; and the reasons for the decision or recommendation.132 The introduction of a legal "right to an explanation" in Australian law, in similar terms to s 23 of the Official Information Act 1982 (NZ), could facilitate the creation of a legislative requirement to design explainable systems."

Former Department of Human Services (DHS) Secretary Kathyrn Campbell was found to have "been responsible for a department that had established, implemented and maintained an unlawful program".

Royal Commissioner Catherine Holmes accused Campbell of knowing that legislation would need to change if the policy was going to introduce income averaging and not doing anything about it, and also noted that a Centrelink staffer had tried to warn her of the issues being raised.

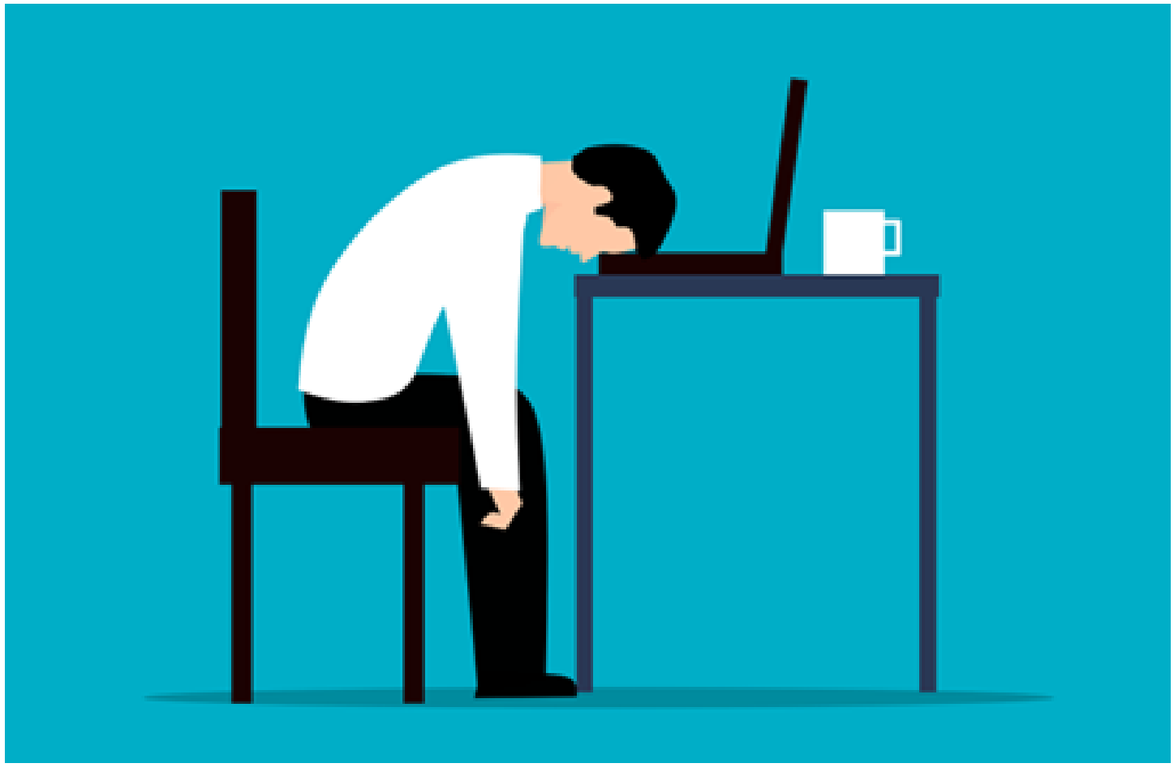
"She contended that her failure to eliminate its misleading effect was an 'oversight'," Holmes wrote.

"That would be an extraordinary oversight for someone of Ms Campbell's seniority and experience. The weight of the evidence instead leads to the conclusion that Ms Campbell knew of the misleading effect of the NPP [New Policy Proposal] but chose to stay silent."

Holmes concluded, "It is remarkable how little interest there seems to have been in ensuring the Scheme's legality, how rushed, its implementation was, how little thought was given to how it would affect welfare recipients and the lengths to which public servants were prepared to go to oblige ministers on a quest for savings. Truly dismaying was the revelation of dishonesty and collusion to prevent the Scheme's lack of legal foundation coming to light."

The full report of the Royal Commission is available HERE.

Why is most corporate documentation so awful?



By George Kesteven

Most organizations have a terrible time with their policy and procedure documentation. Most corporate documentation is ugly, boring, too long, and poorly organized. And usually, somewhat out-of-date.

The core problem is the idea that *documentation* means *documents*. This is a misconception. Documentation is about *knowledge*.

The documentation task is to manage that knowledge: to determine who needs to know what, to ensure that they do know it, and to verify that the knowledge communicated is complete and correct.

Documents - if you use them at all - should be an *output*, not a storage medium. For some purposes documents are a good way to *deliver* information to end-users. But trying to manage corporate knowledge as a library of documents *obviously* doesn't work. *Look at the evidence: when was the last time you saw an organization with good documentation?*

There was a time when documents were effective, back in the golden ages when organizations had typing pools and could afford a dedicated documentation team that did nothing else.

Those days are long gone. In a modern, high-pressure, rapidly-evolving organization, the practical challenges of maintaining documentation as 'a library of documents' are overwhelming.

Documents don't work. Here are some of the reasons:

No editorial oversight

Organizations are complex. By definition, the elements of an organization have to function together, as a whole (that's what *organization* means). But traditional documentation, in practice, treats the elements independently, in separate documents.

The organization changes continually, as does the social and regulatory environment in which it operates. Every change implies a documentation update. And no change is wholly isolated: there are always ripple effects across the organization. A policy changes: *what procedures are affected by the change?* A procedure changes: *is it still consistent with policy?*

No-one is in a position to exercise editorial control over the set of documents as a whole. An individual manager is doing well to maintain the documents for their own area of responsibility; they don't have the time or authority to be working on anyone else's documents.

New documents get added; old ones don't get removed. No-one is saying *If you add this document to the library, section three of that document is now obsolete.*

The result is overlaps, gaps, and contradictions, and a growing accretion of orphaned and obsolete documents.

Confused objectives

Traditional procedure documents are trying to do several things at once:

1. Define the management process followed to achieve an objective: what tasks should be carried out, by whom, in what order.

2. Provide end-user instructions and guidelines on how to carry out those tasks.

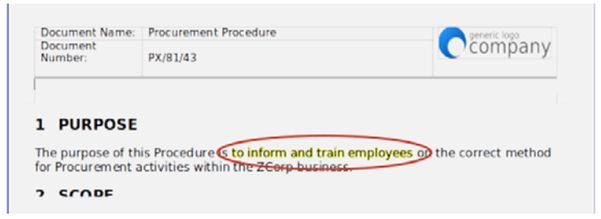
3. Establish compliance with policies, regulations, and management system requirements.

4. Demonstrate that the document itself is controlled as required for ISO and other standards.

Each of these objectives targets a different group of readers. By combining the content required by each group into a single document, each user group is served badly: most of the content is irrelevant to most users.

Insufficient regard for the end-user

The primary objective of documentation is to deliver information to end-users, to the front-line employees who are expected to work according to the documentation. Everything else in the documentation — the policies, the governance framework, the ISO standards — is there to support that objective.



It's common to see procedure documents with statements like: *the purpose of this document is to inform and train employees...* Informing and training your employees is a fine thing to do. But that's the *writer's* objective, not the reader's.

Controlled documents are bloated with large amounts of content that has no value to the end user. Control is important, of course; but you don't need to inflict the control metadata on the end user. End users are not going to check the approval signatures, or read the document history, or look up the references.

Duplicated content

Converting a library of documents to a knowledge management system typically reduces the total page count by over 65 percent. That's a measure of how much duplication and garbage is typically found.

The organization's rules for what content belongs in which documents, if stated at all, tend to be vague at best; and with multiple managers contributing content, duplications and overlaps are inevitable. Everyone wants to be thorough. Policy documents include procedural instructions; procedure documents repeat policy statements. And the HR team may well create its own set of documents for training and induction purposes.

In industrial settings, it's common to see great collections of work instructions or operating procedures, all containing more or less identical sets of definitions and safety instructions. This is poor practice.

- It creates risk. If the same content appears to be repeated in every document, readers will skip over it. So they won't notice if one document has different content. If you have 99 work instructions specifying safety items A, B, and C, no-one will notice that the 100th specifies A, B, C, and D.

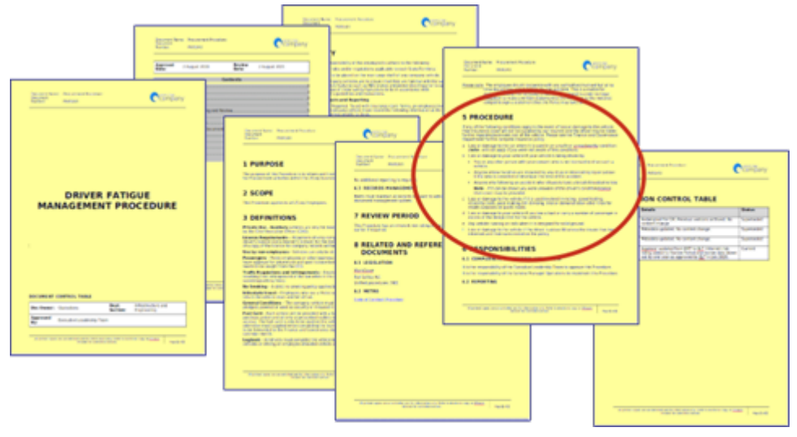
- It's a maintenance nightmare. A minor change to a definition or safety requirement becomes a major editing task, to update hundreds of documents.

Content created by lawyers

In some quarters there's a tendency to include content, particularly in relation to safety, specifically so the organization can defend itself in the event of an incident: *Look, we did tell the employee — here it is in the document. It's not our fault if they didn't read it.* Not only does this create bloated and unusable documents, these days it generally doesn't work anyway. If there's an incident, the test is to ask employees what they actually knew, not to look at what the documentation ostensibly told them. If they didn't read the document, that's on you, not on them. "Your safety system was just ink on paper," as a judge put it in a recent case, fining the company $1m for failing to inform the (now deceased) employee.

When you talk to managers about these problems, most tend to nod in sad resignation, as if lousy documentation were an inevitable feature of modern management. Most managers have never seen good documentation, and many seem unwilling even to countenance the idea that something better than a library of unread documents is possible. s they say in sport: *always change a losing game*. Documentation *can* be done well. Just not with documents.

George Kesteven is a management and documentation consultant specialising in the design, development, and documentation of corporate management systems. https://phrontex.com/



Typical work instruction: seven pages of document, half a page of end-user content

Why financial institutions cannot rely on silver bullet solutions to combat cyber attacks

By Alyssa Blackburn

Financial institutions across Australia are finally waking up to the reality that cyber security threats and attacks are constantly evolving, and the bad actors behind them are relentless. Not only this, but they are becoming more and more sophisticated and advanced in terms of what they will use to launch a cyber attack.

Despite this, the Australian Prudential Regulation Authority (APRA) recently found there are still significant gaps in the industry's approaches to this challenge. One of the most common gaps raised is incomplete identification and classification of critical and sensitive information assets.

Whilst financial institutions have increased awareness of attacks and the severity of the impacts to themselves and their customer base, APRA found banks, insurers and superannuation firms were not doing enough.

Recent research also highlighted heightened awareness among consumers about data security and the strong influence this has on whether they trust and engage with a business. With potential significant impacts to their customer base, financial institutions cannot afford to get this wrong.

Being aware of data risks and threats is simply not enough. Neither is siloed, one-off, or short-term solutions that will not prevent risks.

It is nothing more than a momentary diversion. While it would be nice, there is no single silver bullet that can fend off all types of attacks.

Adopting appropriate countermeasures

As more companies make headlines for various cyber breaches, it is clear that being aware that attacks may happen is insufficient in preventing anything.. Australian executives and Boards are still not taking cyber security seriously enough.

