

legal*i* insider

Top stories in this issue...

- ▶ David Lumsden to take over as Enable CEO, p.2
- ▶ Elite EMEA sales head Peter Gill to join Converge TS, p.3
- ▶ Cripps promotes Jo Owen to newly-created CIO role, p.3
- ▶ Diversity challenge: Play your (small) part, p.4
- ▶ Neota: UK accounting losses are "entirely normal", p.4
- ▶ Accenture Cyber Roundtable: How much is enough? p.6
- ▶ Adventures in the Pessimistic DMS Garden, p.12
- ▶ iManage and HighQ conference reviews, p.21+22

▶ LITI launches CyLok - the Legal Cybersecurity Readiness Index

Legal IT Insider has been working with industry security experts including Accenture as well as a number of CIOs in order to develop and now soft launch CyLok, an interactive tool that allows contributing firms from across all segments of the market to compare their security setup against industry benchmarks and understand their CyLok cyber-security rating. Our research is on-going and we plan to release a regular report on the benchmark and LITI CyLok Index, with comments from key experts.

Our longer-term ambition is that, with engagement from corporate counsel, the LITI CyLok Index may ultimately reduce the level of work required by law firms to prove their security credentials to clients in RFPs and audits.

We are grateful to the law firms from across the range of UK Top 100 firms that have already completed the Index, from which we can provide some exciting early insights. All results are anonymised and for the firms that are early contributors and adopters of the LITI CyLok Index, we will be sharing with them insights on their rating by segment. Based on the research, we will release general insights to help all firms improve their security.

The trends

Towards the end of 2017 we hosted a cybersecurity roundtable in conjunction with Accenture (see page 6), in which Kelly Bissell the global head of security at Accenture, set out a number of cyber best practices that were incorporated in the index and against which we can benchmark the early results against.

Cyber spend

According to Bissell, firms playing 'catch up' with their cyber capability ought – as a very rough guide – to be spending anything from 10% to 20% of their overall IT spend on security.

For firms that are mature in their security, that figure should be around 3-5% of their overall IT spend.

The majority of firms that have completed the CyLok survey spend 10%, with the range of spend between 5% and 30%.

As set out by Bissell, there is a visible correlation between spend and existing capability.

Background checks

Bissell was visibly astounded that any law firm would hire staff without a background check, which in the legal sector has only recently become common practice.

It is encouraging that all of the law firms that completed the Index undertake personnel background checks.

LITI LAUNCHES CYLOK – THE LEGAL CYBERSECURITY READINESS INDEX CONTINUES ON P2

▶ Accenture cyber roundtable - out now!

Don't miss the write up of our cybersecurity roundtable, hosted in conjunction with Accenture, where Kelly Bissell, the global head of security at Accenture, laid out some best practices for law firms.

Legal IT Insider brought together a handful of high profile CIOs or COOs from firms including Dentons; Baker McKenzie; Clyde & Co; Herbert Smith Freehills and Ashurst to discuss some of the biggest security issues facing the legal industry today, and to get input into the datapoints needed for our LITI CyLok Index. See page 6 for more.



Proclaim® is the only Practice Management Software solution
Endorsed by the Law Society.

CALL
01274 704 100

lawsociety@eclipselegal.co.uk



ECLIPSE
Part of Capita Plc

► LITI launches CyLok - the Legal Cybersecurity Readiness Index

CONTINUED FROM FRONT PAGE

Multi-factor authentication

Over 75% of the firms that completed the CyLok Index have implemented two-factor authentication, which is an encouraging early result.

Automatic patching

Within CyLok, we ask if software updates and patches are installed automatically.

Bissell, in our roundtable, said: "I sat a dinner in London on a table no different to this with the head of GCHQ, the head of National Cyber Security Centre, the former head of MI5 and MI6 and some other people and we all agreed that most of the attacks we see are still elementary such as systems that are not patched. We better move our mentality from patch when you can to 'you better patch now' even at the risk of breaking things."

In a big shift for the industry, 100% of firms surveyed answered 'Yes' to the question above.

A restricted matter/document management function

Pessimistic or 'need to know' security – under which access to the document management system is restricted to those involved in a case or transaction is coming, like it or not. However, early indicators point to fewer than a quarter of firms reporting that they have enforced a pessimistic DMS model.

Firms' main concerns centre on the inability to maintain security and also share knowledge but, speaking in our roundtable, Bissell said: "This also has been solved. McKinsey is superb at knowledge management but protecting client confidentiality."

Please contact cylok@liti.co.uk for further details.

► Legal tech win

Dutch specialist litigation firm, bureau Brandeis, has awarded the implementation contract for NetDocuments to Hoffbrand Consulting.

Paul Hoffbrand tells us: "We have been awarded this contract because of our previous work in The Netherlands with a Dutch Government agency and will be another European implementation for us. I am looking forward to this project being as successful as all the others we have done since 2015."

► David Lumsden to take over as Enable CEO

For those with a long legal tech memory, history is just about to repeat itself, when David Lumsden, who was chief executive of RAVN Systems until its acquisition by iManage, takes over as CEO of Enable Business Solutions from founder Liam Flanagan in July. Flanagan, who retains majority ownership, will take on the role of head of business development and innovation.

The appointment is a near repeat of when Lumsden took over in around the turn of the century as CEO of Tikit, which was co-founded by Flanagan. He led Tikit's float on the AIM London Stock Exchange in 2001.

Enable, which Flanagan founded in 2013, has two core products: Word-based pitch building tool PitchPerfect and new solution ExperienceManager, which enables marketing professionals and lawyers to capture experience across the firm by integrating with existing matter systems. Clients that have signed up to ExperienceManager include Stibbe, which in April became Enable's first mainland Europe client.

Flanagan told us: "We're now a mature startup and I'm bringing in the next line of executives to take the business to the next level." Enable has a significant number of investors, of which Lumsden is one.

Lumsden told us: "What Liam is good at is thinking what the product needs to do - he created this product out of nothing and they have a few really big clients all happily using it. He should continue to do that because he has far more knowledge of what the product needs but he won't be focused on running the business day to day.

"The next stage is probably going to be more structured; less on Liam's entrepreneurial skills and more on my structured approach, which means he can continue to do his entrepreneurial thing."

Enable has just under 20 employees and Lumsden says: "I really hope I can help the company grow because the people working there are lovely. Cath Thompson is really organised, which is just what I need!"

► Talking Tech interview with Neil Araujo

Keep an eye out in the next few days for our on camera interview with Neil Araujo, CEO of iManage, which we filmed at London ConnectLive 2018, covering a range of topics including whether the strategy for RAVN remains the same a year after its acquisition.



► Elite EMEA sales head Peter Gill to join Converge TS

Thomson Reuters Elite's EMEA sales head Peter Gill is to join Converge Technology Specialists (Converge TS) as chief commercial officer, we can reveal, as the dedicated legal cloud provider builds up its c-suite in preparation for the next phase of its growth.

Gill, who takes a position on the Converge board alongside CEO and founder Nigel Wright, has previously held senior sales roles at Advanced Legal, Wolters Kluwer and LexisNexis, as well as founding professional services business development consultancy Boreas Partnership.

He starts on 4 June and will be responsible for driving the growth of the business, which in January received investment (the sum was undisclosed) from mid-market investor Tenzing Private Equity.

Tenzing targets high growth UK-based companies with an enterprise value of between £10-50m. Converge TS has achieved over 50% revenue growth year on year in the last three years.

Speaking to Legal IT Insider Gill said: "One of the key advantages is that Nigel is driven and Converge has the ability to be really agile when needed. You can talk to Nigel about things and a day later he'll call and say 'Guess what, we're doing it now.'"

He adds: "I'll be responsible for the overall UK sales number, which I am at Thomson Reuters for EMEA." However he adds: "As a board member I'll be responsible with the other members for the P&L; I didn't have that at Thomson Reuters." Gill will also be directly responsible for marketing, which he describes as "an agile team".

One of the key attractions of working for a smaller company, Gill says, is that he will get to help shape the business. "Nigel has said that he wants me involved driving and improving the business alongside other board members," he said. Converge is currently in the process of hiring a chief financial officer.

The timing is also right in the market. Gill says: "Small firms have been adopting cloud whether be SaaS or IaaS or PaaS for a while but larger firms are now much more open to cloud in whatever that form that might be and Converge has been positioning itself as a leader in legal and partnering with Thomson Reuters, LexisNexis and BigHand. It's the perfect storm: get this right and you can really drive growth and adoption."

As for why Gill has left Elite, he says: "There are edges and boundaries that you have to work in. I've worked in big

businesses before but I've also set up my own business and had to win business, deliver, invoice and debt collect and do the accounting. I loved that and but for the recession might have still been doing it. So the whole flexibility thing is fabulous and Converge is the closest I'm going to get to that. With Nigel at the helm, with his focus and attitude, we have the potential to achieve something quite special."

Converge is known to looking at further organic growth but also strategic acquisitions. Watch this space.

► Cripps promotes Jo Owen to newly-created CIO role

Our congratulations goes out to Jo Owen who has been promoted from operations director to the newly-created role of CIO at Cripps, as the Sussex practice carves out a dedicated IT function.

Owen, who has become a divisional head with a seat on the partnership board, takes over responsibility for IT from Cripps' former chief operating officer and director of innovation Christina Blacklaws, who this year took over as vice president of the Law Society. Within Owen's team of 65 is a centralised Legal Professional Team, which includes project paralegals and document production.

Cripps has two boards: the partnership board and the operations board, with the former responsible for the strategy for the firm.

Former IT director Mike Burton has been promoted to chief technology officer and will report to Owen instead of chief financial officer Adrian Jennings. Owen said: "Mike lives and breathes the technology, makes sure everything works and I am focusing on furthering the business strategy. Our skills complement and work well together."

She told Legal IT Insider: "Our focus is on driving efficiency and achieving quick wins from business process reengineering, using technology to do that." Cripps, which has yet to go live on Peppermint Technology, will be looking at software including BigHand to help further streamline its workflow.

Owen was CIO at Vertex before it merged with Cripps in 2013, when she became deputy head of IT, moving to Clyde & Co as head of IT service delivery in 2014.

Founder of NextUp Events for future IT leaders, which is delivered in conjunction with Legal IT Insider, Owen told us: "It's been my ambition to get back to a CIO role. As CIO at Vertex I was invited to networking and support events but when I didn't hold that title any more I was effectively uninvited – I was ops director and it still wasn't enough."

