FINANCE | HR | IT | MARKETING | BD | MANAGEMENT | RISK | KM

Briefing

AN INCREASINGLY RISKY BUSINESS?

FEBRUARY 2015

Feature

Eyes everywhere

Picking apart risk best practice, from boardroom recruitment to business continuity

JE SUIS CHARLIE

Industry views

Risk and reward

How technology can take strategic risk management to the next level

Uncertainty principles

Scott Nicholl, Hogan Lovells' head of risk, on defeating hackers, avoiding Ebola and creating a compliance culture

Business Intake

(But Much Better)

Efficiently taking on matters is critical to the practice of law. Today, several trends are putting new pressures on law firms to transform the way they evaluate and engage new business:

- Clients expect greater service (and want to pay less for it)
- Lawyers want to start work immediately (sometimes before conflicts are cleared or matter numbers are issued)
- Firms want to more carefully evaluate the clients and matters they accept (to avoid surprises or unpaid bills)
- IT and Conflicts Teams are eager to provide lawyers with easier tools, faster service and a pain-free experience

Thriving in this environment requires an innovative approach to intake and conflicts — one that allows firms to act quickly (while still rigorously evaluating matters), to delight lawyers (especially on mobile devices) and to easily change processes (without outrageous delays). In short, intake must evolve.

Intapp Open is the answer. Instead of complicated tools that require expensive, time consuming implementation projects (and ongoing consulting bills), Intapp offers a fresh approach, built specifically to address the diverse and specific needs of firm management, lawyers, risk staff and IT stakeholders.

Over 100 firms (ranging in size from 70 to 4200 lawyers) have chosen intake and conflicts software from Intapp.

Whether as part of a strategic push to improve client analysis and profitability, a program to reduce risk, or an initiative to speed matter opening and improve lawyer productivity (and satisfaction), Intapp Open has something to offer every firm.

Including yours.

Learn more: www.intapp.com/Open

intapp™

Software for a Changing Legal Market

Running your risk

Letter from the editor-in-chief

Risk management touches everyone in a legal business. While it's the fee earners' job to help clients mitigate, avoid, suppress and dodge risk, who does that for your firm? Hint: there's no fairy godmother.

We live in an increasingly unstable world – disease, terror and environmental crises seem to be riding unleashed around the world in 2015 – yet businesses must survive and grow in this environment. This applies to law firms in particular, which are growing globally and encountering more threats as a result.

That's why in this issue we've further opened up our view to outside the legal industry – interviewing leaders at the UN, the Institute of Directors and in financial services – as well leaders at firms **Dentons**, **Burges Salmon**, **TLT** and **Birketts**, in editor Richard Brent's feature, p12. Expect more of this as we continue to widen our remit.

Our main interviewee, **Scott Nicholl at Hogan Lovells**, gives an overview of the challenges facing a risk leader on p6 – showing that risk on an international stage is truly testing, and rewarding.

And in our industry voices section, from p20, we've a great case study on Eversheds' use of issue sponsor **Intapp's** technology to crush risk, as well as comment and analysis from other leading suppliers.

I hope you also like our new style of cover. If you do, just wait for the imminent redesign...

Rupert White, editor-in-chief of Briefing

Interview: Scott Nicholl, Hogan Lovells

With more than 40 offices from Budapest to Beijing, Hogan Lovells has a bulging risk register. Richard Brent talks to head of risk Scott Nicholl about making sense of an uncertain world

page 06

Feature: Eyes everywhere

Law firms always have an eye on their clients' risks, but they can also learn lessons from other organisations and sectors – and perhaps turn threat to opportunity

page 12

We're proud to have this issue of **Briefing** sponsored by: intapp™

All interview photography this issue: Jonathan Goldberg
www.jongoldberg.co.uk

This month's interview with Scott Nicholl was transcribed by: Dictate NOW

THOMSON REUTERS
ELITE™

YOU VS. FINANCIAL GUESSWORK.