For SMBs alone, 60% go out of business within six months of falling victim to a breach, though most SMBs would not be addressing cyber security today through this lens, it's still a view they cannot afford to ignore.

For financial services enterprises, the risk of their share price tanking or their customers leaving in droves is obvious, and yet many still look for a quick and easy way out. Some, for example, are adopting backup solutions, assuming this will prevent breaches.

A backup solution is certainly a vital necessity as part of a comprehensive program, however assessments need to be made to understand its functions and limitations throughout the business. Further to this, they make the link between incorporating a backup solution with other necessary measures across the organisation, as a standalone 'silver bullet', it's simply not enough.

This approach of seeing data as something that is simply collected and stored increases the already prevalent significant business risk. A risk that continues to multiply with every additional piece of information the business is required to manage.

Instead, organisations need to manage data and content like they would any other asset, ensuring careful protections are implemented as part of a framework approach that doesn't leave one section unguarded.

The first step is to treat data as having a full lifecycle – i.e. there is a beginning, middle and end, possibly with many steps along the way. The beginning should involve backup and protection but equally as important is considering the end stages that require information being destroyed, being re-classified and managed differently after a certain period of time, or something else entirely based on its level of sensitivity or purpose within the business.

In this case, it's quite simple, defensibly destroying data that is no longer required for business or legal purposes, significantly reduces the impact in the event of some kind of breach.

Holistic approaches require company-wide buy-in

Adopting technologies and processes to ensure all data is appropriately identified, classified and managed throughout its lifecycle is only one part of the framework. The people within the organisation are critical to keeping a business' information secure. If the various teams are gathering and storing data in a way that does not align with the corporate standards, risks will continue to exist throughout the organisation despite expensive technology investments.

Everyone – from Board members and CEOs, to CIOs and risk officers – need to be involved and accountable for the processes and management of data and information.

Rather than expecting a new process added to an employee handbook will suffice, financial institutions need to invest in a culture of information responsibility that comes from the highest level of the organisation.

This could include training and education for every employee to ensure they truly understand the importance of secure information management, their role in keeping data safe, and the risks of not following the right processes or calling out when colleagues are acting in ways that create business risk. It further includes ensuring 'compliance by design' meaning that users shouldn't have to move dramatically from their work processes to do the right thing. Making the right thing to do, the easiest thing to do should be the mantra, for both policy and technology implementation.

As business leaders, Board members, and cyber security officers across the financial services sector continue to watch breaches and attacks being reported in the news, now is the time to prepare an end-to-end approach to prevention rather than simply hoping such an attack will not happen to them.

Put end-to-end technology solutions in place, treat data and information as having an end-to-end lifecycle that does not stop when it enters the business, and support employees across the entire business with the tools and knowledge to reduce risk regardless of their level of seniority or specialisation. Essentially, have an arsenal of bullets, rather than relying on the inadequate silver one.

Alyssa Blackburn is Director of Information Management, AvePoint

How to Make Microsoft 365 Copilot Enterprise Ready From a Security and Risk Perspective

By Avivah Litan, Gartner, Inc.

Microsoft 365 Copilot inherits all of Microsoft's cloud security controls, but these were not designed for new AI capabilities. Security and risk management leaders must implement verifiable controls for AI data protection, privacy, and filtering of large language model content inputs and outputs.

We just published Quick Answer: How to Make Microsoft 365 Copilot Enterprise-Ready From a Security and Risk Perspective where my colleagues Matt Cain, Jeremy D'Hoinne, Nader Henein, and Dennis Xu and I explore this topic.

At the time of writing, Microsoft 365 Copilot is not, in Gartner's view, fully "enterprise-ready" — at least not for enterprises operating in regulated industries or subject to privacy regulations such as the EU's GDPR or forthcoming Artificial Intelligence Act. Microsoft might, however, add more security and privacy controls to Copilot before it becomes generally available, because of its dealings with participants in its current preview program.

Our note includes recommendations for supporting Microsoft 365 Copilot readiness for enterprise use in terms of security and risk: (These recommendations can be applied to other enterprise applications that use third-party-hosted Large Language Models).

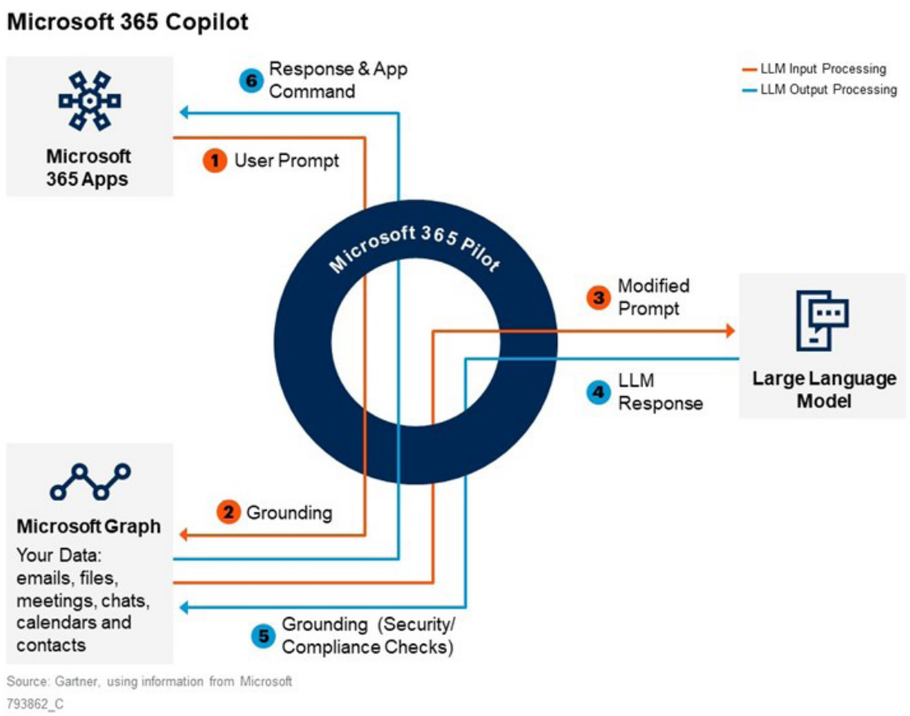
Filtering Microsoft 365 Copilot's inputs and outputs against enterprise specific policies. Such filtering is not included in native Azure content filtering but specialised tools from smaller vendors such as AIShield Guardian and Calypso AI Moderator are starting to feature input and output content-filtering capabilities between user prompts and LLM models.

Verifying Microsoft's data governance and protection assurances that confidential enterprise information transmitted to its large language model (LLM) - for example, in the form of stored prompts - is not compromised. The model itself is stateless, but confidential information can be retained in its prompt history (if customers do not use API interfaces or do not opt out of prompt retention), and potentially in other logging systems in the model's environment. This creates vulnerabilities that bad actors might exploit; alternatively, LLM system administrators could simply make configuration mistakes, as has been reported with OpenAI's LLM environment.

In the meantime, customers must rely on Microsoft's licensing agreements to define the rules governing shared responsibility for data protection. Once it is generally available, Copilot will come under the Microsoft 365 Product Terms.

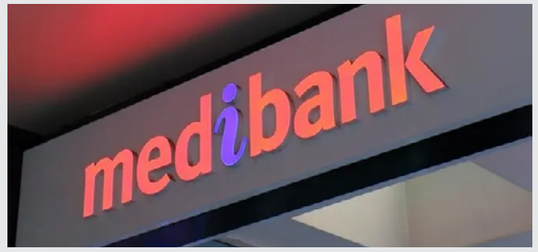
Addressing concerns about LLM model transparency to conduct the impact assessments required to comply with regulations such as the EU's General Data Protection Regulation (GDPR) and upcoming Artificial Intelligence Act. Using third-party security products with Copilot for both non-AI-related and AI-specific security. This will become increasingly important as hackers begin to execute both direct and indirect prompt injection attacks. Coincidentally, Microsoft CTO Kevin Scott was one of the signatories on the Center for AI Safety's statement on AI Risk:

Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war. Certainly, there are existential risks that come with new generations of AI. Those risks are well beyond the scope of this research, which instead addresses the risks of using what Matt Cain calls "Everyday AI".



Source: Gartner, using information from Microsoft
793862_C

APRA's $A250M hit on Medibank Private



The Australian Prudential and Regulation Authority (APRA) has announced it will impose an increase in Medibank's capital adequacy requirement of $A250 million, following a review of its major cyber incident in October 2022.

The capital adjustment, effective from 1 July 2023, will be applied to Medibank's operational risk charge under the new Private Health Insurance (PHI) Capital Framework. It will remain in place until an agreed remediation program of work is completed by Medibank to APRA's satisfaction.

APRA will also conduct a targeted technology review of Medibank, with a particular focus on governance and risk culture. APRA notes that while Medibank has already addressed the specific control weaknesses which permitted unauthorised access to its systems, it still has further work to do across a number of areas to further strengthen its security environment and data management.

APRA Member Suzanne Smith said the October 2022 cyber incident affecting Medibank customers was one of the most significant data breaches ever experienced in Australia.

"In taking this action, APRA seeks to ensure that Medibank expedites its remediation program," Ms Smith said.

"This action demonstrates how seriously APRA takes entities' obligations in relation to cyber risk and that APRA will respond strongly to identified weaknesses in cyber security controls.

"As noted previously, APRA expects Medibank to ensure there is appropriate accountability and consequence management, including impacts to executive remuneration where appropriate. I note that Medibank has consistently dealt with APRA in an open, constructive and cooperative way, consistent with our expectation of all regulated entities.

"Since launching the 2020-2024 Cyber Security Strategy1 APRA has repeatedly stressed the importance of an uplift in cyber security and continued vigilance to identify and address cyber exposures. Unfortunately, not all entities are heeding these messages as we continue to identify poor cyber security practices and inadequate oversight from boards and management," Ms Smith said.

The role of artificial intelligence in information management

By David Gould, EncompaaS

It strikes me as paradoxical that businesses feel very secure in using artificial intelligence to let people know, for example, when it is safe to make a lane change at 100 kilometres per hour, yet they are reticent to use the same technology to classify and manage information through its lifecycle. Artificial Intelligence is used almost every minute of every day, in nearly every smart device we own.

For information management, AI is not a buzzword or a trendy topic. It's a real technology with a real purpose. The emergence of machine learning, natural language processing, and other variants of Artificial Intelligence provide a significant advancement for discovering, classifying, consuming, retaining, and disposing of data no matter its source, location, or creator. AI is the key technology foundation enabling users to manage their data at scale, take their data farther, and make it more dimensional than ever before.

My personal experience and perspective on AI has evolved significantly over the past 12 years. The biggest change is that results generated by AI are actually explainable. You no longer are "required" to have PhDs in Bayesian Inference or Shannon Communication theories to understand what is happening behind the curtain.

Today's AI technology can demonstrate, and we can readily explain, HOW the software processed and produced the answer. There is a logical explanation available each and every time a result is provided. Conversely, when I first helped bring the HP ControlPoint solution to market back in 2012, I remember how difficult – and uncomfortable – it often was to explain the reasoning behind the result.

Many still compare AI to a black box solution. Like all technologies, AI is rapidly evolving and provides much more explainable reasoning behind the processing than ever before. There is a very noticeable lack of trust and confidence when using AI-based tools to analyse, classify and manage information across the enterprise. In fact, there is a discernible level of apprehension, even disdain, among experienced and savvy information governance professionals.

At EncompaaS, we have given this conundrum a great deal of thought – especially when it relates to how we are optimising algorithms and providing "explanation" tools to effectively use AI to analyse and manage very large datasets.

We have seen three core drivers that impact the adoption of AI-based solutions across the enterprise:

It's a threat to my job

AI is a powerful enabling tool. Given the amount of daily data volume created and the need to "fact-check" the assigned manual classification, not even a huge team of individuals can keep pace.