► **Neota: UK accounting losses are “entirely normal”**

Neota Logic has filed its UK arm's unaudited accounts for the financial year ending 31 July 2017, showing accumulated losses of £528,712.

Sole UK director John Lord, who alongside Michael Mills co-founded Neota, which is based in the United States, is down on the accounts as lending Neota UK the shortfall. At the end of the year ending 31 July 2016 there was a balance due to him within a year of £225,755. That has now been replaced by a longer-term loan with no repayment plan or interest, totalling £628,755.

Neota expanded into the United Kingdom in 2015 with the appointment of Greg Wildisen as international managing director.

Wildisen told us: “As you and most of your readers will know, Neota is a US headquartered business and these accounts relate only to the UK trading entity.

"The accounts relate to the second year of trading and the first FULL year of trading for Neota Logic Ltd.

"We are a high growth tech company which grew in excess of 400% last year. We continue to prioritise customer acquisition and success and invest accordingly as part of our global expansion. This is entirely normal for companies at the same stage of business growth."

► **Diversity challenge:**
Play your (small) part

Lack of diversity is an issue faced by the entire legal sector but within legal technology appears to be getting worse not better, with, for example, the number of female CIOs dropping, not increasing each year.

On 10 May Legal IT Insider with help from DLA's former CIO Daniel Pollick gathered a small, like-minded group of CIOs and vendors to help us frame a diversity initiative and form the beginnings of a support group to help promote and improve diversity across the sector.

Present at the inaugural meeting were Pollick and Legal IT Insider editor Caroline Hill, plus Abby Ewen from BLM; Samia Rauf and Kaye Sycamore from Intapp; Julie Berry from RPC; Thereza Snyman from Baskerville Drummond; ex BLP IT director Janet Day; David Aird from DAC Beachcroft; and Jo Owen, newly made up CIO from Cripps.

We heard from Mitra Janes, head of diversity and inclusion at DLA Piper, which was kind enough to host us. It's fair to say that everyone at the meeting came away extraordinarily inspired and motivated to play our small part in effecting change.

Janes gave us a no-nonsense talk: formerly at Ford, she spent the past few years trying to attract girls into the

engineering sector, so she is not new to a challenge.

First off, she explained what diversity really means in all its different guises. She told us: "People who don't fit cultural norms are often excluded. It's not just about what's above the water line – gender and sexuality etc – it's about beliefs, language, values, life experience, sexual orientation, and we need to focus on all of those things and bring them together."

Janes showed us these word clouds – take a look and see what you think they relate to before you read on.



They are the words used in adverts targeted at girls and boys. Whereas boys are given “battle” and “heroes”, girls get “magic” and (more worryingly) “perfect.”

"If you're speaking to girls by the time they are 13 it's too late," Janes said. "If girls are doing technology it's usually home economics. We need to work at this for the long game."

Trying to 'fix' women with special interventions and mentoring suggests that there is something wrong with them but "girls outperform boys at every stage of school," Janes said.

“What do you look for when you’re recruiting? How do you decide who gets what work? Don’t just focus on the outcome, we must address the systemic issues,” Janes said.

Gender reporting across the UK, which has been sparked by legislation that forces organisations to declare their pay gap, looks at who earns the most in an organisation. "They now know men dominate the highest paid professions and women dominate the lowest, well congratulations," said Janes. "What are the highest paid roles and what percentage of those are men?"

“Organisations need to do a deep analysis to work



LINK App

Edit, annotate, redline, search, send
DMS, Outlook, Word



Watch our
2-minute
video

out where are the points that affect the talent pipeline," she said.

In the here and now, we need to look at the language we are using to attract women in particular.

"Among nursery children who are given tubes and margarine tubs and asked to build a bridge the boys get stuck in but the girls hold back and it seems they are uninterested," said Janes. "But if you give it context and purpose and say 'we need to build a bridge to get to the hospital or the shops' they respond to that. It takes fine tuning around the language."

That translates into the way law firms and vendors advertise for positions, which are often inadvertently male in their language.

"Look at the job titles you use and go for more neutral titles, so 'manager' rather than 'programmer'. Ask yourself 'what's my inclusion reach?' Why say 'energetic' or 'dynamic' if you mean 'enthusiastic' and 'passionate.'"

Textio is a useful tool that analyses if job posts are gender neutral and Janes said: "Be clear with the agency you use and tell them that you are serious. Ask them how this is a diverse list of people. You're telling them that this is important and that you are holding them to account."

Collaboration is important and we are collaborating on diversity initiatives with Legal Week and Legal Geek among others.

Most importantly Janes said: "Each individual needs to commit – what are you going to start doing differently? It can be very small but you need to be personally accountable."

So, we are keeping it simple: each of us present at the first meeting has made a pledge that we must keep and we invite you to join us. The group is there not to compete with others but to unite, support and connect.

We have formed a LinkedIn group and would love other like-minded people to join and pledge one thing that you will do in the next month or so; be that talk to your local school about your job; check that your advertising is neutral and change it if it isn't; or refuse to sit on a panel if it is comprised only of men (and preferably help to get women involved.)

Janes warned us: "Don't try to boil the ocean," and she has a good point. But we will be arranging for more talks by the likes of Janes and while we might not boil the ocean overnight, we're going to try bloody hard to create a few bubbles.

► Vizlegal grows caselaw repository

Vizlegal is making progress in its ambitious bid to create a global repository of indexed and structured legal judgments and filings, with UK Upper Tribunal (Tax & Chancery) decisions now converted from PDFs to searchable and easy-to-read HTML.

Unlike in the United States, where the likes of Lex Machina is making great strides in applying legal analytics to centrally stored and widely available legal decisions, in the UK and Ireland, judgments and statutes are disparately stored and can be difficult to access and track.

The recent Upper Tribunal decisions supplements Vizlegal's other recent sources:

- UK First-Tier Tribunal (Tax) decisions since inception
- Ireland Tax Appeals Commission decisions since inception
- Ireland Information Commissioner decisions since inception
- European Court of Human Rights decisions since inception

Right now Vizlegal, which in 2016 secured €30,000 at NDRC's Investor Day sponsored by Bank of Ireland, is working on allowing Irish practitioners to track Circuit Court Diaries and says it is open to suggestions on what to work on next. NDRC invests in early stage start ups and its Investor Day involves startups pitching, Dragons Den style, to a panel of investors.

► Elevate acquires E-STET

Elevate has announced its acquisition of the assets of U.S.-based e-discovery company E-STET, bringing Relativity in-house. The eagle-eyed among you may have been left wondering about the details of the deal because EY announced in November that it had acquired E-STET and the E-STET team joined the EY eDiscovery team. We asked for some clarification and it turns out that Elevate has acquired E-STET's infrastructure and a number of customers who opted not to transfer across to EY. Vice president of legal services, Kunoor Chopra said: "Alongside our partnership with cloud e-discovery technology provider, Everlaw (which will continue after this acquisition), Elevate's litigation support business has offered Relativity through a partnership with E-STET over the past five years. This acquisition allows us to provide those services in-house now."

► Accenture Cyber Roundtable: How much is enough?

The days of law firms needing to be reminded of the importance of investing in appropriate cybersecurity solutions or how much of a target they are have long gone, but greater awareness has not been matched by greater clarity over how much is 'enough', when the risks are sky high, but the budget is finite.

In a roundtable discussion hosted in conjunction with Accenture, Legal IT Insider brought together a handful of high profile CIOs or COOs from firms including Dentons; Baker McKenzie; Clyde & Co; Herbert Smith Freehills and Ashurst to discuss some of the biggest security issues facing the legal industry today, and to get input into the datapoints needed for a cyber benchmark for legal industry (see front page). We were privileged to have at the meeting Kelly Bissell, the global head of security at Accenture, who prior to our gathering was at a not dissimilar dinner with the head of GCHQ, the head of National Cyber Security Centre, and the former head of MI5 and MI6.

Setting out some of a few objectives at the outset of the discussion, Marcel Henri, global CIO at Dentons said: "I've been at Dentons for nearly 18 years and obviously a lot has changed during that time. At Dentons at present we have around 15,000 lawyers around the world, which inevitably presents challenges and opportunities, not least from a security and data privacy standpoint. What I'd like to get out of today is some kind of scorecard or rating with a number of baseline requirements so that we can assess the degree of sophistication and maturity of security platforms."

Haig Tyler, CIO at HSF, said: "For me it comes back to the fact that we need a technology operations baseline of what is good enough. In terms of managing infrastructure security, those sorts of things are pretty well defined. But the whole pushing out into the cloud is an area where I'd love for us to be able to define some more comfortable benchmarks, baselines and approaches."

Leading cyber solutions and employees such as chief information security officers (CISOs) do not come cheap – why would they in the current environment? But for CIOs trying to convince their boards to raise levels of investment it isn't easy and the focus has shifted from building castle walls to how to prevent or pick up the pieces when the next member of staff falls for a phishing attack.

At Ashurst, outgoing global IT director Bruna Pellici said: "[Cyber] doesn't come cheap: it's expensive and how do we fix the gaps with technology when people are still your weakest link?"

While lawyers are among some of the brightest people on the planet, many are notoriously uncompromising and still put the need to act quickly ahead of security considerations. Chris White, global CIO of Clyde & Co said: "The thing that always intrigues me working with lawyers is that they spend their lives working with highly

confidential material and if anyone should understand the nature of and the value of data it's them, but so often they don't act accordingly."

That is in spite of the fact that law firms are viewed as the soft underbelly of UK PLC; Rick Hemsley, managing director for Accenture Security Practice, reporting to Bissell, said: "Ultimately we look at the supply chain: the ecosystem around organisations become the root in to attack. If I wanted to attack an oil giant or a drug company to get market sensitive data I would attack the law firm because it will typically be far simpler than attacking the organisation itself."

Law firms have already been publicly embroiled in full scale cyber attacks as in the case of DLA Piper, or suffered leaks as in the Panama Papers that ultimately led to the downfall of Mossack Fonseca – the only surprise in that case, was that it took so long.