Thomson Reuters Elite™ offers a complete enterprise business management solution for more efficiency, transparency, and profitability. The current business climate is still an open question, but now you'll be ready to offer answers that benefit your bottom line. From streamlined accounting procedures to improved invoice management; better budgeting and forecasting to insight into key operational metrics, Thomson Reuters Elite can help you maximize financial performance. And make guesswork a thing of the past.

DISCOVER A BETTER WAY AT ELITE.COM

THOMSON REUTERS™

Industry analysis index

Who we are...

Briefing is published by Legal Support Network, the only media and events business focused on legal business services

Rupert White is editor-in-chief of **Briefing** and LPM, head of content and community for LSN, and secretly actually the Gruffalo
rupertw@lsn.co.uk

Richard Brent is editor of **Briefing** magazine. He is responsible for scoops, creative flair and keeping Berocca in profit
richardb@lsn.co.uk

Declan Tan is **Briefing**'s assistant editor, responsible for word wrangling, fact checking and liquid layout skills
declant@lsn.co.uk

Sarah Cox is LSN's head of client services and chief Streatham Mum. Contact her about advertising in **Briefing**
sarahc@lsn.co.uk

The Briefing Interview

That was close...

Bad stuff happens – the risk management trick is to not be the victim of it. From jurisdictions in economic danger zones to Generation Y judgment, Hogan Lovells' head of risk Scott Nicholl talks to Briefing about driving down risk at home and abroad – and how to keep partners on course

Words: Richard Brent
Photography: Jonathan Goldberg

Where would lawyers be without risk and wrongdoing? It is, quite simply, their bread, butter and everything in between. From the Serious Fraud Office's first convictions under the Bribery Act in December to the traditional January divorce spike, trouble and strife is the start of many a matter – and profit pool.

Changes in the global risk landscape also offer new opportunities, as firms trade on their knowledge of how businesses ought best to respond. The largest law firm in the world has just set up a wholly owned subsidiary, promising more cost-effective updates on changing international cybersecurity laws. And a number of firms have established cross-practice Ebola groups to cover the web of legal issues suddenly facing their clients in many sectors due to spread of infectious disease.

Yet risk management can be a major challenge for law firms' own leaders, says Scott Nicholl, head of the stuff at Hogan Lovells. A confusing matrix of reporting lines, the cultural complexities of global expansions, and the competing voices of partnerships, create an environment where risk must assume responsibility for hard-won client service consistency.

"Experience shows there are actually few instances of firms falling down because of malpractice or negligence," says Nicholl. "But hierarchy, authority and lines of control are usually much clearer in a corporate environment. In a partnership they can be open to interpretation, at best."

Nicholl should know – he arrived at the firm from Aon Global Risk Consulting (formerly he was at competitor Marsh) in 2011 – the early days of the SRA's outcomes-focused regulation, which replaced the rulebook with a responsibility to judge the controls needed for your firm's own sphere of activity.

"The sector had gone through a lot of change, I was interested in the risks associated with that, and this was an opportunity to formalise examples of good risk management in a new environment," he says.

Need for speed

Law firms have sought to implement practices or tools that can help them combat a tendency toward siloed working for some time – whether because of traditional practice group separation, or simply a lack of oversight as to who's doing what day-to-day. This is desirable not just from a business development perspective (missing fewer opportunities to leverage client contact points) but also to keep a watchful eye on firm-wide risk profile. A law firm is a Hydra – and to mix metaphors, the left hand needs to know what the right hand is doing.

Although he sits alongside members of the international management committee in meetings, Nicholl sees this as a challenge for risk. "I'm not a lawyer, and I think lawyers sometimes see compliance as something that'll slow them down" – in a worst-case scenario, something that will cost a client. "They believe they'll be on the receiving end of a lot of questions – and of course there's an element of truth to that."

With anti-money laundering checks, for example, due diligence requirements vary by jurisdiction. Hogan Lovells will typically apply the highest standard internationally regardless – but that means potentially introducing competitive business risk, as some organisations in other jurisdictions won't. "It means we may take longer to accept and open a new client, and that can prove frustrating for partners," says Nicholl.

A related potential conflict is the lawyer's understandable desire to please an existing client. "Partners tend to be very reluctant to tell a client they can't or won't do something," he says. "They want the work, of course, and err toward agreeing to any demands in the guidelines for outside counsel."