Instead of reclassifying manually, handle this with AI-driven solutions. Let the technology do that work for you. AI frees your time to focus on what is most important: creating and managing policy, enabling colleague productivity, and protecting your company's brand reputation by discovering and protecting sensitive or crown jewel information.

David Gould **is Chief Customer Officer at EncompaaS. Email him at** david.gould@encompaas.cloud

Humans can do it better

The problem is that most large enterprises are creating upwards of 10,000 pieces of content an hour. It is physically impossible for those responsible for data management to physically review that size of information corpus without technology-enabled support. Farming out file boxes of content to low-cost locations for manual review will undoubtedly produce a poor and inconsistent result.

I don't trust it

When AI found its way into applications, it was difficult to explain the result. Most of the focus was on the concept of confidence – how confident was the software that the document being returned was what the user expected.

However, accuracy – supported by recall – is a much better and more meaningful metric to evaluate the effectiveness of AI. Confidence has always been a problem to explain and, frankly as the key metric, it didn't do much to create more "confidence" among potential buyers to acquire any AI-based auto-classification solutions. AI is the driving technology that will give information, data, and records managers more power, more control, and more extended uses of information than ever before.

Our goal at EncompaaS is to make you feel more comfortable with the AI imperative and help you better understand how this technology will revolutionise your information management practices throughout your enterprise. I would love to hear your thoughts – feel free to reach out to me.

ASIC seeks to assess cyber resilience

The Australian Securities and Investments Commission (ASIC) has launched a survey to measure cyber resilience in Australia's corporate and financial markets.

ASIC-regulated entities, including publicly listed companies, have been invited to participate in the ASIC cyber pulse survey, will measure entities' current cyber security and controls, governance arrangements, and incident preparedness.

The survey will be one of the largest conducted into Australia's cyber resilience.

The Australian Cyber Security Centre estimated cybercrime cost Australia $42 billion in 2021.

ASIC Executive Director, Markets, Greg Yanco said, 'recent high-profile cyber attacks demonstrate the need for all businesses to have robust cyber capabilities. Cyber attacks are becoming more frequent and complex and are not limited to companies with large retail customer bases.'

'Cyber attacks can disrupt an organisation's business operations and result in financial, legal and reputational harm. The interconnectedness of our financial system can mean the impact of cyber attacks can spread well beyond a single entity. This self-assessment will provide valuable insights to entities on their own cyber resilience measures compared to their industry peers,' said Mr Yanco.

ASIC expects directors of public companies to ensure their organisation's risk management framework adequately addresses cybersecurity risk, and that controls are implemented to protect key assets and enhance cyber resilience.

Participation in the survey is voluntary, with all responses anonymised. The survey has been designed to help an entity assess its ability to:

govern and manage organisational-wide cyber risks

identify and protect information assets that support critical business services

detect, respond to and recover from cyber security incidents.

The survey is accessible to ASIC regulated entities by logging into the ASIC Regulatory Portal, and following the link provided.

ASIC will publish a report with key findings from the survey later this year.

More information on the cyber pulse survey is at asic.gov.au/cyberpulse.

All information collected will be de-identified and anonymised and cannot be used in any regulatory or enforcement action.

Global Ransomware Attacks up 40%

A 12 month study of recent ransomware trends by cloud security company Zscaler found the barrier of entry has decreased, while cyberattacks have grown in sophistication, due to the prevalence of RaaS, a model where threat actors sell their services on the dark web for 70-80% of ransomware profits.

This business model has continued to increase in popularity over the last few years as evidenced by the frequency of ransomware attacks, which increased by nearly 40% over the last year.

"Ransomware-as-a-Service has contributed to a steady rise in sophisticated ransomware attacks," said Deepen Desai, Global CISO and Head of Security Research, Zscaler.

"Ransomware authors are increasingly staying under the radar by launching encryption-less attacks which involve large volumes of data exfiltration.

"Organisations must move away from using legacy point products and instead migrate to a fully integrated zero trust platform that minimises their attack surface, prevents compromise, reduces the blast radius in the event of a successful attack, and prevents data exfiltration."

The United States was the most targeted country by double-extortion ransomware attacks, with 40% of all victims calling this region home. The following three countries combined, Canada, United Kingdom, and Germany, had less than half of the attacks that targeted U.S. entities.

Over the last year, the most-targeted market sector globally was manufacturing, where intellectual property and critical infrastructure are attractive targets for ransomware groups.

All ransomware groups tracked by Zscaler victimised businesses in this industry, which included companies engaged in goods production for sectors including automotive, electronics, and textiles - just to name a few.

In 2021, ThreatLabz observed 19 ransomware families that adopted double or multi-extortion approaches to their cyberattacks. This has since grown to 44 ransomware families observed.

The reason these types of attacks are popular is because after they encrypt the stolen data, attackers threaten to leak the data online to further increase the pressure on victims to pay.

The increasing popularity of Encryptionless Extortion attacks, which skips over the process of encryption, employs the same tactic of threatening to leak victims' data online if they don't pay. This tactic results in faster and larger profits for ransomware gangs by eliminating software development cycles and decryption support.

These attacks are also harder to detect and receive less attention from the authorities because they do not lock key files and systems or cause the downtime associated with recovery.

Therefore, Encryptionless Extortion attacks tend to not disrupt their victims' business operations - which subsequently results in lower reporting rates

Six ChatGPT Risks Legal and Compliance Leaders Must Evaluate

Legal and compliance leaders should address their organization's exposure to six specific ChatGPT risks, and what guardrails to establish to ensure responsible enterprise use of generative AI tools, according to Gartner, Inc.

"The output generated by ChatGPT and other large language model (LLM) tools are prone to several risks," said Ron Friedmann, senior director analyst in in the Gartner Legal & Compliance Practice.

"Legal and compliance leaders should assess if these issues present a material risk to their enterprise and what controls are needed, both within the enterprise and its extended enterprise of third and nth parties. Failure to do so could expose enterprises to legal, reputational and financial consequences."

The six ChatGPT risks that legal and compliance leaders should evaluate include:

■ Risk 1 – Fabricated and Inaccurate Answers

Perhaps the most common issue with ChatGPT and other LLM tools is a tendency to provide incorrect – although superficially plausible – information. "ChatGPT is also prone to 'hallucinations,' including fabricated answers that are wrong, and non-existent legal or scientific citations," said Friedmann.

"Legal and compliance leaders should issue guidance that requires employees to review any output generated by ChatGPT for accuracy, appropriateness and actual usefulness before being accepted."

■ Risk 2 – Data Privacy and Confidentiality

Legal and compliance leaders should be aware that any information entered into ChatGPT, if chat history is not disabled, may become a part of its training dataset.

"Sensitive, proprietary or confidential information used in prompts may be incorporated into responses for users outside the enterprise," said Friedmann.

"Legal and compliance need to establish a compliance framework for ChatGPT use, and clearly prohibit entering sensitive organizational or personal data into public LLM tools."

■ Risk 3 – Model and Output Bias

Despite OpenAI's efforts to minimize bias and discrimination in ChatGPT, known cases of these issues have already occured, and are likely to persist despite ongoing, active efforts by OpenAI and others to minimize these risks.

"Complete elimination of bias is likely impossible, but legal and compliance need to stay on top of laws governing AI bias, and make sure their guidance is compliant," said Friedmann.

"This may involve working with subject matter experts to ensure output Is reliable and with audit and technology functions to set data quality controls."

■ Risk 4 – Intellectual Property (IP) & Copyright risks

ChatGPT in particular is trained on a large amount of internet data that likely includes copyrighted material. Therefore, it's outputs have the potential to violate copyright or IP protections.

"ChatGPT does not offer source references or explanations as to how its output is generated," said Friedmann.

"Legal and compliance leaders should keep a keen eye on any changes to copyright law that apply to ChatGPT output and require users to scrutinize any output they generate to ensure it doesn't infringe on copyright or IP rights."

■ Risk 5 – Cyber Fraud Risks

Bad actors are already misusing ChatGPT to generate false information at scale (e.g., fake reviews). Moreover, applications that use LLM models, including ChatGPT, are also susceptible to prompt injection, a hacking technique in which malicious adversarial prompts are used to trick the model into performing tasks that it wasn't intended for such as writing malware codes or developing phishing sites that resemble well-known sites.
"Legal and compliance leaders should coordinate with owners of cyber risks to explore whether or when to issue memos to company cybersecurity personnel on this issue," said Friedmann.

"They should also conduct an audit of due diligence sources to verify the quality of their information."

■ Risk 6 – Consumer Protection Risks

Businesses that fail to disclose ChatGPT usage to consumers (e.g., in the form of a customer support chatbot) run the risk of losing their customers' trust and being charged with unfair practices under various laws. For instance, the California chatbot law mandates that in certain consumer interactions, organizations must disclose clearly and conspicuously that a consumer is communicating with a bot.

"Legal and compliance leaders need to ensure their organization's ChatGPT use complies with all relevant regulations and laws, and appropriate disclosures have been made to customers," said Friedmann.

Why Microsoft Teams Archiving is More than Capturing Chat

By Bill Tolson, Archive360

With the onset of the global shift to remote work in 2020, many workers found themselves working from home for the first time. During this period, staying in touch with fellow employees and workgroups, as well as customers, proved to be challenging. Consequently, organizations aggressively adopted collaboration apps such as Zoom, Slack, Meet, GoToMeeting, WebEx, Jabber, and Microsoft Teams to help their newly remote workforce maintain communication and productivity.

For instance, in 2020, it was reported that Microsoft saw a surge in Teams users from 32 million to 44 million in a single week. As of mid-2023, Microsoft Teams has continued to grow and establish itself as one of the leading collaboration platforms, with over 250 million monthly active users.

Owing to the heavy reliance on Microsoft's Microsoft 365 platform by numerous companies for day-to-day operations, it was a logical step for Microsoft-centric organizations to adopt Teams for seamless communication and collaboration during the remote work era.

Why you need to be thinking about data compliance for Teams

While the initial emphasis was on ensuring the safety and productivity of the workforce, organizations had to contend with the implications of rapid adoption of new applications on their regulatory, compliance, and litigation obligations concerning data retention and management.

This concern is ever-present, particularly as hybrid work models have become a mainstay in the modern workspace.

It is essential to understand that all data – including data generated by Teams - is potentially discoverable in litigation. Organizations that are subject to government regulatory data retention requirements need to strategize on archiving Teams content compliantly.

In essence, if your organization is subject to any regulatory data retention or privacy mandates, or if you have internal data governance policies, you must implement measures that encompass Teams usage

Teams Data is More Than Just Chat

A notable challenge in extending data retention policies to Teams is that Teams generates a plethora of data objects through its various functionalities. For example, even simple chat content can be categorized into **three distinct capabilities:**

- **1 to 1 chat**
- **1 to many chat**
- **Files shared and accessed during chat**

Additionally, Teams hosts a variety of data types including group conversations, calendar invites, voice and video calls, meeting recordings, contacts, voicemail, transcripts, and wikis. More recently, Teams has introduced new features such as task assignments, breakout rooms, and polls.

A critical aspect to consider is that Teams does not possess a singular storage repository within Microsoft 365. Instead, it saves data across multiple services within the platform. This multifaceted storage system can complicate data management.

As Microsoft Teams continues to evolve, it has brought forth new methods for managing and archiving data, streamlining processes for IT professionals.

Nonetheless, staying informed of these changes and adjusting data management strategies accordingly is paramount.

One point of contention is that Teams does not facilitate the application of a universal retention policy across an entire Team. Instead, it necessitates the creation and application of retention policies for each data type within each separate repository.

This stipulation posed a significant compliance challenge, particularly for sectors with fluctuating regulatory requirements. It is important to note that Microsoft has been actively working to improve and simplify compliance processes within Teams, and organizations are advised to regularly monitor updates and best practices in this area.

Built-in Teams archiving

When a Team is no longer needed, a Team owner can delete it. When a Team is deleted, it disappears from the Teams client and is no longer available to end users. When a team is deleted, the various data objects in the deleted Team are automatically deleted at the same time and retained on the backend of Microsoft 365 for 30 days and recoverable any time before the 30-day period ends. After 30 days, the Team and its associated data are permanently deleted. A safer practice is to archive the Team instead.