Gareth Ash, deputy CIO at Hogan Lovells said: "In DLA it was quite a wakeup call for all of us in the legal industry since it's the first time you've seen law firms spread across the front pages of the broadsheets and the BBC website. For me it's not just a question of 'if' but 'when', so not just defending the perimeter but how quickly can you detect something. If you are hit you want to ensure you had done as much as possible to protect yourself."

This is made no easier when client demands, which often force a certain discipline on an industry, are inconsistent. Simon Thompson, COO at Baker McKenzie said: "I've consulted and worked in a number of law firms and sometimes we will not use cloud services because the clients says we can't. But then you go to another law firm and they use cloud services but have the same set of clients."

The client

Information security starts with the client, which should be central to any assessment of appropriate risk parameters.

Pellici said: "You need to understand the type of information that you are dealing with and the markets that you are working in and consider the risk appetite of the business. You need to consider risk tolerance and how you achieve the relevant environment with the right mix of technologies, policies and procedures, governance is key. Information Security isn't only about technology."

Hemsley added: "From my experience, law firm tolerance has to be in line with the business and clients that they are working with."

The fact that clients send mixed messages means that one law firm's interpretation can be vastly different to another, particularly when it comes to cloud services, and Thompson adds: "What I'm genuinely confused about is that two global law firms can come up with two sets of answers to the same question."

Clients may refuse to entertain the idea of a law firm providing a cloud-based service when they themselves are 'in the cloud'.

Bissell said: "Not only do we have our own internal tolerances of risk, so do our clients, and clients do have



Case Management
Matter Management
Practice Management
Client Self-Serve

Online Case Tracking
Business Intelligence
CRM
Debt Recovery

Contact Us
www.linetime.co.uk
tel: 0113 250 0020
email: info@linetime.co.uk

double standards sometimes. Because they have different risk tolerance for third parties than they do themselves."

Some obstacles can be overcome via old fashioned communication and White said: "A lot of it comes down to your relationship with the client. There are certain government departments who require you to tick every single box otherwise they won't deal with you. I have come across this time and time again and where the client asks for something and you can't tick that box but you can have a discussion with them. What they are interested in is that you have thought about your cyber security in a professional manner and that you're not taking it lightly. So, if they say "Are you ISO-accredited" and we say we are not, we can say, 'however, this is what we are doing' and then they are satisfied. So, I think it's often used as an excuse."

White adds: "CIOs also need to be more robust. If someone comes and tells me that we can't go to the cloud I explain that going to the cloud is no different to bringing in any other service I'd argue very strongly that in many occasions, it's more secure."

The cost

While the amount spent on cyber must be in proportion with the overall budget, there is also now a huge cost associated with not spending enough. Henri said: "It's not just the cost of doing this, it's the cost of not doing it. We can't underestimate the marketing value of cyber security. I'm sure everyone spends a lot of time talking to clients. We're all pitching for the same panels and in my experience GCs all now want to talk about two things: predictably and security. It's not just a question of how much is enough. If you don't do it properly you are not going to win business, you're going to lose business."

Recommended cyber spend as % of overall IT spend

Firms playing 'catch up' – 10% to 20% of IT spend

Firms that are mature in their security – 3-5% of IT spend

Bissell, who specialises in breach incident response and privacy and data protection, said: "It's a big challenge in the market because if you're a big bank, they are spending a billion dollars in security and no law firm is going to do that."

Law firms spend 1-3.99% of their turnover on technology according to ILTA's 2017 technology survey, but typically the Magic Circle and large global firms spend around 4.5-5%, which is high compared to other industries and sectors.

Hemsley said: "In the consumer goods sector it will be around 2%."

Competition from cyber for that budget is growing and Bissell said: "I want to offer a couple of ranges of percentages, because if you are a law firm that just does paperwork,

nothing electronic - that doesn't exist but for argument's sake - you don't need much cyber security technology. But if you're a law firm like most of us who are really almost all electronic, then there is a percentage that you should be spending as a percentage of IT spend. And the ranges I would offer is if you've got nothing you're going to spend a lot to catch up and that's in the 10 to 15% range or even 20% of your IT spend, which is gigantic. And if you're already mature in your security then it will be lower than that, in the 3 to 5% range but those are just guidelines, because everyone is different."

Tyler said: "It's got to be case driven how you build that spend up. You can spin whatever you want with numbers and percentages and benchmarks, just go and read any Gartner paper. I just think about what we're doing now, think about the level of effort we now put into patching, which is probably a quantum leap above the level of effort four or five years ago. And multiply all those those heads and outsourced contracts and all that bit you're paying extra for because you're patching more regularly and there are a whole load of costs over and above the security costs."

Other significant added costs include the appointment within many firms of a dedicated CISO, and performing background checks, which until fairly recently was uncommon in the legal sector.

Henri said: Security spend is split across three different budgets. There's the cyber budget. The compliance budget in risk. And this year we appointed a global security officer who will be in charge of travel security and physical security. We're investing in background checks which we hadn't done previously - are we hiring the right people? Are we hiring someone with a criminal record?"

"It's still common to not perform a check?" asked Bissell. "It is becoming more common," said Thompson.

Ash added: "It's appearing on client audits too. Clients have asked about lawyers and staff all round the world. You can't do full background checks in some countries, but lawyers have to have passed the bar."

Insider threat

Even when staff are thoroughly vetted, that is no guarantee that behaviour won't slip.

Ash said: "The awareness is far better than it used to be but the partner and associate on the line just want to get the deal done and that's where the risks can arise if eg they send an email to their Gmail; it's not necessarily malicious."

The pressures of life also mean normal people do misbehave and Bissell said: "One of the main drivers of people doing bad things is the stress of marriage and financial troubles - they do things that they wouldn't normally do."

ACCENTURE CYBER ROUNDTABLE CONTINUES ON P.9

aka 'The Orange Rag'



WHEN IT COMES TO CLOUD DMS, EXPERIENCE MATTERS



When it comes to something as mission-critical as document and email management, law firms with a cloud strategy want to partner with a cloud-first provider – one that has the highest levels of confidence and experience in the security, reliability, and scalability of its native cloud platform. NetDocuments is committed to the vision of becoming the trusted cloud platform in legal and delivering world-class DMS service to firms ready to leverage the next generation document and email management service.

netdocuments®



LEARN MORE ABOUT
CLOUD DMS
www.NetDocuments.com



1.866.638.3627
UK +44 (0)20 3455 6770



Info@NetDocuments.com

ACCENTURE CYBER ROUNDTABLE CONTINUED FROM P.7

Insider trading cases have proliferated: one of the best-known examples occurred at Foley & Lardner, where former partner Walter "Chet" Little received a 27-month sentence for insider trading, after profiting from trading on corporate announcements that were yet to become public.

Hemsley said: "There are some great stats around insider risk versus external threat and one of those that was presented at a conference I was at is that 56% of breaches are caused by insiders either maliciously or accidentally. People don't typically join an organisation with malicious intent but then there are stresses that drive behaviour and it's incumbent on us to have the right cultural behaviours in an organisation to recognise where we see those risks happening to then intervene because if you intervene at that point, you minimise the chance of it becoming an unfortunate incident. Understand how your insiders are behaving. Train your people, patch what you're doing and watch what your people are doing."

There has been a real shift from building your castle walls to watching how your people behave on the inside and Ash said: "The emphasis has turned to insider threat products as someone could get in or already be in and it falls to us to be able to detect those things quickly and we're certainly looking at more investment in this space."

"The difference is that in other sectors you can mandate a lot of things and lock them down which is a challenge in a professional services firm as over 50% of the firm are lawyers and they need to be able to transact with clients."

Pessimistic security

Law firms are still deeply divided when it comes to whether they have to lock down their document management system internally, including a certain amount of division within our roundtable.

Henri, who began the process of restricting access to the DMS in 2016 said: "I'm not sure we have any choice. There's a metaphor I've used over the past few months, which is that it's difficult to get into the castle but once you're in it's a hotel and you can wander around the lobby but you once you get in, you can only get into the rooms for which you have a key. There was an article in your publication pessimistic security and I think all firms will have to go down that route."

Legal IT Insider in 2016 first floated the idea that all law firms will have to move to a pessimistic security model, thanks in large part to conversations with Henri and (separately) iManage.

At the time, the idea was met with huge resistance from UK CIOs, but since then UK top 20 law firm Bird & Bird is among those to opt for a restricted DMS approach, as we first revealed in September 2017.

Technology is evolving so that you can extract and share knowledge and experience on an anonymised basis and here Bissell shed some light on best practice outside of the legal sector, particularly among the Big

Four, commenting: "The audit firms have succeeded in not breaching client confidentiality but deriving value from that data: the Big Four have done particularly well at that."

"Using data analytic skills to say 'do we see data trends across our clients across a sector or geography' they get data scientist to look at that not auditors. So, this is where the professional services and the technology come together to bring a different value than they ever could before independently."

Henri commented: "We're doing it in two different areas and it's not a panacea but we're doing it in the credentials space so when you're pitching what's the expertise we can find for a pitch and the expertise space - when you're very big people don't necessarily know each other and you can't just go crawling through a public file you have to look at the narrative and matter descriptions and use machine learning."

However, many firms are unnerved by the impact this will have on global collaboration efforts Pellicci said: "You've got to look at how lawyers work. We're trying to create synergy between global teams and we do have information barriers if needed but how much do you really need to lock things down?"

White added: "Law firms are based on sharing knowledge and the challenge as you grow and globalise is how does the lawyer in London know what the lawyer in Sydney is doing so we're not reinventing the wheel the whole time. We've invested so much money in sharing that knowledge to then lock it all down."

Bissell said: "This also has been solved. McKinsey is superb at knowledge management but protecting client confidentiality. I do believe that knowledge management and communities of practice, whether specialist in an industry or whatever the industry is this can be solved."

Best practice

With law firms anxious to gauge best practice outside of the industry, we asked Bissell for guidance on some of the minimum cyber practices and solutions that law firms should have in place.

"Yes, we can open up that Pandora's Box," Bissell said. "Because best practice for law firm A may not be the same as best practice for law firm B and it does depend on what you have, like cloud or not cloud and those sorts of things. But I would suggest that there are some very basic, elementary things that all leading practices should have and that is:

- Multi-factor authentication, not just user IDs and passwords but multi-factor even out of bands, so text, cell phone or some other sort of function.
- A controlled matter management function, document management, so that you know who has access and who doesn't have access and then all that logging. I can't tell you how many times I have seen clients that no logging is turned on. So even when something occurs, you don't even know.
- I wouldn't waste a whole lot of time in more firewalls or more castles. It's really the detection that we have

to do and I suggest that you come up with ten and only ten scenarios. Meaning, we want to prevent X from occurring. Like, we want to prevent everyone from downloading all matters. And I'm just making up stuff, right? And then create the protective and the detective controls to prevent those ten things. Don't do 100, just 10, okay? There are probably 10 off the top of my head I could probably come up with.

Being aware of who the adversary are is key and to understanding the risks and Bissell said: "There are four attacker types:

- There is the insider. That is the lawyer trying to do stupid things even if that person is trying to leave the law firm and take a bunch of clients with them.
- There is the nation state that you are not going to defend against no matter what. And maybe that your target, your client is the pharmaceutical company that is producing new clinical trial results and China wants to know exactly what that result is or that new research, that new intellectual property that you're filing, whatever that issue is.
- There is the person who is trying to do what we call front running. For a company to go public, maybe their financials or M&A activity or joint venture or all these things that you do as a law firm, they want to know so that they can trade on that information publicly before it's released. So again, that's front-running.
- And then there is still that hacker in his mum's basement. It still happens.

He adds: "And I think that we need to think like a bad hacker, these four types and create those scenarios."

10 Scenarios

Distilling your scenarios down from 10 can help to clarify minds and Hemsley added: "I was with the CISO for one of the large critical government departments last week and he very much kind of said the same thing. We've got our ten scenarios and that's what every project, cloud or whatever kind of comes against, but then he said we distil it down to five, and then we distil it down to three. So, they have a fixed Post-it note that goes at the side of every whiteboard when they start talking about projects and it's very much: these are the top three scenarios that will put us in the front of whatever newspaper that we don't want to be in the front of. Does what we are about to do are fit within these? Great. Then it's the five, then it's the ten. So, they take very much that same approach of that government department."

Patching

Patching has traditionally been something that law firms don't do immediately for fear it will break something, but Bissell said organisations no longer have that luxury: At his dinner with GCHQ, NCSC and the former head of MI5 and MI6 he says: "We all agreed that most of the attacks we see are still elementary such as systems that are not patched.

We better move our mentality from patch when you can to 'you better patch now' even at the risk of breaking things I think we have to do that."

Logging

Firms also need to ensure that they keep secure logs and Hemsley said: "A number of times I've seen where there's been a data breach and we've been involved in trying to help organisations deal with that problem and if it's cloud or if it's within on premise. Logging, having secure logs, having them in a way that you can actually interrogate is quite key. If you have logs that are sitting on the box that's been attacked the first thing I'm going to do as a hacker is clear that log. So, have the right infrastructure in place to understand the breach."

Hunting and beaconing

Vast quantities of leaked data is available on the web and organisations invest in paying the likes of Accenture to find it. "We call it hunting," says Bissell. "We hunt inside and out of the dark web for information."

However, an emerging practice is 'beaconing', and Bissell says: "There is something we should look at, particularly for law firms, which is beaconing. There is capability that you can enter documents, knowing that document has left your enterprise, that you can 'call home' so to speak. That's an advanced and emerging practice that's going on right now."

cleanDocs
The smart way to send.

Oops!
...no!
...stop!
...RECALL!

Send the right information to the right person, every time and remove the risk of accidental leaks.

Learn more at docscorp.com/cleandocs

DocsCorp
Work smart

Cyber as a service

With so much to think about and potentially limitless costs to obtain the best cyber systems and coverage, it is unsurprising that the market is moving towards a cyber as a service model.

Bissell said: "That's where the market is going because no one firm no matter how big you are, not JPMC or Goldman Sachs or HSBC or Barclays no one firm can solve the problem alone. In my 28 years in security - much of which was before it was 'cool' - the market in security is moving towards this as a shared service model, not outsourced."

Ashurst last year signed a security operating service and Pellicci said: "The idea is that they will help us put the different layers on top because while we have information security staff it's not our area - it's not a law firm's area - and we don't have the capacity to keep the tools up to date."

Best practice

All leading practices should apply:

- Multi-factor authentication
- A controlled matter/document management function so that you know who has access
- Secure logs that are protected from potential hackers
- Internal detection and prevention capability based on 10 scenarios
- Background checks

And practices should:

- Patch immediately
- Consider paying to 'hunt' for leaked material on the web and dark web
- Consider using 'beaconing' to track documents.

The four key attacker types

- The insider. "The lawyer trying to do stupid things even if that person is trying to leave the law firm and take a bunch of clients with them."
- The nation state that you are not going to defend against no matter what.
- The person who is front running or insider trading.
- The hacker in his mum's basement. "It still happens."

Cloud

The arguments for cyber as a service also apply to cloud, where organisations such as Microsoft and Amazon are ploughing billions into their security arrangements and hiring the brightest minds. What was once seen as risky is increasingly regarded as a more secure option than on premises.

Asked to advise on a framework for moving to the cloud and whether it's more or less secure, Bissell said: "At Accenture we're 80% in the cloud. It depends on what you want to put in the cloud and what you want to keep on premises. There isn't one recipe. I do believe the cloud is more secure but there is a major problem among cloud

providers: Microsoft; AWS; Google even, that they are not part of your security team and they need to be more engaging. They take no risk, and no responsibility and the CIOs and CISOs need more information from them and that's a real shift going on in the marketplace right now.

"As a giant cloud user and SI [systems integrator] our methodology for securing the cloud is pretty immense. There is a checklist we go through to ensure the security of our data. We have 536 AWS buckets, just AWS. We're the largest cloud user in Microsoft. And going through a checklist is critical. You may do that for one app and then you skip stuff and then you have holes. So, having a method and a checklist is critical."

Data privacy, however, continues to be a thorny issue and Tyler said: "The perception or view that these big players are technically more secure, I don't think there is an argument against that. It just comes back to the fact that some clients or types of clients have very clear jurisdictional requirements. They have statements as to where their data has to be. We often have discussions and debates with them and to your earlier point Chris, some of them will move but there is a hardcore that won't."

Culture

Ultimately, much of the success or failure of cyber initiatives doesn't come down to the technology but the people and culture of an organisation.

The partner culture may be tough to rally against, but the CIO needs to be, as White describes it: "top of our game and in charge of our destiny." He says: "If you can't make the business case for investment you're in the wrong job."

Henri said: "Things are going in the right direction aided by the likes of the Paradise Papers and now really is our time and lawyers are listening hard. I'll give you two examples. Some of our regions were doing table top exercises in business continuity and we did one with global management committee, which took two hours, in a room, that wouldn't have happened a while ago.

"The other example is that we have invested in security wellness training SANS. We were struggling to past the 85% compliance and now the COO has said we can block compensation. If they aren't doing it they aren't going to get paid."

Imposing financial penalties is the clearest indication that cyber is no longer optional in terms of engagement.

Accenture applies both carrot and stick. Everyone has to do security training and Paul Dillon, managing director at Accenture Consulting, said: "If you don't do it your rating is impacted, which goes straight to the bottom line."

Hemsley says: "In addition to the stick we use the carrot in our training - we offer shields or badges that people can add to their profiles to show different levels of commitment to information security."

Cyberattacks are without doubt one of the biggest risks facing organisations today but if anything the tech is the easy bit: at the end of the day it's the people you have to master.

For details of our brand new CyLok cyber readiness index see front cover & p.2!

► Adventures in the Pessimistic DMS Garden: 9 Challenges Security Solutions Must Address

By Keith Lipman, president and founder of Prosperoware

Over the past year, we've seen an increase in the number of firms moving to need-to-know or pessimistic security for non-public data. The driver is simple: clients are demanding it. The underlying reasons are simple: (1) industry (such as finance) regulators are requiring it for clients' data; and/or (2) clients' security officers are demanding it as best practice. There's also a simple truism of cybersecurity professionals: it's not "if" a business will be hacked, but rather "when." Law firms are in the unique position because most of the data they hold is owned by their clients.

The change to need-to-know security can be emotional and even scary for firms. Collaboration in legal today is dynamic and fast paced. Lawyers heavily leverage past work product for new work. Such a significant change may cause partners to worry about the impact on their ability to service clients. Meanwhile KM, Records, and Information Governance professionals worry about end-users avoiding document management and other systems if their ability to work is hindered. The fear is that if people cannot get access to the appropriate document when they need it, they will simply revert to saving elsewhere and sharing via email, defeating the entire system.

It's therefore crucial to be aware of and understand the complete set of requirements before selecting or implementing a particular technology. It's even more important to understand how people actually work in law firms – unless you don't care about adoption or compliance.

Security Models Matter (Document, Profile/Metadata, or Rooted Container)

There are three different approaches to securing content: (1) document; (2) profile or metadata; and, (3) rooted container. Each exists in iManage and NetDocuments. These three approaches work quite differently. You need to understand how each approach secures content in determining your strategy for Need to Know.

Document Security

With document security, security is placed on each individual document. Typically, this is achieved via users or groups.

- Security changes take place at the document level
- Users can be granted or denied individual access subject to other types of security
- When documents are secured via a group, adding

a user to that group provides instant access. Making changes to a large number of documents where security needs to be evaluated separately will take more time to complete.

Metadata Security

With metadata security, the security is placed on the client, matter, or other metadata (which is dependent on the system) that identifies the document. If you secured Matter X's metadata:

- Any user that doesn't have access to the matter will not see the matter number in look-up, nor will they find any documents
- Granting the user access to the metadata will provide access to all documents in that matter or client instantaneously
- On its own, metadata security is not capable of securing individual documents
- Metadata security is most efficient for denying access at the matter or client level

Rooted Document Security

All document management systems are designed with a rooted model. Both iManage and NetDocuments provide this at the library/database or cabinet level. By contrast, SharePoint offers this at the Site level. In the Windows file system, it is at the folder.

In the two most widely-used DMS for legal (iManage and NetDocuments), rooted document security is controlled at the top-level (e.g. database). However, for firms considering using SharePoint, it's important to note that a user would need to first be given access to the site.

Understanding Ethical Walls / Information Barriers v. Need-to-Know Confidentiality

Whether you call them ethical walls or information barriers, there is a fundamental distinction between them and need-to-know security. Ethical walls were designed to be binary – a risk management tool that protects the firm itself from ethical violations. They are firm-centric, designed to address conflicts of interest, not client security. Decisions are typically made by the risk team at the onboarding of a lateral lawyer or a matter with a conflict. Access decisions are made and controlled by the risk management team.