Microsoft has made Teams archiving available to individual Team owners. But unlike a live archiving capability such as a live journalling feed from an email box to an email archive, the archived Team is a snapshot in time meaning when archived, all activity in that specific Team is frozen and made "read-only," including all uploaded/shared files. This makes sense in that the Team owner is designating the Team as no longer needed; they may still want to retain the data for regulatory, legal, or business purposes.

As I mentioned in the previous section, archived Teams groups can have retention policies applied to them but because Teams utilizes several Microsoft 365 applications, Teams retention policies will need to be set in each of the separate Microsoft 365 apps.

It's also important to note that Microsoft has been actively working on enhancing the archiving capabilities of Teams.

Innovations such as integration with cloud-based storage and enhanced search functionality have been introduced, and organizations should continuously monitor for new features and options that may better serve their compliance needs.

Although the archived Team is discoverable through the Microsoft Purview Compliance Portal search and could be used in an eDiscovery case, content within the Team is not guaranteed to be retained for a specific period of time since the Team can technically be restored or deleted at any point by the Team owner – an obvious litigation hold issue.

Capturing Teams Data for eDiscovery

eDiscovery is the process in which electronically stored information (ESI) is sought, secured (legal hold), reviewed,

(Continued Over)

The need to Backup Teams vs the need to Archive...

Historically, organizations have treated backup and archiving as separate processes. The backup process was originally created for disaster recovery. Backing up is the process of making a copy of operating systems and data resident on servers and storage repositories for the purpose of restoring the entire system (OS and data) to the affected server in the event of system issues. For example, an email server becomes corrupted, and the server OS, email application, and messages store needs to be restored as soon as possible. The biggest problem with backups is that data that can be lost between backup cycles (usually 24 hours). In the email server example, the email sent and received between backups is permanently lost when the email server is restored using the last backup data set– also referred to as the recovery point objective (RPO). The backup is usually performed utilizing a backup application that creates its own custom-formatted data container – meaning it is very difficult to search for and act on specific files in a backup file. In reality, the backup must be fully restored to the server to search and act on specific files.

On the other hand, the archiving process stores a single copy of individual files for long-term storage and management for legal, regulatory, and business reasons. A key distinction here is that individually archived data, if stored in its native format, is easier to search for and act on.

Even today, some organizations continue to rely on backups as a substitute for low-cost archives. While the cost of backup storage has continued to fall, finding and restoring these individual files can be extremely slow and expensive. For example, the estimated cost to restore, search, delete PI, and create a new backup tape can range between $US1,000 and $US3,000 per tape. Imagine how many of your organization's backup tapes contain a particular data subject's PI...

To learn more read this article: A Backup is not an Archive ... but a Cloud Archive can be an Effective Backup

and turned over to opposing counsel with the intent of using it as evidence in a civil or criminal legal case. In the U.S., the eDiscovery process is represented by the Electronic Discovery Reference Model (EDRM) and the Federal Rules of Civil Procedure (FRCP).

Responding to an eDiscovery request fully and in a timely manner is an absolute responsibility for any organization, under the U.S. legal system. Failure to respond in the appropriate manner can result in loss of case, fines, having to pay the cost of opposing counsel, loss of professional designation (J.D.), and in limited circumstances, jail time. As I mentioned in the opening of this blog, all relevant data is potentially discoverable no matter where it is stored, including all metadata.

Obviously, this means Teams data (and all metadata) is not exempt from an eDiscovery request which means that companies across all industries that have incorporated Teams into their remote or hybrid workforce must be able to capture and secure all Teams data in a legally defensible manner when litigation is anticipated.

How would your organization find and secure potentially responsive Teams data of select custodians if needed? The obvious answer is "with difficulty." And could you guarantee that all relevant Teams data would be found and placed on a litigation hold? The truthful answer: maybe not.

In fact, Teams has a somewhat complicated persona when dealing with litigation hold and eDiscovery. To begin with, not all Teams content is discoverable from within Microsoft 365. All Teams 1:1 or group chats are saved (journalled) through to the respective users' mailboxes and are therefore discoverable.

Originally published April 22, 2020 and updated 5/19/2020, This article has been revised for 2023. The original topic remains the same: companies should be aware of the full ramifications of archiving and discovering Teams content and plan accordingly to ensure full compliance with regulatory as well as eDiscovery requirements.

All standard channel messages are journalled through to the group mailbox representing the Team. Files uploaded in standard channels are covered under the eDiscovery functionality for SharePoint Online and OneDrive for Business. eDiscovery of messages and files in private channels works differently than in standard channels. Additionally, placing a user on hold does not automatically place a group on hold or vice-versa.

However, Teams' continuous evolution has led to improved eDiscovery capabilities. Teams now supports more advanced search and holds options, making it easier for administrators to retrieve and preserve content relevant to litigation.

This has been a significant step forward in addressing the complexities previously associated with eDiscovery in Teams. Microsoft Teams' compliance features have also been updated to better align with international standards, ensuring a more global application.

When eDiscovery is run from the Microsoft Purview Compliance Portal, Teams data will appear as IM or Conversations in the Excel eDiscovery export output. Administrators can use an eDiscovery case to create holds to preserve content that might be relevant to a given case.

You can place a hold on the mailboxes and sites that are associated with Microsoft Teams or Yammer Groups. When you place content locations on hold, content is held until you remove the hold from the content location or until you delete the hold.

Microsoft has been investing in expanding the capabilities of the Microsoft Purview Compliance Portal to provide more granular control over eDiscovery processes, which reflects their commitment to supporting compliance needs across various industries.

One issue to be aware of after you place a content location on hold, it can take up to 24 hours for the hold to take effect - enabling inadvertent data spoliation. However, with the rapid advancement in technology, Microsoft has been working on reducing the time it takes for holds to take effect, thereby minimizing the risk of data loss.

So, what is the answer to these Teams' regulatory and eDiscovery challenges?

Teams data consolidation and archiving

Because Teams stores data across several applications in Microsoft 365, placing a litigation hold and reviewing data across Teams repositories can be complex, risky, and time-consuming because it involves manual processes. To simplify the process and ensure compliance with regulatory and eDiscovery requirements, companies should look to consolidate their journalled Teams data streams into a central archive ensuring data management, search, placement of litigation hold, review, and production can be quick and compliant.

Challenges and Importance of Teams Data Archiving

With the ever-growing usage of Teams, especially in hybrid work environments that have become the new norm in the post-COVID era, the need for efficient data consolidation and archiving has become even more critical. Moreover, an essential capability for compliant Teams regulatory response and eDiscovery review is the ability to capture Teams content in context.

Specifically, the ability to capture and review not just an individual chat conversation or uploaded piece of content, but entire conversation threads, with all data objects, within complete timelines. Only this form of Teams archiving will ensure that the true meaning of the conversation and any Teams object posts can be accurately viewed, and the meaning easily determined.

Entity	Storage	Storage
Message	Chat service table storage (moving to Cosmos DB)	Ingested to Exchange to enable compliance
Image	Media service on Azure (using Blob storage)	Ingested to Exchange to enable compliance
Files	Team files → SharePoint Chat files → OneDrive for Business	
Voicemail	Individual mailbox in Exchange	
Recording	Media service on Azure (using Blob storage) (<24 hours)	Encoded to Stream
Calendar meeting	Individual mailbox in Exchange	
Contacts	Exchange	
Telemetry	Microsoft Data warehouse (No customer content)	

Table 1: Teams data is stored in different repositories depending on the content type. (Table taken from Microsoft article: "*Location of data in Microsoft Teams*")

For organizations looking to implement a third-party Teams archiving solution, beware that some Teams archiving applications are unable to capture and manage all Teams data and only capture the chat function.

Advancements in AI and data analysis have seen remarkable developments in recent years, leading to a marked improvement in the accuracy and contextual understanding of Teams data. When selecting a third-party archiving solution, it's paramount for organizations to opt for one that seamlessly integrates these cutting-edge technologies, ensuring that data is captured more efficiently and effectively. [read our blog on predictive information governance here]

Again, in litigation, all data is subject to litigation hold and eDiscovery. Data objects that cannot be discovered pose a significant liability for organizations responding to eDiscovery requests.

In a typical scenario, a knowledgeable attorney may intentionally target Teams data objects that they believe can evade discovery searches, potentially leading to complaints about incomplete eDiscovery. It is important to recognize that the Teams ecosystem is not static.

With continuous updates and improvements in Teams and related third-party solutions, the range of discoverable data objects is constantly expanding. Organizations must stay vigilant and informed about the evolving capabilities and limitations of the available tools.

A consolidated Teams archive simplifies this complex situation. Instead of searching across multiple Microsoft 365 storage locations, the archive provides a single, unified dashboard for efficiently searching, securing, and reviewing Teams content to ensure regulatory compliance and support eDiscovery. I

t is encouraging to witness the emergence of innovative third-party solutions that specialize in Teams data consolidation and archiving. These advanced solutions streamline data management by offering automated tagging, categorization, and other efficient features. For instance, Archive360 offers an archiving solution tailored for Microsoft Teams, helping organizations efficiently consolidate and manage their Teams data in a secure and compliant manner.

Microsoft Teams is undoubtedly a highly productive collaboration tool. However, its use in organizations bound by regulatory retention requirements or involved in litigation introduces a layer of complexity. To navigate this complexity, streamline Teams archiving, and mitigate risks associated with compliance and eDiscovery, it is crucial to employ a comprehensive, standalone Teams archiving application capable of managing all Teams data effectively.

Conclusion

In conclusion, the landscape of data management and compliance is continuously evolving. It is vital for organizations to stay informed, periodically review, and adjust their Teams archiving strategies. Aligning these strategies with the latest best practices and regulatory requirements is not just a checkbox exercise; it is a strategic move that facilitates meeting legal obligations and unleashing the full potential of Microsoft Teams as an indispensable tool in the collaborative workspace of today and tomorrow.

For more information on how Archive360 can help solve your Microsoft Teams archiving needs: Click Here.

Contact Us to speak to an expert or schedule a demo today.

Bill Tolson is the Vice President of Global Compliance for Archive360. Bill brings more than 29 years of experience with multinational corporations and technology start-ups, including 19-plus years in the archiving, information governance, and eDiscovery markets. Bill is a frequent speaker at legal and information governance industry events and has authored numerous eBooks, articles and blogs.

MinterEllison expands cyber security practice

MinterEllison Consulting, the consulting business of law firm MinterEllison, has added consultants to its national cyber security practice. This expansion comes just three months after the appointment of cyber security expert Shannon Sedgwick, who joined as lead partner of the practice.

Tulin Sevgin joins as Director in the Sydney office bringing with her over a decade of experience working with local and global organisations in financial services, energy, infrastructure, construction, and for the US government. She is a third party risk management specialist.

She has a depth of knowledge about what makes organisations resilient to data breaches and supply chain attacks and delivers solutions that integrate cyber risk into risk management frameworks.

Russell Weir, a new Director in the Brisbane office brings a wealth of experience from his previous roles as Head of Cyber Security and CIO.

Most recently, Weir was the first dedicated cybersecurity professional in local government at the City of Newcastle, where he established their cyber security strategy and governance framework.

Natasha Basukoski and Jamie Dunn join the Sydney practice bringing a further depth of cyber analytics to the team. Basukoski previously worked with a global consultancy firm and spent four years within financial services. Dunn brings in-depth experience in supply chain risk management after a number of years specialising in this area within a well-known cyber security technology vendor.

"I am thrilled to welcome Tulin, Russell, Natasha, and Jamie to our growing cyber security practice," said Shannon Sedgwick Partner, Head of Cyber Security MinterEllison Consulting.

"They bring an added depth and dimension to our combined consulting and legal cyber security offering."

"Over the past year, there has been heightened awareness of cyber security risks among some of the country's largest companies which have suffered significant breaches. Cyber risk remains a top five priority for organisations, as confirmed by our recently published 2023 Cyber Risk report."

"Clients face challenges due to under-resourcing, under-preparedness and limited understanding of their regulatory, legal and technical requirements. They are turning to our rapidly growing team of consultants and existing highly experienced legal practitioners for a comprehensive response to cyber security encompassing strategic planning, incident response, data governance, M&A due diligence, supply chain risk management, regulatory and legal, and technical cyber security advisory."

$A4.4M funding for Singapore Startup

Singapore-based start-up, OneView has secured $A4 million in seed funding from ADERA Global, Beyon Connect, part of the Beyon Group, and New Zealand-based Cumulo9 to introduce an innovative digital platform for secure communication of documents and facilitating value-added e-services.

ONEVIEW's platform aims to revolutionise bill payments by transforming the interaction between consumers and senders, thereby simplifying everyday digital communications with a more convenient, sustainable, and spam-free experience.

ONEVIEW plans to roll out digital post box and communication services by the end of the year in Singapore, enabling users to easily access their documents and communications from multiple billers and senders within a single app.

Using Singapore as a testbed for the Southeast Asian region, ONEVIEW aims to set the benchmark for innovative, eco-friendly digital solutions that improve people's lives. By partnering with key players in the industry such as ADERA Global, Beyon Connect, and Cumulo9, ONEVIEW's platform offers a comprehensive solution that meets the needs of both consumers and senders.

ADERA Global, headquartered in Singapore, is a leader in data security and automation, serving global banks, financial institutions, telecommunications and government agencies around the world.

Beyon Connect, part of the Beyon group based in Bahrain, is a provider of new technologies with great innovation potential, Software-as-a-Service platforms, and advanced IT solutions for both the public and private sectors in the MENA region.

New Zealand-based Cumulo9 provides business services for the digital delivery of transactional documents, as well as CCM (Customer Communications) solutions throughout APAC.

ONEVIEW aims to enable effective and secure communications between government, agencies, business enterprises and individuals in Singapore. The platform is designed to simplify secure document transmission and encourage greater digitization of utilising embedded e-services to fulfill actions such as payments, document verification and other value-added services.

ONEVIEW will reduce the need for paper bills, thus reducing carbon footprint and promoting sustainability.

"Our mission is to revolutionize the way people pay and manage their important documents such as bills, while also helping Singapore achieve its vision of becoming a Smart Nation," said LEE Kok How, CEO of ONEVIEW.

"Our app is designed to simplify the process, save users time and hassle, and help them stay on top of their action items, such as payments, with ease. With the support of our investors, we are confident that our platform will set a new standard for digital bill payment services in the region, while contributing to Singapore's vision of a Smart Nation."

https://oneview.sg/

The burgeoning business of bots

Digital employees, such as chatbots powered by artificial intelligence, are increasingly utilised alongside human employees to create a dual frontline service, but how are customers experiencing this trend?

University of Auckland researchers explore the burgeoning business of chatbot-human collaboration and customer perceptions in a recent paper titled *The Future Of Work: Creating an Effective Collaboration Between Human and Digital Employees in Service*.

Rather than looking at chatbots as just tools, these non-human agents can be considered collaborators and team members, says Associate Professor (Marketing) Laszlo Sajtos.

"Doing so can foster customer recognition of a positive alliance and effortless human-bot teamwork through their awareness of the team's joint efforts in handling service requests," he says.

In their article, Sajtos, former Business School doctorate student Khanh Bao Quang Le and Associate Professor Karen Fernandez detail five experimental studies they undertook with 1,403 participants. One scenario saw participants play the role of a prospective student looking online for a data science programme. Another placed them within a finance consulting setting.

"We found that making the human-digital employee collaboration visible to customers during their service encounter can reinforce their perception of a cohesive team and a fluent service process and that this drives satisfaction," says Sajtos.

"The key word here is transparency. When human and digital employees work together, it's critical to provide clear communication to and in front of the customer about what happens during the service provision – who takes care of which task and what information is transferred between entities. It's important to demonstrate a cohesive team through communicating a joint goal."

The research also shows that having a human employee in a supervisory role increases customer satisfaction. Additionally, the study suggests that the human employee's effectiveness as a supervisor lies in improving the customer's perception of a cohesive team. The marketing expert says businesses will be well served if they move towards building human-digital employee teams that represent their brand and business as a dual frontline.

"We recommend that firms train their digital and human employees to work as a cohesive team in front of customers. This could be achieved by coding the chatbot to notify customers about task handovers and instructing human employees to acknowledge the transfer in front of the customer."

Explaining the process to the customer and setting expectations at the beginning of the experience can enable businesses to create a seamless customer experience and the impression of a cohesive team, says Sajtos, who is currently working on a project investigating the use, and perceptions of, robots employed in restaurants in China.

Good Governance: A Great Way to Build Trust and Positive Relationships

By Jack Krutak

Ever wondered what might be (one of the) secret ingredients for a successful, transformational IT project? Well, other than the obvious and well-documented stuff such as good Project Management discipline, you will also need a robust and effective governance, shared with your customer. It's not an unnecessary overhead or an administrative burden. It is key to every project's success.

What does good governance look like? And how does it work?

Several key features of good governance can proactively de-escalate and resolve conflicts in IT projects before they boil over:

- Robust terms of reference established early on
- A strong and decisive Project Executive, with a balanced view of the business and project priorities
- Proactive communication strategies
- Ability to build consensus among stakeholders
- Regular review of risks and mitigation strategies
- Cultivating a culture of collaboration and trust.

It is absolutely crucial that both vendor and customer are aligned from the beginning on all of these issues.

We're In This Together

Good governance provides a joint platform for proactive risk management and mitigation and creates a shared responsibility for managing risks (noticed how I didn't say "shared ownership"? You still need just one risk owner.

The Project Board typically drives governance. It provides the opportunity for vendors and customers to meet regularly to discuss progress, identify risks and solutions, and come to agreed decisions quickly.

For example, business users using the project product might be unable to clearly articulate and prioritise requirements. This is likely to create problems later down the track during testing and deployment but such a problem can be solved, so identify it early on. The Board can escalate this internally and assist the business either by mobilising additional resources or clarifying business priorities. It is a great way to build trust and positive relationships.

Projects need transparency and clarity at all levels. Accomplish this with open and structured communication and escalation processes.

Good governance should be set up to represent Senior Users from the Business, Senior Suppliers including internal suppliers (for example, the IT department of the customer), and Project Executives (Senior Responsible Officers) with appropriate seniority within the customer organisation.

When implementing multiple levels of governance, avoid having the same group of people meeting repeatedly under different circumstances. Maintain separation of duties. Keep the process efficient and effective.

Good governance in IT projects

IT projects come with their special challenges.

The most common mistake in managing IT projects is for good governance to be seen as unnecessary, optional, or burdensome.

Sometimes, the customer has established good governance, but the vendor (Senior Supplier) is not represented. There's a risk here that the Board might be presented with incomplete or skewed information. Suboptimal decisions will be the result.

Again, ensure everyone is aligned. Additionally, conduct regular project governance reviews. Make sure your project is delivering against the expectations of both parties. Set the expectations early. And be sure to tailor the governance process to the risk profile of your project.

By implementing good governance from the beginning, you can de-escalate and resolve conflicts, ensuring an effective and efficient project.

And in the long term? Build a great reputation.

Jack Krutak is Global Head of Delivery at Objective Corporation.

COMPANIES WITH ANSWERS AND SOLUTIONS FOR YOUR DIGITAL TRANSFORMATION INITIATIVES

ezescan
making digital work

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

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
SMARTER SAFER FASTER

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

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
a Citadel Group Company

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
Document Process Automation

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

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

AvePoint

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

archTIS teams with Janusnet for Data Classification

Australia's archTIS has enhanced the capabilities of NC Protect, its Security solution for Microsoft 365, Sharepoint Server and File Shares, in a new partnership with data classification specialist Janusnet. he integration combines Janusseal's robust classification with NC Protect's dynamic access and protection capabilities, creating a strong data-centric security posture for Defence and industry customers using Microsoft applications.

Greg Colla, co-founder of Janusnet, said, "The partnership between Janusnet and archTIS is a great example of the whole solution being greater than the sum of its parts. Combining the rich metadata embedded by Janusnet technology with archTIS' exceptional Attribute-based access control (ABAC) capabilities delivers customers an outstanding solution to meet complex regulatory and security requirements for appropriately handling unstructured data.

Janusnet's Janusseal Documents provides data classification solutions for government and industry. Janusnet's products are used by the governments of Australia, New Zealand, the United States, and the United Kingdom.

archTIS' NC Protect solution adds dynamic fine-grain ABAC policies to control access to and apply file-level protection to Microsoft application data with security capabilities such as in-transit encryption, secure read-only access, dynamic security watermarks, CUI markings, and file obfuscation to the platform.

Access and security controls are dynamically adjusted based on realtime comparison of user context and file content to ensure users access, use and share business-critical data according to set policies. Joint customers can now use Janusseal's classifications and pair them with NC Protect's dynamic access and data protection policies to safeguard sensitive data and meet compliance obligations using the new Janusseal Connector in NC Protect.

The Janusseal Connector integration is part of NC Protect's 'bring your own classification' model which allows customers to use NC Protect's classification engine or leverage existing classifications as one of the attributes used by the product's dynamic ABAC policies.

Kurt Mueffelmann, Global COO and US President of archTIS stated, "Customers are looking for ways to add ABAC protection without sacrificing existing technology investments and classification processes.

"This new integration allows Janusseal customers to use their existing classifications with NC Protect policies to enhance sensitive data labelling capabilities with dynamic protection to meet government, defence and enterprise needs."

https://www.janusnet.com/ https://www.archtis.com/

Data Management Powered by GPT-4

Astera Software has unveiled a new suite of AI-driven integrations powered by GPT-4. The initial integration will be with Astera's data extraction solution, ReportMiner. With new AI capabilities, users can generate report models 90% faster, providing more accurate, actionable insights in a fraction of the time.

"We are enabling businesses of any size to have access to the insights they need to take action and make data-driven decisions with confidence," said Ibrahim Surani, Astera's founder and CEO.

"With our new AI powered features, we're taking the first step towards a future where data management is no longer a burden, but rather, a source of competitive advantage."

The primary feature of this AI-driven tool is its ability to automate template creation, which streamlines the process of creating report models.

The model can be trained to identify and extract data fields, use semantic matching/natural language processing to understand the context of the document, and create a layout that can be reverse-engineered to create templates.

Astera's new AI capabilities also extend beyond template generation, offering customers the ability to validate data and identify errors, perform universal mapping, and automate other data management tasks.

https://www.astera.com/

Flowfinity Process

Flowfinity, a no-code platform for business process automation, has announced the launch of a new free application called the Project Asset Hub. The Asset Hub was designed to help people responsible for managing process improvement projects by being a single source of truth for assets including records and documentation related to stakeholders, requirements, scope, QA testing and more.

The Project Asset Hub is based on pest practices as described by the International Institute of Business Analysis and organizes records and documentation in eight discrete stages throughout the life of a project.

The application is highly scalable whether utilized by a team of one or one hundred and can be easily configured without code to meet the needs of any specific project, large or small.

The Project Asset Hub is the latest addition to Flowfinity's suite of no-code software applications for business process automation. With a focus on empowering business users to automate their workflows, The Flowfinity platform has been adopted by organizations across a wide range of industries, including engineering, manufacturing, and field services.

https://www.flowfinity.com/

AvePoint launches Confide on Syntex

Now available through private preview, the next generation of AvePoint Confide, will utilise Microsoft Syntex repository services, giving organizations control and flexibility to manage data and workflows across a range of business projects with unique sharing requirements.

Microsoft Syntex repository services provides both ISVs and enterprises with an embeddable file and document management platform.

With AvePoint Confide, organizations can now take advantage of their existing Microsoft investments to accommodate scenarios with complex sharing needs that require differentiated security and storage capabilities.