Need-to-know security is client-centric. It requires a systematic approach to determining how clients want to control access to their non-public data. Determinations typically should be made on a per-client basis with the ability to provide tighter security controls when dictated by a client.

	Ethical Wall / Information Barrier	Need to Know
Creation	Conflict of interest	Client security request
Decision to apply	Risk team	Relationship Partner (with IT)
Pervasiveness	Small percent of matters	Will encompass all data
Notification of Rules	Custom, per barrier (typically)	Template
Type of Security	USA: exclusion UK: limited access (inclusion)	Inclusion, by design
Occurrence	Episodic	Constant

1. Providing Flexibility for Securing Content and Self Service

Establishing need-to-know security should incorporate a rules-driven approach that provides options that enable a person to select appropriate access for groups of or teams. For law firms, the logical groupings are as follows:

- Matter Team
- Client Team
- Sub-department or Practice Group (of Matter)
- Department (of Matter)

This requirement tends to bring some very clear challenges for groupings:

- It's easy to identify initial members at new business intake; however,
 - » Business services / admin staff likely will be mapped to fee earners
 - » It becomes more complicated as matters progress
 - » The process quickly becomes unwieldy as matters scale-up and teams are more matrixed
- Practice groups and departments tend to be far more dynamic than the firm tracks

Sound challenging? It is. There are only two ways to manage: scale up the IT or Risk Team service desk (and provide 24/7 cover), or implement a layer of self-service that enables certain access decisions to be delegated to appropriate individuals or team members.

2. Self-Service: Push or Pull (or both)

Delegating decision-making authority means deciding who can grant others access. This could be limited to risk officers only, the responsible lawyer, client/matter team, or even self-determined (think of this as closer to an 'optimistic access, once requested' model).

It's also important to understand how access is gained. It can be via 'push' where a person authorizes and then delivers that access to another, or via 'pull', wherein a user seeking access will request that access and then an automated access request is sent to someone authorized to either grant or deny access. To enable scale, workflow-driven rules are crucial to ensuring a smooth, automated process.

3. Partial / Limited Access to Individual Documents or Folders

Imagine a typical litigation matter, or an M&A deal, or even a large corporate transaction – some pieces of work may require a specialist to review or complete. Whereas, in the past, there was little focus on security and confidentiality, it's no longer in line with today's clients' expectations to grant access to everything in an entire matter to a specialist. Imagine there's HIPAA protected PII, or GDPR covered 'personal data' or any other non-public information. Full access wouldn't meet the standard. In such instances, firms need a process in place to enable the sharing of individual folders or, better yet, documents without having to defeat the entire security around that matter or client.

For this requirement, only document level security works.

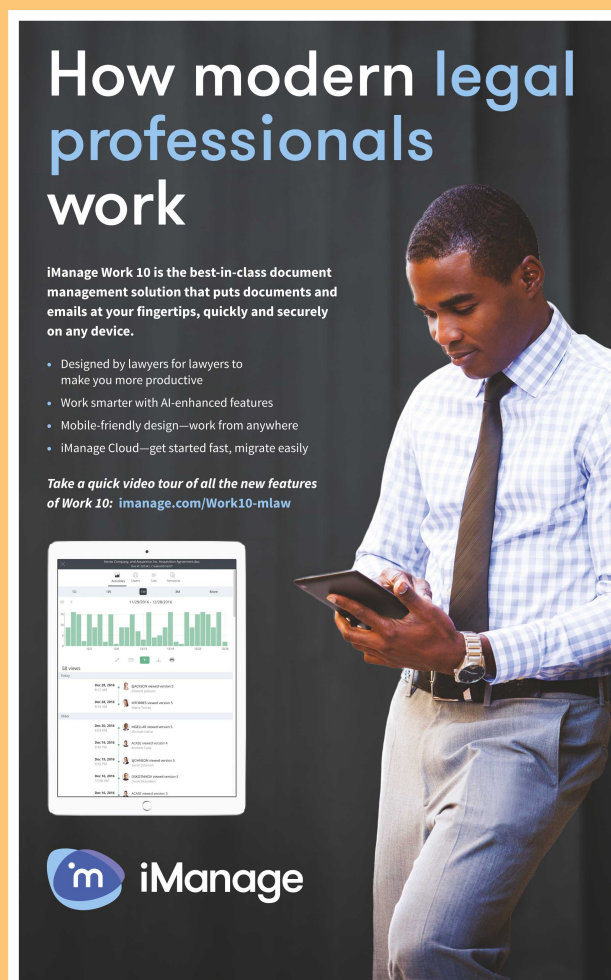
4. Granting Temporary Access

A common scenario today involves using associates, staff attorneys, paralegals, or 'floater' secretaries to temporarily assist on matters that they wouldn't normally access. It's the norm now that firms have professionals who are rarely limited to working within just one team, either to foster individual expertise or to create more flexible and cost-effective resourcing. Now, to maintain the client's security posture, consider how the firm will provide access to a single document or folder or even an entire matter or client. That should be achieved while still ensuring the firm maintains a 'least privilege access' model.

Again, for this requirement, only the document level security model works.

5. Enabling People to Keep Documents Secure from the Rest of the Team

Partners maintain numerous sensitive documents such as those involving client or matter finances. Best practice dictates holding them as part of the client or matter file. However, due to their sensitive nature, it's common to want to limit who can see them or even know of their existence within a file; they require tighter security than other documents in the file.




How modern legal professionals work

iManage Work 10 is the best-in-class document management solution that puts documents and emails at your fingertips, quickly and securely on any device.

- Designed by lawyers for lawyers to make you more productive
- Work smarter with AI-enhanced features
- Mobile-friendly design—work from anywhere
- iManage Cloud—get started fast, migrate easily

Take a quick video tour of all the new features of Work 10: imanager.com/Work10-mlaw

 iManage

This level of granularity can only be accomplished with document level security.

6. Providing Access to Billers and Others for Specific Functions

Another practical consideration is how billers or other business services can operate across matters without having full access to all matter content (which would contravene client expectations). They need to be able to view and access very specific, limited content within a matter folder.

Document level security works best here.

7. Controlling a 'Break Glass' Solution to Providing Out of Hours Access

It's no secret that lawyers work long hours. What happens when a lawyer or other professional needs access to secure data after hours? Is it reasonable to staff a support desk 24/7? One solution a firm I met with suggested was this concept of 'break glass'. Their idea was to lockdown all matters and, in the event of an after-hours emergency, the person needing access could 'break glass' and gain immediate access, without approval first. This would be logged and then reviewed later.

Skipping the approval process may seem like a solution to the urgent need problem. Unfortunately, it's a slippery slope as it inevitably slides from the occasional 3AM emergency to everyone 'breaking glass' at all hours of

the day under the guise of urgency. No one will bother to follow the standard procedure or wait for formal approval if they can act first and apologize later. The idea quickly becomes unworkable. Someone will be left wasting a significant amount of timing 'cleaning up' after.

8. Keeping Public Data Public and Adjusting Security when Non-Public Becomes Public

What about when there's too much security? Clients or regulations will dictate that matter data must be secured, but it doesn't make sense to secure data that's become public. This could include pleadings, court rulings, public filings, agreements filed with the SEC, etc. Because much of this information initially is private, there needs to be an efficient mechanism to accommodate the change – a fluid approach to confidentiality management.

9. A Client May be Clients and a Matter May be Matters

In numerous law firms, a client is typically represented through the use of multiple client numbers. This may be related to compensation issues or other factors. Similarly, a matter may be split across multiple matters numbers. This can also occur for a multitude of reasons, but it is typically related to differing fee types (e.g. hourly, fixed, etc). The end result is that a single team may need to have access to multiple client or matter numbers.

Balancing People + Process + Technology

You can't make a decision about how to update security processes in a vacuum. As with almost any process, it's crucial to understand and accommodate all three pillars of the 'people + process + technology' equation. Get one of them wrong and the project will likely fail. 'People' have only more recently been focused on this need for content security. It could be thanks to clients, cyber security awareness, or regulatory demands. The 'process' needs to be the next focus – and technology is closely aligned with process.

Before jumping in with any decisions, it's important that firms understand the complex workflow and collaboration needs that their firm relies upon. Firms need to ensure that the technology selected can complement rather than hinder execution. If the software can't support all these use cases, people will become frustrated. If they can't get their work done within the defined process, people will find ways to get it done – likely by working around the DMS and content systems, negating the entire benefit of those systems and destroying any semblance of security.

Are your documents 'in the wild'?

REDUCE YOUR GDPR RISKS WITH RBRO'S **LINK2DMS**

If you're saving documents 'in the wild', outside of your document management system, you're increasing your risk of GDPR non-compliance.

Improve your content compliance, data governance and productivity—simply and seamlessly—with RBRO's **Link2DMS**.

Link2DMS is a powerful and easy-to-use solution that seamlessly enables you to save and open documents created with popular non-integrated applications directly within **iManage Work**.

It's time you regained control.



RBROSOLUTIONS.COM

0800-088-5378

aka 'The Orange Rag'



! Misfire on lateral hires

! Confuse capabilities

! Underestimate experience

! Fuss with fixed fees

! Procrastinate proposals

A better path to winning new business

Take advantage of the latest innovations in the client development process. Now, with your firm's collective experience and historical pricing data at your fingertips, you'll be able to respond to changing needs quickly. The Intapp Professional Services Platform makes it possible by utilizing the power of intelligent search, AI integrations, workflows, and data augmentation to give you the answers you need to outcompete your peers and win more business, more simply.

www.intapp.com/clientdevelopment

© 2018 Intapp Inc. All Rights Reserved. Various trademarks held by their respective owners.

► What's hot & what's not: wins & deals

UK & EMEA LexisNexis announced that **Irwin Mitchell**, the 11th largest law firm in the UK, has selected LexisPSL as its preferred KM/practical guidance platform. LexisPSL will provide over 1500 users within Irwin Mitchell with legal insights and answers across more than 30 practice areas. And residential conveyancing and property law firm **Fletcher Longstaff** is deploying legal workflow and case management solution **Lexis Visualfiles** to streamline and automate business processes from quote development through to completion of conveyancing transactions. Fletcher Longstaff will use the Visualfiles Conveyancing Accelerator to help realise this benefit quickly.

Middle East law firm **Al Tamimi & Company** has become one of the first firms to adopt Blueprint, Tiger Eye's knowledge management add-on tool for iManage developed by **Tiger Eye Consulting**.

Blueprint is a KM workflow tool that enables lawyers to submit their documents to professional support lawyers with one click, streamlining the submission and approval process and encouraging lawyers to ensure their knowledge finds its way into a curated platform.

Bermans, a niche commercial practice specialising in lease and asset finance, with offices in Liverpool and Manchester, has signed a 10-year deal for the PeppCX Platform, combining CRM with practice, case and document management from **Peppermint Technology**. PeppCX is an SaaS solution delivered in the Cloud.

DocsCorp just announced that **Delphi**, one of Sweden's top commercial law firms, has chosen contentCrawler as part of its GDPR compliance strategy. The firm selected the contentCrawler OCR module to help address the "dark data" issue that was discovered after an audit of their file systems. The audit found that 30% of the documents in the firm's **iManage DMS** were non-searchable, with nearly 70% of these being image-based PDF files, thereby undermining the firm's ability to manage clients' personal data and to adequately respond to a Data Subject Access Request (DSAR). In other DocsCorp news... top-tier Scottish firm **Burness Paull LLP** bought cleanDocs to ensure documents are cleaned of metadata when emailed or stored in their iManage DMS, while another iManage DMS client, **Collas Crill Group Services** based in the Channel Islands, went with contentCrawler to ensure all documents stored in iManage repositories are fully text-searchable and retrievable. The decision to go with contentCrawler was part of the firm's GDPR compliance strategy.

UK firm **Girlings** opted for **Tikit** to supply them with a 110 user **Tikit P4W** and Tikit Connect system for practice and case management and CRM, and Danish firm **IUNO Advokatpartnerselskab** purchased **Tikit Carpe Diem** to streamline their time recording.

High Wycombe law firm **Reynolds Parry Jones LLP** has signed up to integrated practice and matter management system **SOS Connect** from **Solicitors Own Software** after canvassing the views of fellow members of national legal network **LawNet**. Partner Robert Hill said the firm's incumbent legal software had become unsatisfactory – prompting him to look for alternatives. "We are members of LawNet, spoke to various people about their views on the market, and narrowed the choice down to three suppliers". And, Scottish firm **Caesar & Howie**, which offers a range of legal and estate agency services at offices across the Central Belt, has also signed up to integrated practice and case management with **SOS Connect** from **Solicitors Own Software**. The firm will initially use **SOS Connect** for Power of Attorney, Wills and Advance Directives work, and then look to roll it out into areas like Residential Conveyancing, Purchase and Sale.

Top tier Norwegian law firm **Wikborg Rein** has adopted **Luminance** following a successful pilot of the technology where the law firm directly compared the manual findings of a live due diligence review against those enabled by Luminance. Swedish corporate law firm **Setterwalls** has selected Luminance for its due diligence process in M&A transactions. The announcement marks the 18th Nordic law firm to adopt the machine learning technology. And corporate law firm **Gattai Minoli Agostinelli & Partners** has gone with Luminance to streamline the M&A due diligence processes at the Italian firm.

**LESS EFFORT
RECORDING TIME.**

**MORE TIME
PRACTICING LAW.**

SMART TIME ENTRY FOR
THE LEGAL INDUSTRY.



Machine Learning capabilities expedite narrative clean up



Time Entry made simple with consumer grade user experience



Real-time synchronization across all devices



Capture billable time without the fear of "big brother" watching



Access online or offline, on-the-go with no data loss



Flat monthly fee (fixed-price)

Epoch™
Intelligent Time Entry

An innovative product by **fulcrum GT**

Tricostar has been awarded two contracts, including one with **Ofsted**, for their TCM legal case management system using the GCloud Framework. Ofsted's key criteria included tight integration with their SharePoint DMS and a court bundling application both integrated with TCM and SharePoint. Another key factor was that the application was current with Microsoft's latest desktop, browser and server technologies. To further improve accessibility, the application has been delivered in the cloud using Microsoft's Azure hosting platform. The second contract, a major city council, were looking to replace their existing AIM Evolution system, integrate with SharePoint, and in addition are undergoing an extensive data migration exercise, as well as being trained in advance workflow automation.

NORTH AMERICA AmLaw 100 firm **Blank Rome** is the latest Big Law firm to turn to **Casetext** and is now utilising Casetext's newly updated CARA AI technology to automate legal research tasks. Other recent Casetext wins include White & Case, DLA Piper, O'Melveny and Cozen O'Connor.

Canadian firm **Langlois Lawyers LLP** has selected the **LexisNexis InterAction** CRM system for business development work.

Wolters Kluwer ELM Solutions announced that **CHS Inc.**, a large US farmer and rancher-owned cooperative, has selected its **TyMetrix 360°** solution. CHS is utilizing TyMetrix 360° to automate its eBilling process and gain in-depth visibility into matter management and legal spend. It also enables CHS to easily share related data and track all documentation associated with a large matter portfolio in a secure and consolidated place for collaboration with internal business partners and outside counsel.

Cassels Brock & Blackwell LLP, one of the largest business law practices in Canada, has selected **Litera Microsystems** latest product Clause Companion, which provides legal professionals with an easy way to store and retrieve preferred clauses from within Microsoft Word. Travis Leon, Litera Microsystems Executive Director said "By adding Clause Companion to their workflow, lawyers at Cassels Brock will be able to quickly store, search for, and access language which has been painstakingly crafted by experienced legal drafters, whether it is for their own purposes or to share with less experienced colleagues." Litera Microsystems also announced that **Goldberg Segalla**, with more than 20 offices across the US and UK, is to roll out Litera Microsystems complete product suite. Known as Litera Desktop, it comprises all Litera Microsystems products for drafting, proofreading, comparing, repairing, cleaning, and securing documents. Litera Desktop replaced products from several vendors including BigHand and Levit & James.

Gould & Ratner LLP has agreed to be a beta client to integrate **Wilson Legal Solutions** Ideate software with **Rippe & Kingston** Legal Management System. This will be the first integration of Rippe with Wilson Ideate.

Anaqua Inc reports that US law firm **Blueshift IP: Software Patent Experts**, which is based in Cambridge

(MA), has chosen the ANAQUA platform for paperless management of IP documents.

As firms increasingly look to transition from an open access document management system to a need-to-know or pessimistic security model, Am Law 200 firm **Thompson Hine** has selected Confidentiality Manager from **Prosperoware**. In September 2017 the firm migrated from an OpenText eDocs DMS to **NetDocuments**. The move triggered an ancillary need to select a new tool to manage matter and document-level security for implementing ethical walls and enabling need-to-know access.

New England-based firm **Hamilton Brook Smith & Reynolds** chose **DocsCorp** cleanDocs as its preferred metadata cleaning and recipient checking tool.

APAC **Russell McVeagh**, one of the 'Big Three' law firms in New Zealand, has selected Luminance after a successful pilot of the technology, which allowed its legal team to review a large number of contracts from historic transactions. **Maddocks** in Australia has also adopted Luminance's machine learning technology to streamline the due diligence processes at the Australian firm. And, **Weerawong Chinnavat & Partners**, one of Thailand's largest independent firms, has become the first Thai legal practice to deploy Luminance machine learning technology to improve the efficiency of their contract review. The deal follows the opening of Luminance's office in Singapore.



the document & information lifecycle specialist

iManage Partner, Cloud Evangelist & Deployment Pioneer

"In addition to good account management and accountability for support services, we wanted a technology provider who could take on a consultative role in helping us realise our strategic, five-year vision for technology adoption. Ascertus met these criteria."

Clive Knott, IT Director, Howard Kennedy LLP

...a refreshing alternative

"Ascrtus continue to impress us with their knowledge and professionalism. Their deep understanding of the iManage suite allows them to efficiently resolve complex issues that we escalate to them allowing us to focus on delivering benefits to our firm"

Steve Dalgleish, Applications Manager, Shepherd & Wedderburn LLP

+44 (0) 20 3126 4960 contactus@ascrtus.com

in /ascrtus @ascrtus www.ascrtus.com

► Movers & Shakers

UK & EMEA **Stu Gooderham**, LexisNexis' head of client relations for ERP solution LexisOne, has joined **Wilson Legal Solutions** as commercial director for EMEA in yet another significant UK hire for the Pennsylvania-headquartered company that recently acquired/merged with London-headquartered BD and CRM consultancy **Stanton Allen**. Gooderham's hire by Wilson means he will be reunited with VP of strategy **Norm Mullock**, who he worked with at business intelligence software company Redwood Analytics. Mullock was a co-founder and chief strategy officer Redwood Analytics, which Gooderham joined as a sales director as it was acquired by Lexis and worked in that role for five years. Aderant acquired Redwood from Lexis in 2014. Everyone keeping up with the revolving doors of legal tech?

As part of a wider technology and change management strategy review led by **Janders Dean**, Mayfair-based real estate and private wealth law firm **Forsters** has hired former Harbottle & Lewis interim IT director **Anthony Stables** to fill the newly-created role of CIO. Stables is a director and founder of RESHAPE IT, an IT consultancy set up last year that specialises in strategy and transformation. Previously Stables was Olswang's interim IT director and played an integral role in shifting the firm's infrastructure to a private cloud prior to its three-way merger with CMS and Nabarro.

NORTH AMERICA **NetDocuments** has made three senior internal promotions: **Leonard Johnson** will now lead NetDocuments' global partner community and strategic technology partnerships, **Dan Hauck** will assume the role of VP of product and user experience, and **Ian Kujawa** will be taking on the role of director of corporate strategic sales. Johnson is a veteran of over 20 years at NetDocuments. Hauck, a former Big Law attorney and CEO of ThreadKM, will now transition into Johnson's former product role. And Kujawa, formerly the president at Esquire Innovations and managing director at BigHand, was hired in 2017 to head NetDocuments integration, services and channel partnerships.

Vound, a provider of forensic, eDiscovery, and early case assessment technologies, has expanded its leadership team by hiring **Sharon Marvin** as Chief Operations Officer. Sharon, a certified Lean Six Sigma Lean Black Belt, will lead Vound's global expansion and growth strategy. Most recently she was the VP of DKI Services, a \$3.2 billion franchise network.