"We built AvePoint Confide as an industry-focused solution to help key business stakeholders collaborate on projects with complex sharing needs like vendor management, bids and tenders, and due diligence," said John Peluso, Chief Product Officer, AvePoint.

"As a launch partner for this new Syntex technology, we are excited to offer organizations an even more sophisticated approach to secure collaboration that drives operational efficiency and meets their unique business requirements."

Today marks an evolution of AvePoint Confide's existing secure project room solution launched last year. Now, organizations with complex sharing scenarios can spin up digital workspaces that are isolated from the rest of the tenant in a unique repository. Then, project admins can provision custom security and governance settings to ensure that internal and external collaborators can share data within the workspace's project library, collaborate on files and tasks, and access real-time project insights.

Unlike third-party vendors that often store data and limit controls, AvePoint Confide enables organizations to apply custom tenant controls, achieving agile, native collaboration without sacrificing compliance and security.

To learn more and sign up for AvePoint's private preview program for AvePoint Confide, built on Microsoft Syntex repository services, go to https://www.avepoint.com/lp/confide-private-preview

#AI-Powered Cyber-security analyst

CrowdStrike has introduced Charlotte AI, a new generative AI cybersecurity analyst that lets users ask natural language questions – in English and dozens of languages – and receive intuitive answers from the CrowdStrike Falcon platform.

Currently available in private customer preview, Charlotte AI initially addresses three common use cases:

Democratizing Cybersecurity: With Charlotte AI, everyone from the IT helpdesk to executives like CISOs and CIOs can quickly ask straightforward questions such as "What is our risk level against the latest Microsoft vulnerability?" to directly gain real-time, actionable insights, drive better risk-based decision making and accelerate time to response.

Elevate Security Analyst Productivity with AI-Powered Threat Hunting: Charlotte AI will empower less experienced IT and security professionals to make better decisions faster, closing the skills gap and reducing response time to critical incidents. New security analysts, such as a Tier 1 member of a SOC, will now be able to operate the CrowdStrike Falcon platform like a more advanced SOC analyst.

The Ultimate Force Multiplier for Security Experts: Charlotte AI will enable the most experienced security experts to automate repetitive tasks like data collection, extraction and basic threat search and detection while making it easier to perform more advanced security actions.

It will also accelerate enterprise-wise XDR use cases across every attack surface and third-party product, directly from the CrowdStrike Falcon platform. Hunting and remediating threats across the organization will be faster and easier by asking simple natural language queries.

Charlotte AI utilizes the trillions of security events captured in the CrowdStrike Threat Graph, asset telemetry from across users, devices, identities, cloud workloads and CrowdStrike's threat intelligence.

https://www.crowdstrike.com

Identity Security Based Browser

CyberArk has announced what it claims is a 'first-of-its-kind' Identity Security web browser to enable organizations to better protect against attacks with a flexible, identity-based approach to securing employee and third-party access to enterprise resources.

By 2030, Gartner predicts enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience.

Browsers provide a vital connection between identities, applications and data, making them a prominent attack vector and a target for cybercriminals – especially in distributed, work-from-anywhere environments.

A rise in post-MFA authentication attacks targeting session cookies reinforces the need for defense-in-depth strategies. Part of the CyberArk Identity Security Platform, the Chromium-based CyberArk Secure Browser supports enterprise Zero Trust initiatives with integrated security, centralized policy management and productivity tools while delivering a familiar user experience.

CyberArk Secure Browser is designed to eliminate existing security gaps between consumer-focused browsers and SaaS applications, endpoint-based controls and identity providers. By extending the CyberArk Identity Security Platform to the browser itself, CyberArk offers a way for IT teams to tailor security, privacy and productivity controls on managed and unmanaged devices.

Key features include:

- **Cookieless Browsing:** Cookieless browsing is a key differentiating feature that allows users to access and use web-based resources without exposing cookie files to attackers. The cookies will be stored remotely on CyberArk servers enabling secure and seamless web browsing without saving cookie files on the endpoints. This approach makes it difficult for attackers or third parties to steal, forge, alter or manipulate cookies to gain unauthorized access to sensitive resources and helps ensure that users' web sessions, data and accounts remain confidential and secure.

- **Data Exfiltration Protections:** Companies can control the browsing experience with fine-grained policies designed to prevent data exfiltration attempts that can compromise corporate data.

- **Password Replacement:** CyberArk Secure Browser features patent-pending password replacement functionality. Instead of showing stored credentials for privileged resources or websites, the browser displays a one-time alphanumeric string. This string works only once, only in CyberArk Secure Browser and only for intended targets – eliminating the possibility that end users will see these privileged credentials in plain text.

- **Extensibility:** Third-party identity providers and out-of-the-box integrations are supported with the CyberArk Identity Security Platform solutions, including CyberArk Workforce Password Management and CyberArk Secure Web Sessions. This allows companies to customize session protections, access controls and credential management to each user based on their roles. It also works in conjunction with CyberArk Endpoint Privilege Manager to mitigate potentially risky web access and vulnerable endpoints.

- **Quick Access Bar:** The built-in quick access sidebar helps ensure end users can utilize their Single Sign-On (SSO) credentials to securely access frequently used apps, third-party tools and CyberArk privileged access management resources directly from CyberArk Secure Browser with the click of a button.

Dynamically mirroring controls and access policies existing on Chrome and Edge browsers that are already deployed on the end user's device, CyberArk Secure Browser reduces IT overhead and accelerates the deployment timeline for employees, contractors and vendors.

Planned availability for CyberArk Secure Browser on Windows endpoints is by the end of 2023. To learn more visit https://lp.cyberark.com/secure-browser-early-access.html.

Risk/Compliance models address Generative AI Concerns

In response to growing use of generative AI tools, Darktrace has launched new risk and compliance models to help its 8,400 customers around the world address the increasing risk of IP loss and data leakage.

These new risk and compliance models for Darktrace DETECT and RESPOND make it easier for customers to put guardrails in place to monitor, and when necessary, respond to activity and connections to generative AI and large language model (LLM) tools.

This comes as Darktrace's AI observed 74% of active customer deployments have employees using generative AI tools in the workplace. In one instance, in May 2023 Darktrace detected and prevented an upload of over 1GB of data to a generative AI tool at one of its customers.

New generative AI tools promise increases in productivity and new ways of augmenting human creativity. CISOs must balance the desire to embrace these innovations to boost productivity while managing risk.

Government agencies including the UK's National Cyber Security Centre have already issued guidance about the need to manage risk when using generative AI tools and other LLMs in the workplace. In addition, regulators in a variety of jurisdictions (including the UK, EU, and US) and in various sectors are expected to lay out guidance to companies on how to make the most of AI without exacerbating its potential dangers.

"Since generative AI tools like ChatGPT have gone mainstream, our company is increasingly aware of how companies are being impacted. First and foremost, we are focused on the attack vector and how well prepared we are to respond to potential threats. Equally as important is data privacy, and we are hearing stories in the news about potential data protection and data loss," said Allan Jacobson, Vice President and Head of Information Technology, Orion Office REIT.

"Businesses need a combination of technology and clear guardrails to take advantage of the benefits while managing the potential risks."

Darktrace's Chief Executive Officer Poppy Gustafsson said: "CISOs across the world are trying to understand how they should manage the risks and opportunities presented by publicly available AI tools in a world where public sentiment flits from euphoria to terror. Sentiment aside, the AI genie is not going back in the bottle and AI tools are rapidly becoming part of our day-to-day lives, much in the same way as the internet or social media. "

https://darktrace.com/

Data Governance Application with Generative AI

data.world has launched new automations and automation-driven workflows to accelerate the delivery of governed data across enterprise teams. The announcement introduces the third class of AI-driven bots on the data.world Data Catalog Platform.

The data governance-focused Eureka Bots join the data discovery-focused Archie Bots and DataOps-focused BB Bots to address the most pressing challenges to working effectively with data, automating data management processes, and delivering governed data for AI.

AI initiatives have intensified the workloads of data governance teams with an emphasis on data privacy, data security, and the accurate use of data. Governance is no longer a choice, but a requirement for both data consumers and responsible AI.

data.world's inclusion of Eureka Bots in both its standard Data Catalog Application and in the new premium Data Governance Application ensure that teams at every stage of data catalog adoption can utilize robust governance capabilities.

With diverse governance automations, teams can elevate the focus of data governance teams from purely tactical program execution to strategic initiative leadership. Foundational challenges like the security of personal identifiable information (PII) and compliance with regulations like GDPR and CCPA, threaten to stall data, analytics, and AI initiatives.

Go-to-market timelines are slowed further by an overwhelming reliance (70%) on manual data governance, as found in a recent survey of enterprise data governance leaders conducted by data.world and Goldman Sachs Asset Management.

Unsurprisingly, nearly every data governance leader (96%) wants increased automation in their organization. But the complex requirements of data governance have made it difficult to adopt automations without a complex coding environment.

"Innovations in generative AI are designed to improve the complex work of knowledge workers like data governance professionals. A recent MIT study on generative AI saw that ChatGPT reduced skill inequalities, changed how users spent their time, and increased productivity by up to 59%," said Juan Sequeda, head of AI Lab at data.world.

"data.world bots integrate with generative AI and automation to deliver similar results through the data.world applications for data cataloging, DataOps, and data governance."

With the new Data Governance Premium package, Eureka Bots are enabled to support automations with multi-step workflows and task management that incorporate a combination of human and machine decisions.

https://data.world/

Privacy leak detection supported by Microsoft AI

The data auditing platform Datatrue is launching a patented data validation and personal identification system that employs artificial intelligence (AI) and machine learning (ML) to identify and prevent data leaks.

DataTrue is collaborating with Microsoft to enhance this new offering, integrating Azure's advanced AI and ML into its technology stack.

Over 2,700 security breaches have been reported to the Office of the Australian Information Commissioner (OAIC) since the beginning of 2020, impacting millions of individuals. The breaches at Latitude and Optus alone have affected approximately 15 million people.

DataTrue's Data Validation Engines (DVE) and Personal Information Identification (PII) leakage detection solution decodes information in data packets containing cookies, URLs, and request bodies, including data transfers to and from third-party servers.

The system analyses this information to ascertain whether it includes any personally identifiable data that should not be present. It then uses AI and machine learning to improve itself and make the detection of issues continuously more precise and faster.

According to Dean Gingell, DataTrue's co-founder and the co-inventor of the PII technology, Microsoft's AI and machine learning offerings:

"Significantly enable to improve the leakage detection solution. Not only does it decrease the configuration time for the feature, but it also reduces the development time needed to expand the feature vastly."

One customer using DataTrue's PII detection tools is Coles, which stated:

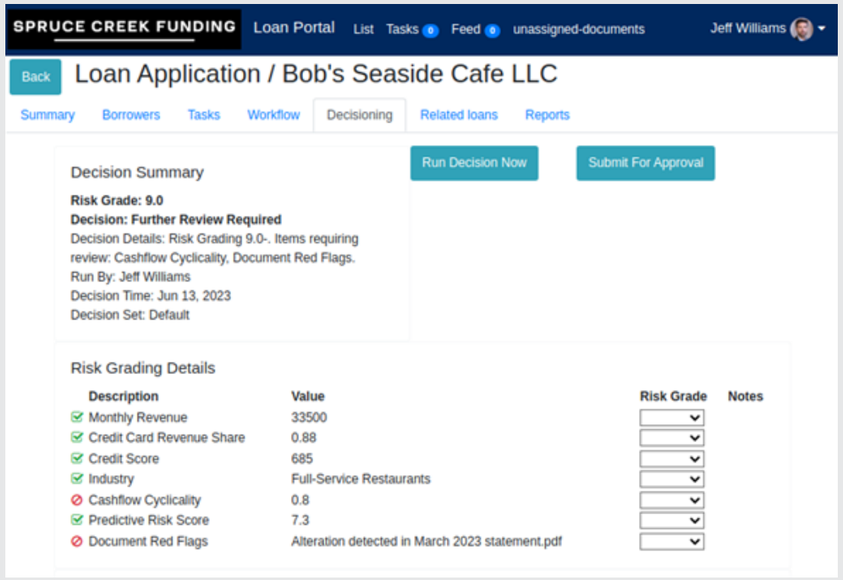
"DataTrue has helped us maintain secure and accurate end-user data through significant changes and investments – including switching analytics vendors and launching our new Angular site. Our comprehensive test suites keep us on top of any issues and alert us to any unexpected data problems, including data leakage to third parties."