Iridium Technology has promoted **Keith Dunn**, who joined the company earlier this year as a senior BI consultant/developer, to Product Manager for the entire Iridium BI product line. Before joining Iridium, he was Director of Financial Systems at Womble Bond Dickinson.

Gregory Lutz has joined eDiscovery and litigation support services company **Consilio** as managing director in charge of the Eastern United States sales team. Prior to joining Consilio, Lutz served as a senior VP at Epiq, and, previously, director of discovery consulting, sales and

marketing at Inference Data, as well as a sales manager at Fios and LexisNexis.

Private equity firm **LLR Partners** has engaged **Cary Burch**, a software executive in the legal, mortgage and financial services industries, as a Senior Operating Advisor. Burch will help LLR identify and evaluate new investment opportunities. Burch was most recently the CIO at Thomson Reuters and held CEO and COO roles at the company's legal software business Thomson Reuters Elite.

► Fraser Mayfield launches Clio rival matters.cloud

Legal technology specialist Fraser Mayfield has launched a brand new cloud-based matter management solution called www.matters.cloud, which is based on Google Cloud and has data security at its heart.

The multi-tenanted system, which runs in five languages, is targeted at the small law firms market and intended to help them manage existing clients and matters as well and developing contacts and opportunities; capturing time in the office and on the go; and collaborating with colleagues on tasks and deadlines.

The system, which offers a fully automated sign up process, will compete with the likes of Clio, offers the ability to operate in the following languages: English (UK), English (US), Dutch, French, Spanish and Russian.

It uses Google Cloud Compute to provide web based services in each region with load balancing between environments to provide scale as the number of users grow.

Users are able to record time against both opportunities and matters to track total time spent with a client.

To ensure data is kept secure, Matters.cloud will be offering data centres in Europe, the USA and Australia.

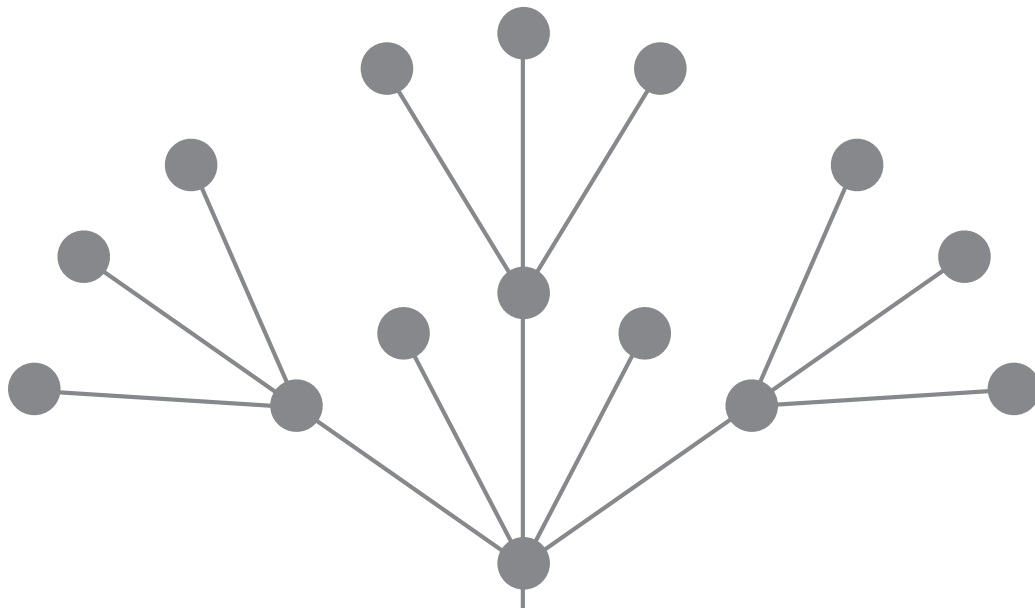
Mayfield is founder of Cintelli, which provides strategic advice, project management, implementation consulting and technical services to the legal industry. He is also Director EMEA for Iridium Technology a leading provider of Business Intelligence for law firms, which is an ongoing role.

aka 'The Orange Rag'

3E guides your firm to a future without limitations.

THOMSON REUTERS
ELITE™

Gain the strategic visibility to embrace change fearlessly.
Arrange a demo today at elite.com/3E



The intelligence, technology
and human expertise you need
to find trusted answers.



the answer company™
THOMSON REUTERS®

© 2017 Thomson Reuters S048590/6-17

aka 'The Orange Rag'



The MindCycle Tour
in support of MQ Mental Health

USING PEDALS TO POWER PIONEERING MENTAL HEALTH SCIENCE



**I am Rob Stephenson. I am the founder of Inside-Out.org
I am a father. I am a husband. I am a cyclist. And I am bipolar!
We're not simply one thing...**

Find out more about how I
am **#SmashingTheStigma**
of mental illness in the
workplace – *with a bicycle!*



INSIDE OUT

I will be visiting workplaces across the UK
during July to cycle the full 3,300km of the Tour
de France on a static bike in support of MQ:
Transforming Mental Health.

MQ funds ground-breaking research to increase
our understanding of mental illness and
radically improve diagnosis and treatment.
Their aim is transform what it means to
experience mental illness starting now and for
every generation to come.

To find out more about how you can help, visit www.mindcycle.cc

Current Supporters:



maven
partner
Exceptional knowledge and experience.



Transforming
mental health
through research



validus

► HighQ: New workflow tools could be transformational

We flagged back in February that HighQ was launching an AI Hub and at its well-attended user conference on 23 May the hub formally went live, but much of the user excitement centred on the new workflow capability being built within HighQ Collaborate iSheets, which has the potential to be transformational.

HighQ is working on introducing triggers into iSheets (which allow teams to work collaboratively with structured data) whereby when a task is completed it triggers a dynamically generated outcome: if an iSheet record is completed that might trigger a document to be automatically populated; a calendar appointment to be made; or a task created, significantly reducing human intervention.

Addressing delegates in the Grange, St Paul's in London, Rob MacAdam, head of legal design at HighQ, said: "You can start to define the process from start to finish so you have a fully automated process. We're aiming to allow you to standardise and automate legal matters."

There are several benefits to automation including that you can mitigate against error, reduce manual intervention, speed up the cycle, gather metrics, and ultimately facilitate a self-service approach. It may be the client that updates the iSheet, which then creates a task; generates an engagement letter; and/or auto generates an event in your calendar.

In the demo given by MacAdam, for three manual interventions, 14 actions were generated.

In a break at the conference one IT head said: "I wish some of the lawyers at my firm were here to see this – it's really exciting but then I have to go back and explain it. It's not the same." Whether lawyers are really ready for these changes is another question altogether.

Overall the conference centred on the launch of Collaborate 4.4 and Publisher 4.7.

Collaborate has six new features:

AI Hub - available in 4.4, the brand new hub means that you can use multiple AI engines 'invisibly'. Chief strategy officer Stuart Barr told us: "You don't have to go to Kira and export data back to HighQ. All the data gets stored in the hub and you can use it to create data visualisations such as dashboards to summarise provisions such as contract language and jurisdiction. You can ask 'what am I dealing with?' at the beginning of a deal. Data can be pulled into iSheets and used for due diligence analysis. If you want to extract the start and end data and the parties or the contract value that can all happen using AI Hub."

The Hub already connects to Kira (which you will need a separate license for) and the plan is that there will be further integration announcements over the next few

months. "Two clients today already expressed interest in a connection with LexPredict and Leverton," Barr told us at the conference. "You'll see these things being added to the AI hub."

AI hubs are very on trend and iManage at its user conference also outlined its own platform play but Barr said (we like to think in the voice of the Highlander) that there can be more than one. "What it's about is HighQ being the hub, not Kira or Luminance - they recognise they are an engine and need to be able to integrate. Data visualisation happens in our platform. That's the same for the other vendors we compete with and it's not a problem to have multiple hubs." However, he adds: "With our iSheets and data visualisation we've gone a step further. Clients are saying this is unique."

Other product updates announced at the user conference include:

- Improvement to HighQ's data visualisation engine - launched at Legalweek New York, this engine has been enhanced so it is more flexible and you can do calculations on data before visualising it. For example, you can do real time WIP calculations in advance. Barr says: "Last year this was all manual, but we have productised it and in a few clicks you can visualise the data."
- Real time editing in O365.
- DocuSign improvement – you can now tag multiple signatories.
- Tasks timeline view - the timeline chart now shows when tasks start and end and can help identify if people have been allocated the same work.
- Customisable site navigation – this enables you to transform spaces in Collaborate for diverse cases. The nav bar can now be customised for every deal and link to different iSheets.

HighQ gets mortally offended now if you describe it as a deal room provider and that's fair enough, although it still has a branding issue. Speaking to delegates, MacAdam described how HighQ can now be integral to managing your workstreams, project tracking, budget planning and due diligence reporting.

The dashboard builder allows you to see you where you are in terms of WIP, billed hours, outstanding tasks, and tasks by phases.

"One way that lawyers have been managing is through Excel but that's not dynamic. This is a different way of managing tasks that is far more dynamic and visual," MacAdam said.

"This is not just M&A but managing the discovery process in litigation or managing a property portfolio – you can track different workstreams."

There is no doubt that HighQ is reinventing itself (and, much like iManage, stepping on a fair few toes in the process.) Barr says: "We're moving from document-centric to process-centric, which is more valuable than just documents. File sharing is inherently commoditised, and the deep challenges now are how people work differently

and how do they automate and optimise the work they do."

Chief revenue officer Paul Hunt added: "There is so much unstructured data and unstructured process – we're bringing that together and streamlining and commoditising it to release the value."

Barr adds: "Firms are struggling with how to modernise and digitise – they are all under huge cost pressures. They need to get rid of manual laborious processes to free up higher value legal work. Fundamentally that's digital transformation – we're allowing our clients to be smart using AI and process automation."

► May Highlights: iManage smashes ConnectLive London

One of the highlights of the London legal tech calendar in May was iManage ConnectLive 2018, where a UK top 30 IT director nicely summed up the mood after the keynote, saying: "Four years ago I'd practically written these guys off but I'm so impressed with what I'm hearing."