By partnering with Microsoft and leveraging Azure's solutions and platform, DataTrue provides businesses with a powerful tool to protect private data, comply with privacy laws, and safeguard information.

Beyond its cybersecurity offerings, DataTrue also conducts thorough data audits for Analytics, Marketing, and Compliance enterprise departments, which face increasing challenges to ensure the information they utilise is accurate and secure.

https://datatrue.com/en/

Fraud Detection in OCR Automation



MonJa, a developer of intelligent automation for financial institutions, has added an advanced fraud detection feature into its OCR document automation software.

This feature offers automatic identification of potential fraud signals in bank statements, tax returns and other financial documents.

James Wu, CEO of MonJa, said, "In the past few months, we have detected an increased number of fraudulent or altered financial documents.

"This latest feature aims to not only to make document management easier and more efficient, but also to add a safety net against fraud.

"We want our clients to feel at ease knowing they've got this extra safeguard in place. Our company is continually working towards meeting the evolving needs in financial document analysis."

The advanced feature automatically scans and analyses bank statements and other documents for possible indicators of fraudulent activities.

It works by leveraging AI and machine learning algorithms to detect inconsistencies and anomalies that could suggest fraud, offering financial institutions an additional tool to safeguard their operations.

https://monjaco.com/

Document AI minus the 'Hallucinations'

Eigen Technologies (Eigen), an intelligent document processing (IDP) developer, has announced the global availability of its new integration with GPT. This option allows users to combine Eigen's no-code AI-powered platform with the power of GPT.

The integration means that Eigen customers can now choose to use OpenAI's GPT model alongside Eigen's proprietary machine learning (ML) for intelligent automation and document processing purposes.

Eigen users will be able to choose between using GPT, or any other large language models (LLM), as an alternative to BERT to enhance Eigen's Instant Answers and extraction capabilities.

Eigen Instant Answers enables users to build models 3x faster and is designed for users who need high-accuracy data quickly, particularly from complex documents such as contracts, reports and prospectuses.

The combined offering integrates GPT with the Eigen platform's full workflow, which enables the comprehensive management of usable data from document through to post-processing.

Critically, the optional integration gives Eigen customers the choice to use GPT where they see fit, ensuring users have full control and transparency over its use. By doing so it enables business users to overcome one of the biggest barriers to using LLMs by guarding against errors and hallucinations.

The information retrieval and prompt engineering features in the Eigen GPT integration provide additional guardrails to protect the user from these risks.

https://eigentech.com/

dtSearch updates search tools

dtSearch is releasing version 2203.01 and beta version 2023.02 of its enterprise and developer product line for instantly searching terabytes of online and offline data.

The product line's proprietary document filters cover popular "Office" formats, website data, databases, compression formats, and emails with attachments. dtSearch products can run either "on premises" at organisations or in a cloud environment such as on Azure or AWS.

The release adds a new search results display for dtSearch's enterprise products.

The beta adds sample code demonstrating use of the dtSearch Engine in an ASP.NET Core application running in a Windows or Linux Docker container.

The dtSearch Engine is a multiplatform SDK that lets developers add dtSearch's document filters and instant terabyte searching to "on premises" or cloud applications, such as on Azure and AWS.

Other features include:

Terabyte Indexer: dtSearch enterprise and developer products can index a terabyte of text spanning multiple folders, emails with nested attachments, online data, and other databases in a single index. The products can create and search any number of terabyte indexes.

Concurrent, Multithreaded Searching: Indexed search is typically instantaneous, even in a concurrent search environment covering terabytes of mixed online and offline data. For online use, dtSearch products have no limits on the number of concurrent search threads. Updating indexes to reflect new content does not affect instant multithreaded concurrent searching.

Document Filters and Supported Data Types: dtSearch's proprietary document filters support Microsoft Office files, OpenOffice files, PDFs, compression formats, emails along with nested attachments, web-ready data, and more, along with browser display with highlighted hits. The dtSearch Engine SDK makes dtSearch's document filters directly available to developers.

More than 25 Search Features; International Languages; Forensics-Oriented Search: The dtSearch product line has over 25 full-text and metadata hit-highlighted search options, with integrated relevancy ranking across multiple data repositories. Unicode support covers hundreds of international languages with special double-byte Asian character options and handling of right-to-left text like Arabic and Hebrew. Forensics-oriented options include identifying credit card numbers in data and hash value generation and search. The dtSearch Engine adds developer-oriented search features like faceted search and granular data classification.

dtSearch Engine SDKs: The SDKs provide C++, Java and current .NET APIs for Windows, Linux and macOS encompassing Apple Silicon (M1, Arm). Along with API access to dtSearch's general search features and document filters, APIs cover faceted search and granular data classification using any number of full-text and metadata parameters. The beta adds an ASP.NET Core Docker application running under Windows (NanoServer) and Linux.

https://www.dtsearch.com/

Hyland enhances Content Services

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/

Enterprise Recon 2.9.0

Ground Labs has announced the general availability of Enterprise Recon 2.9.0. The latest version of this sensitive data discovery solution delivers improved data risk scoring capabilities along with security and functionality enhancements in addition to offering new personal data types and maintenance updates.

Enterprise Recon helps organizations to discover, manage and remediate all types of business critical and sensitive data to meet their security, privacy and compliance objectives. Enterprise Recon enables compliance with a wide range of international data protection and privacy regulations including GDPR, PCI DSS, CCPA, CPRA, HIPAA, PDPA, PIPEDA and CDPA.

Key new features and benefits of Enterprise Recon 2.9.0 include the following:

Enhanced Data Risk Scoring: Enterprise Recon's risk scoring capabilities have been enhanced to leverage custom data type patterns. This extends its capability beyond the 300+ standard personal data patterns to virtually any data type that the client wishes to now create through Ground Labs GLASS Studio. Enabling management of intellectual property, custom data for mergers and acquisitions, organization specific PII and more.

New Global Data Types: The ability to scan and remediate locations that store unsecured mailing addresses and PO Box addresses in Singapore, and Singaporean passport numbers, supporting compliance with the Personal Data Protection Act (PDPA) and other related data privacy regulations.

IBM AIX Data Discovery Update: Support for AIX is a long-standing unique feature of Enterprise Recon. The ability to install natively on AIX and directly discover data on the local filesystem will greatly benefit IBM customers with updated AIX version support.

Early Access Features: Available for usability and performance feedback, Enterprise Recon 2.9.0 now supports improved support for Box Cloud Storage in addition to Apache Hive databases.

www.groundlabs.com

Digital Evidence Analysis with AI+

UK based Detego Global has expanded its range of winning digital forensic software solutions with the release of Detego Analyse AI+. This latest offering incorporates state-of-the-art AI technology to empower investigators and accelerate the analysis of vital evidence.

Analyse AI+ unveils a suite of cutting-edge tools, such as AI-powered semantic search, rapid identification of similar images and patterns, lightning-fast AI audio/video transcription and the real-time translation and transcription of audio and video evidence.

Alongside these features, Detego Analyse AI+ offers advanced AI-powered object detection, multi-language OCR (Optical Character Recognition) and off-line document translation from over 230 languages to English.

Among the key features of Detego Analyse AI+ is the advanced semantic search which helps investigators save hours of manual data sifting by leveraging AI to search for broader concepts and contexts within images and videos. This tool significantly reduces the limitations of keyword searches.

It helps investigators pinpoint any advanced concepts such as "men in masks with automatic weapons in London at night", "drug deals in a black sports car belonging to a specific brand", "screenshots of customer account details", "distressed children" and "uniformed teams holding flags with terror-related symbology".

The solution also provides investigators with the ability to swiftly scan evidence for similar images by uploading a reference image or by utilising the "show similar" feature on existing images – helping accurately match specific locations, signs, movements and objects as well as unique patterns or designs in tattoos, wallpapers, graffiti or clothes – all in a matter of seconds.

Detego Analyse AI+'s rapid AI transcription functionality accurately transcribes and indexes words from a wide range of audio and video files including voice notes, voicemails, video messages, and social posts and stories, recording transcription speeds well over 1,000 words per minute.

This in turn helps eliminate the need to manually review hours of audio/video recordings and helps investigators to identify data that's related to investigations by using advanced text and keyword matching capabilities on the data indexed from any audio and video files.

Cross-border/international investigations are also further strengthened with the new AI-powered translation capabilities. In addition to the off-line document translation capabilities from over 230 languages to English through Detego Analyse, Analyse AI+ allows investigators to translate and transcribe audio/video content from over 50 languages, including Arabic, Swahili and Russian, to English in realtime.

Analyse AI+ also allows investigators to uncover hidden files using enhanced compound file steganography, delivers improved evidence management features and provides users with enhanced tag management capabilities for better organisation and control of evidence. Users can now save filters to specific exhibits or make them available across all exhibits, ensuring seamless and consistent filtering across investigations.

The new release also intoduces various other enhancements, including optimised video frame processing, improved support for GrayKey extractions, and greater support for MSAB imports stemming from the technological partnership with MSAB that's gone from strength to strength.

https://www.detegoglobal.com/

FileInvite Launches Free Plan

NZ firm FileInvite has made available a free plan for its secure document collection software to help businesses streamline their information collection workflows.

The company says it is the first free plan in the document collection software category, and allows users to explore the secure, time-saving application at their own pace.

The company is SOC2 Type II-certified and compliant with GDPR, HIPAA, and FERPA standards. Its enterprise and bank-grade security is maintained across all offerings, including the free plan, enabling all users to confidently and securely collect sensitive information.

"We're excited to break down barriers to technology adoption and make our efficient document collection solution accessible to everyone with our free plan," says James Sampson, CEO of FileInvite.

"The entry-level option can easily scale up to support high request volumes and meet the needs of complex workflows, providing new users with a risk-free way to try out the secure solution for requesting information."

FileInvite aims to transform the document collection process, making it faster and more efficient.

This solution is designed for document-heavy workflows and regulated industries such as banking, lending, accounting, education, and legal services.

With FileInvite, users can easily and securely request and receive documents, saving time, improving operational efficiencies, and enhancing customer experiences.

https://www.fileinvite.com/

Process Automation for Insurance

The newly-released expert.ai Platform for Insurance powers underwriting and claims solutions so that insurers can use natural language processing to eliminate documents from review cycles, extract needed data and prioritize which submission or claims need an expedited review or to be assigned to a senior adjuster based on complexity.

It provides insurance teams with a way to automate the repetitive tasks associated with document reviews, extraction and assessments, freeing up time to focus on de-risking underwriting decisions, determining coverage and conducting preliminary claims investigations.

Key platform capabilities include:

• Out-of-the-box data extraction for common data fields

• Urgency, severity and intent routing for claims and submissions packages

• Extraction of key exposure factors, e.g., coverage exclusions, limitations, pre-existing conditions, etc.

• Accurate summarization for human review, e.g., pre-assignment of risk grades for human validation/ evaluation from property risk engineers

• Data redaction for GDPR and PII (personally identifiable information), etc.

• Record type categorization and elimination of records from review cycles

• A customizable insurance-trained language model

From submissions and claims management through policy comparison and risk engineering, the expert. ai Platform for Insurance supports even the most intricate, complex and language-intensive uses cases.