Accompanied by loud music, branded blue background and sky scraper imagery, the morning of day one saw a confident senior iManage executive team set out their achievements to date and an ambitious roadmap going forward.

iManage's CEO Neil Araujo thanked the iManage community for their support, which has seen revenue increase significantly year on year since iManage's MBO from HP in 2015. Profit has remained flat – a testimony, Araujo said, to iManage's commitment to invest in the business.

One measure of that investment is growth in people – iManage had around 150 staff when it left HP and now that number has risen to over 400.

"The pace of change is only accelerating," said Araujo. "Digital transformation is about changing mindsets and processes and potentially business models. It's about having employees embrace digital and creating positive digital attitudes."

Digital transformation was a recurring theme and Araujo said: "Legal technology can stall innovation and get in the way – it feels like an anchor that sucks up your resources. It's our response to help you overcome these challenges that has inspired our own growth."

iManage is now talking about a platform approach and setting itself up as the hub for DMS, AI and security, with a seamless user interface to create "frictionless" workflow.

On the roadmap for 2018:

- Ensuring the successful deployment of iManage Work 10

- Making upgrades simpler
- Improving encryption on premises and in the cloud
- 'Out of the box' AI – Araujo said: "without that it's hard to get a broad usage of AI. We're enabling you to exploit your own data to drive the use of predictive analytics."
- Expanding the scope of iManage's governance products
- Enhancing its cloud offering. Araujo said: "This year is going to be game changing. Our goal is to make our cloud SLAs the best in the industry – the same as you're used to in the consumer industry."

A few of our highlights:

- VP of product management, Shawn Misquitta set out the newer features of Work 10, which includes the ability to easily restrict and facilitate access to folders. "You can see this case is protected by a security policy and who has access under that policy," he said in a demo to the ConnectLive audience. "Using a plugin you can quickly build a shared folder. Users don't have to ask IT to get access. They go to an email chain and drag and drop into the shared folder. It all shaves off time and users are added as collaborators."
- Work 10 keeps a track of who has worked on a document and when. If a document gets overwritten, users can work out when it happened, call IT and ask to get it restored to eg as of 5pm yesterday.
- Work 10 can now be used on a Mac natively within Word – users go 'save' and it will give you an option to save in iManage.
- iManage now has an interface embedded in Microsoft Teams. Users can work within a team room and the content will be stored in iManage.
- Documents can be automatically classified using RAVN technology, which conducts deep analysis of parties and shows titles and other key data. "You're witnessing iManage becoming content aware," said Misquitta.
- Again with the benefit of RAVN technology, a clause library will flag similar clauses to speed up associate drafting.

On a personal note, I'm physically incapable of writing about ConnectLive in any kind of sensible timeframe, largely due to the fact that iManage knows how to throw a party. Thanks to the vast number of vendors that work with iManage, ConnectLive is a great industry get together and, as observed by DLA's Jason Plant, has an ILTA feel to it.

Here Plant, blogging on his site No Option for Law Firm, had the following observations about the day:

1. The RAVN indexer. Not the most exciting thing on the face of it. But there are a couple of things that I really liked. First off the architecture, it's old school iManage, simple, well thought out components (not like IDOL, though shall I publish that blog post on initial thoughts of IDOL now from the early days of the

Autonomy merger?). It's also been designed to scale. But overall seems it will require less hardware and storage than IDOL. Second and more important it will fulfil a promise that I was looking for at the time of the Autonomy/Interwoven merger that never materialised, this being one index to fulfil many solutions, so once you've indexed your DMS you can use this index to get all the good stuff from Extract, Insight and the excellent idea that is Classification (using machine learning to auto classify/profile those documents!). No need for an index for this, another one (of the same document set!) for something else.

2. New cloud. Sorry I'm not sure what the actual name for this is, but it's the new architecture that is designed from the ground up for the cloud. It uses all the latest tech that is used to scale all those platforms that are MUCH bigger than any law firm data set, twitter and the like. Rafiq's keynote on the tech on the second day was one for the tech geeks, great! Be good to see this platform in the wild.

3. Security Policy Manager. Now this product has been around for a while, but it was a couple of things on the horizon that made me think that this is becoming more than a replacement for "the other product". First off was the ability to use it to manage policies of other legal products, for example the policies for Workshare Protect, very interesting concept and could be great to reduce admin in stretched IT depts. Second was talk of DLP (data loss prevention) and DRM (digital rights management), imagine one place to manage the rights to client/matter information that then manages where that data can go and if it goes outside the perimeter it can be managed and controlled or blocked! This could be really exciting and the DRM aspect is one I've suggested before.

There were a couple of other areas that I need to think on a bit more:

1. Go drive. This is a product I think I can buy into, but think I would want to use it myself for a bit and maybe try it with a few lawyers first. There are a few parts to mention.

- First there is the functionality that is essentially like OneDrive is for cloud files on Windows 10 but looking after the documents from your DMS (wherever that is). I can see plenty of use cases for this.
- Then there is the tech underneath to manage the file transfer better that allows for improved experience over links with high latency. Again can get this.
- Lastly is the ability to display the DMS in file explorer, now this I can sort of see but think I would need to use a bit I think to make a final view.

2. Auto update feature. I get this, it's the move Microsoft and others are making to ensure we're all on the latest versions. But with MS we're using their tooling to manage all of the updates in the new Windows 10 Office and 365 evergreen world, another set of tooling to manage the iManage updates? Will it scale to organisations with thousands of machines to update from Seattle to Brisbane? Need to look some more at this.

► LawGeex Buyer's Guide

In case you missed it, LawGeex' In-house Counsel's Legal Tech 2018 Buyer's Guide came out in May and is well worth downloading. It features 16 different categories of legal tech from contract drafting to eDiscovery and digital signature, to prediction and litigation analytics software.

It includes not only listings of key providers in each category but highlights the latest legal trends as well as the experiences of legal teams at the vanguard of new tech adoption including Google, Microsoft, Facebook, McDonald's, NetApp and others. You can download it for free here: <https://www.lawgeex.com/buyersguide/>



Connected thinking
for your data

Discover Phoenix information
management solutions

Optimise productivity, security and insight
with secure, governed information management
solutions from the world's leading iManage partner.

Talk to Phoenix about your specific information
management requirements today.

@phoenixbs
phoenix-business-solutions
www.phoenixbs.com

phoenix

ABU DHABI | CHICAGO | FRANKFURT | LONDON | NEW YORK | SYDNEY

aka 'The Orange Rag'



ECLIPSE

Part of Capita Plc

25,000 people can't be wrong

Eclipse's Proclaim system is the solution of choice for 25,000 legal professionals in over 1,000 organisations. Proclaim encompasses Practice, Case and Matter Management, and is [the only system to be endorsed by the Law Society](#).

From new start-ups to industry heavyweights, Proclaim is the system of choice for forward-thinking law firms.

- Fully integrated Practice Management Software solution
- End-to-end case and matter management workflow processes
- Ready-to-go workflows for specific practice areas
- SAR-compliant legal accounting
- Fast to implement, easy to use

Contact us for a demonstration

01274 704 100

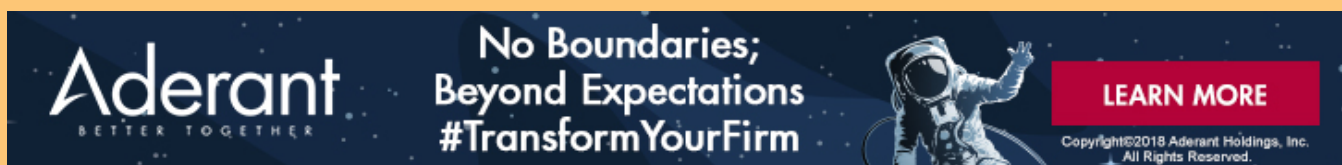
Email: info@eclipselegal.co.uk

www.eclipselegal.co.uk

Endorsed by



The Law Society



► GDPR Day

Our April GDPR readiness survey revealed that 40% of law firms still do not feel ready for an ICO audit now that GDPR has come into force. Surprised? We're not.

We also asked how confident firms are that they can deal with an influx of subject access requests – 80% said yes. Unsurprisingly, no-one wanted to be contacted.

GDPR day itself came and went without event for many, oh apart from Facebook, Google, and Facebook-owned businesses WhatsApp and Instagram, which were immediately sued by NOYB – a privacy campaign group set up specifically for this purpose by Max Schrems, who is lovingly described by The Register as “the thorn in Facebook’s side”.

The claims argue that users of these sites are being forced to consent to their data being retained because it’s a condition of using the service. Schrems says it should not have conditions attached. In a blog on NOYB’s website he calls it “fictitious consent.”

You can read that here: <https://noyb.eu/>

NOYB stands for none of your business and the site lists the donations coming in to support the claims, which now run into the hundreds of thousands.

Elsewhere, Ghostery sent out a GDPR email on May 25, 2018 that unintentionally resulted in the exposure of account holders’ email addresses to other Ghostery account holders and users.

In a statement Ghostery said: “Unfortunately, due to a technical issue between us and the email sending tool we chose, the GDPR email, which was supposed to be a single email to each recipient was instead sent to a batch of users, accidentally revealing the email addresses for each batch to all recipients of a batch by adding everybody directly in the “To” field. We sincerely apologize for this incident. We are horrified and embarrassed that this happened, and are doing our best to make sure it never happens again.”

legal*i* insider

The next Insider newsletter will be published on **Wednesday 27 June**.

To keep up with the latest news visit www.legaltechnology.com

And follow [@Legalitinsider](https://twitter.com/Legalitinsider) + [@ChristianUncut](https://twitter.com/ChristianUncut) + [@chillmedia](https://twitter.com/chillmedia) on Twitter at [#legalit](https://twitter.com/legalit)

Editor:

Caroline Hill

t: +44(0)203 587 7822

m: +44(0)7786 245612

e: caroline.hill@liti.co.uk

🐦 [@chillmedia](https://twitter.com/chillmedia)

Associate Editor:

Charles Christian

t: +44(0)1986 788666

m: +44(0)7786 738172

e: charles@legaltechnology.com

🐦 [@ChristianUncut](https://twitter.com/ChristianUncut)

Advertising Sales Director:

Jeremy Hill

t: +44(0)203 5877821

m: +44(0)7973 483131

e: jeremy.hill@liti.co.uk

🐦 [@legalitinsider](https://twitter.com/legalitinsider)