The expert.ai Platform for Insurance supports:

Risk Engineers: automate scoring and unintended exposure, and identify policy inconsistencies for commercial building insurance

Metrics Impacted:

• Increase review capacity by 4X

• Automate risk scoring across 10 key categories

Underwriters: expedite policy review, comparison and routing based on underwriting triage guidelines, reducing leakage and risk exposure while ensuring coverage certainty and standardization

Metrics Impacted:

• Generate quotes 50% faster

• Save 2 hours on every policy review

• 24×7 coverage of submissions across channels

Claims Handlers: automatically extract critical content needed to accelerate claims processes and enable subject matter experts to focus on high-value tasks

Metrics Impacted:

• Reduce claim review times by 50+%

• Improve objectivity and accuracy

• Reduce document review times by 90%

"At expert.ai, we've deployed insurance solutions for Global 100 providers across the range of workflows from claims automation and risk engineering through policy reviews and submissions intake. Artificial intelligence, in fact, offers insurers tremendous potential to transform their operations, improve combined ratios and establish a lasting competitive advantage," said Walt Mayo, expert.ai CEO.

"The expert.ai Platform for Insurance provides AI-based NLP solutions to reduce time to production and scale in the future. From customizable language models to insurance use case trained models, we help insurers deliver real value across their organizations, with high levels of accuracy, significant time savings, tangible capacity gains and better customer engagement."

https://www.expert.ai/

AI-Powered Document Classification

OneTrust has launched artificial intelligence (AI)-driven document classification to help organizations more accurately and completely identify and classify unstructured data and automatically apply governance and protection policies.

"An organization's data is what fuels innovation and gives them a competitive edge," said Blake Brannon, Chief Product and Strategy Officer at OneTrust.

"Yet, data sprawl and lack of visibility into where sensitive data lives across the organization can quickly turn that data into an Achilles' heel, risking the financial and reputational impacts of breach and increasingly important data misuse.

"Using AI to classify unstructured documents at scale, organizations can automatically apply the right policies to protect their data and become more data-driven, knowing data is being used responsibly across the business."

OneTrust's AI-driven document classification capability:

Analyzes full file content and context: OneTrust uses AI to analyze the entire context, patterns, and terms within an unstructured file to not only identify the terms and classifications in the file, but also the type of file. Common examples include resumes, financial statements, source code, and medical records.

Automates data policies such as data retention: Many retention requirements are targeted to specific types of documents, such as resumes and medical records. Tagging documents according to this full context, not only the terms found within, better enables organizations to understand which retention policies apply and automate remediation actions such as deletion and redaction.

This capability joins a number of powerful identification and classification capabilities available through OneTrust Data Discovery:

■Named entity recognition (NER) identifies exact named entities such as people, organizations, and locations within unstructured data.

■Optical character recognition (OCR) AI models extract characters from images, including printed or handwritten text.

■Security classifiers for API keys for AWS, Azure, and Google, plus encryption keys and secrets, passwords, and usernames reduce the risk of exposure through a data leak or breach.

■Regulatory intelligence enhances jurisdictional insights by correlating classified personally identifiable information (PII) with applicable laws and regulations, such as CPRA.

OneTrust Data Discovery is part of the OneTrust Privacy and Data Governance Cloud which offers one platform for security, marketing, and privacy teams to discover, control, and activate the responsible use of data throughout their organization.

BPM With GPT

OpenBots has launched its new upgrade, Version 2.1, a fully integrated and bundled Business Automation Platform suite with robust Intelligent Document Processing with GPT, along with its core Robotic Process Automation suite.

"OpenBots Documents with GPT replaces traditional and proprietary ML models and training interfaces by utilizing Large Language Models like GPT and LLaMA as next-generation AI Technology to extract and classify information.

"OpenBots Automation and Documents allow digital workers to extract data from structured and unstructured documents and use them in line of business applications," said Ashish Nangla, CTO at OpenBots.

Intelligent Document Processing (IDP) has been widely fragmented for several reasons. Most vendors use proprietary machine learning models that require significant implementation and training, but even with that effort, the accuracy and effectiveness of most IDP products are simply not there.

Some vendors have tried to focus on industry segments or sub-segments to train their ML models more effectively, which has increased accuracy levels.

The new OpenBots 2.1 uses Microsoft Azure's GPT technologies to extract and analyse data from documents such as invoices, contracts, and forms. OpenBots Documents is used in various industries, including healthcare, finance, legal, banking, and other institutions with a high volume of document transactions.

"A process that used to take months training IDP models is now reduced to minutes, and the accuracy increased to over 95%," said OpenBots' CMO, Gilberto Marcano.

OpenBots offers a free 30-Day trial for users who want to test the technology with their own documents. Plans start at $US99 per month for individual users, $US999 and $US1,999 per month for medium and larger companies.

Learn more at https://www.youtube.com/ watch?v=m1m7yCfKRLc

Pega Generative AI added in workflow

Pega GenAI is a new a set of 20 new generative AI-powered boosters to be integrated across Pega Infinity '23, the latest version of Pega's low-code platform for AI-powered decisioning and workflow automation.

For example, a bank looking to automate their loan processing operations would traditionally need to start by identifying, designing, and developing dozens of workflows from scratch. With Pega GenAI, they simply tell Pega they are building a "loan processing application," and Pega will automatically create the related workflows, data models, user interfaces, sample data, and more based on responses from generative AI models like those from OpenAI.

Because the responses from generative AI are mapped directly into Pega's model-driven architecture, low-code developers can easily configure and change these suggested starting points to rapidly deliver a completed application. Pega GenAI boosters like these will be infused throughout Pega Infinity, allowing users to accelerate their low-code application development, enhance customer service, and improve customer engagement.

A new API abstraction layer, called Connect Generative AI, will allow organizations to get immediate value from generative AI with a plug-and-play architecture that allows for low-code development of AI prompts. Rather than directly calling OpenAI, or other APIs directly from UIs or workflow steps, Pega uniquely provides an API abstraction layer so developers can easily swap out large language models running on both public and private clouds and build reusable generative AI components that can be leveraged across applications.

Connect Generative AI will be able to automatically replace personally identifiable information (PII) data with placeholders in generative AI prompts, helping organizations enforce their data protection policies and advancing secure use of public and private models.

Generative AI powered boosters in Pega Infinity '23 facilitate rapid development of innovative new capabilities and give low-code developers the power to infuse generative AI functionality into decision-making and workflow automation.

As large language models, cloud services, and data privacy needs continue to evolve, this "AI choice" architecture allows Pega and its clients to continuously innovate new secure solutions. Pega will initially offer connectors to OpenAI's API and Microsoft Azure's OpenAI APIs and will be supplemented by additional downloadable connectors to other providers on Pega Marketplace.

https://www.pega.com/technology/generative-ai

Indico Data integrates Azure OpenAI services

Indico Data, a developer of intelligent intake solutions for unstructured data, has announced the launch of its integration with Microsoft Azure OpenAI Service. This extends Indico's Enterprise Large Language Model (LLM) capabilities using the latest in generative artificial intelligence (AI).

Initial use cases will focus on enabling insurance carriers to dramatically increase underwriting and claims intake capacity and improve processing efficiency.

The first product enhancements to be released will include the Indico Prompt Studio and Summarization Studio. Both features take advantage of Azure OpenAI Service to allow users to accelerate the ease and speed at which they can automate processes, in some cases going from days to hours.

Integrated with Indico's patented Intelligent Intake application interface, Indico's Prompt Studio will fully automate the creation of custom machine learning models by just describing with a simple text prompt the desired data elements to be classified and extracted from the submissions related to claims, underwriting, and policy servicing.

This accelerates machine learning model creation from days to minutes, accelerating customer time to value. For data security, these models are then converted to use Indico's Enterprise LLM entirely within the customer's firewall.

Indico's Summarization Studio integrates with Azure OpenAI Service to extract claims and policy data and present a summarized view of all related policy details to the analyst. The summarized view supports decision making and points out anomalies in an effort to expedite "covered or not" decisions.

By utilizing state of the art machine learning, users are now able to "interrogate" submitted documents and produce summary data that typically take hours to research and create manually.

Looking into the future, Indico also plans to enhance its workflow canvas with a variety of no-code features through Azure OpenAI Service, enabling users to customize Indico workflows to meet their specific business needs without requiring custom coding.

http://www.indicodata.ai/

Cybersecurity Incident Response

Kyndryl has unveiled a Cybersecurity Incident Response and Forensics (CSIRF) service to help customers proactively prepare for and respond to threats by applying the latest threat intelligence and experience from Kyndryl's deep domain security experts.

The new service helps customers investigate and respond to a detected security incident by leveraging capabilities such as incident triage, incident response, threat intelligence, compliance monitoring and management. Customers may also select proactive services that may significantly reduce the time to respond to an incident.

Kyndryl's CSIRF service provides integrated and seamless incident response (IR) support, forensics, and recovery capability to help customers analyse, identify, compare, and understand the evidence and causes of a cyber incident. In the event of an occurrence, such as ransomware, Kyndryl's CSIRF experts provide on-demand, hands-on support to assist in resolving threats to a customer's business.

The new CSIRF service complements Kyndryl's Recovery Retainer Service, which is designed to help customers recover and rebuild their environments after catastrophic events. When coupled with the Recovery Retainer Service, CSIRF provides on-demand availability of qualified experts that can effectively help customers recover from and mitigate the impact of cyberattacks.

https://www.kyndryl.com

No Code Process Automation + AI

Pipefy has announced the upcoming release of Pipefy AI, a technology that combines artificial intelligence with Pipefy's no-code process management and automation platform.

Pipefy AI enhances process management efforts by delivering crucial data insights and accelerating the speed at which processes can be built. The result is better decision-making and greater operational efficiency throughout the enterprise.

Pipefy AI harnesses the power of OpenAI and GPT-4 to enhance data analysis and help teams model and optimize any type of process.

With Pipefy AI, users will be able to ask any question about their current processes or data sets and receive an answer in seconds. To complement its data analysis capabilities, Pipefy AI also helps users complete a wide range of previously manual tasks.

Another core component of Pipefy AI is its ability to create custom processes based on the parameters and requirements set by the requester. Its goal is to build the most efficient version of the user's process for them, every time.

Users simply tell the AI what kind of process or workflow they need, what kinds of data they want to collect, and any other characteristics they'd like it to have - Pipefy AI does the rest.

https://www.pipefy.com/

Kyndi adds Generative AI

Kyndi has announced several new enhancements to its natural language processing offerings, including advanced generative AI capabilities, enhanced analytics, and automated query suggestions.

These enhancements expand on Kyndi's existing Answer Engine and generative capabilities, enabling enterprises to provide direct, accurate, and trustworthy answers to customers and employees instantly for improved decision-making, efficiency, and productivity.

Kyndi's generative AI-powered Answer Engine is designed to revolutionize the way employees and customers find answers to their queries. With enhanced capabilities built into Kyndi's award-winning products, including Kyndi Natural Language Platform and the two applications built on top of it, Kyndi Clarity and Kyndi Natural Language Search, enterprise users can now receive direct and trusted answers rooted in enterprise content, every time they have questions about a business.

By combining embeddings, LLMs, generative AI, and vector and semantic databases on the same secure platform, Kyndi's generative AI-powered Answer Engine offers an end-to-end solution that saves companies time and costs from developing and managing separate technologies.

Unlike ChatGPT and traditional search engine tools, Kyndi's Answer Engine is an enterprise-class, complete solution that provides immediate and trustworthy answers in a secure environment as answers are generated solely from enterprise content. Data privacy measures such as GDPR and CCPA are built into Kyndi's Answer Engine to ensure no customer data is compromised. With Kyndi, users get one correct answer instead of a long list of results they have to sift through to find the exact information they seek and there is no misinformation in the results.

"Unlike other offerings, Kyndi's generative AI-powered Answer Engine offers users accurate answers from trusted content that is explainable and easy to run in an enterprise environment," said Ryan Welsh, founder and CEO of Kyndi.

"Our vision has always been to provide organizations of any size, and in any industry, with a complete solution that integrates components necessary for building a state-of-the-art answer engine. Not only does this improve the customer and employee experience and support a true digital transformation, but it reduces costs significantly and can be deployed 9x faster than other offerings."

https://www.kyndi.com/