The key is to recognise – and communicate – that it isn't about slowing down at all costs. It's about lines that can't be crossed. Nicholl's team conducts detailed analysis of all factors that might affect business, and creates procedures for alerting and escalating incidents or errors at the appropriate time. Critically, though, these same systems must be designed not to damage productivity.

He says he tries to communicate this remit internally with a good old-fashioned metaphor – the high-performance cars partners might have a fancy for. You wouldn't push them to their limits without good brakes to slow things down when necessary. Likewise, legal work.

"Rather than a handbrake that's permanently on, risk brakes need to come in and out at the right time, perhaps halting things completely, but fundamentally keeping control over the whole course. If the risk environment is right, individuals and groups are enabled, encouraged – and rewarded – for the right risk-taking behaviours.

"To be competitive, we want to manage that dynamic better than our peers, and to do that we need structure and definition about what's an appropriate risk, and when and how to seek guidance." That's across the firm's various jurisdictional, cultural and language differences – providing a common understanding of risk internationally.

Big picture thinking

Risk assessment covers local and global threats in a range of categories – those that might be controlled with race-level brakes, but also scenarios more likely to be prepared for than prevented. A global pandemic or spread of infectious disease, for example, is something that has risen up the ranks of risks to global business continuity – and to take it topical, many a business will have had an eye on the Ebola headlines.

"We adapted our policy in terms of who could go where – and I know a peer group firm spent time developing plans should someone feel unwell at an Africa practice group seminar in London last year."

"These are things that need constant monitoring, as a situation can change very quickly. But you can't know exactly what you'll need to do to respond, so it's about building in resilience. That means preparing to be able to respond quickly to an unexpected event, irrespective of the cause or the impact."

Geopolitical risks are also potential resilience tests. EU-US sanctions against Russia and the unfolding of the Eurozone currency crisis have been high on his watchlist. With offices in Madrid and Alicante, a Spanish exit from the euro could have been problematic, he says, both in terms of remuneration arrangements and changes to terms of engagement with clients.

He says Hogan Lovells is increasingly using scenario-planning exercises to assess its resilience. "We need to understand the potential outcomes, the different options for dealing with them, and what we could be doing now, either to influence those different outcomes, or to be better prepared for the likely outcome."

But there's also potential danger lurking in internal workplace politics – owing to factors such as societal shifts. Risk needs to liaise with HR and training departments – for example, surrounding the much-discussed behaviour of Generation Y, says Nicholl.

"In the past, you'd come to a firm as a trainee, work hard, and consider yourself lucky if you became a partner. You'd be on lockstep, and go on until you gracefully retire. A younger generation's expectations may not necessarily align with that now."

Different priorities – for work/life balance or more varied work, say – means recruitment and retention need to be on the risk radar too. Firms may need to create new career paths and plans, benefits and incentives, to compete with businesses that offer more alternatives – or even a non-traditional law firm model, such as virtual freelancing.

Data damage

Even decisions taken to address risks can have ramifications. For example, if employees are offered flexible working arrangements, Nicholl needs to consider a younger generation's often dramatically different relationship with the technology it uses.

"Lives today are often so much more open on social media, and there's an obvious conflict with the confidentiality at the very heart of how a lawyer behaves," he says. "Bright people make some very obvious mistakes surrounding confidentiality – and one main weakness we all still have in terms of overall security is simply people. The way we want people to work won't necessarily be seen as the easiest or most productive option."

It comes back to time – tasks taking those three minutes longer. And risk of data transfer with unknown variables increases when global travel is involved.

"There are jurisdictions where we know chances are high people will have their iPhone cloned by the time they reach their car at the airport. Lawyers need to be productive on the move, but in giving flexibility we're also inherently exposing ourselves to risk.

"Conflicting situations like that need to be managed mimecast®

More Law Firms Simplify Their Email with Mimecast

Law Firms Choose Mimecast for:

- Bottomless Mailboxes
- Secure Sending/ Receiving of Large Files
- Data Leak Prevenion and Encryption
- Anti-Spear Phising
- 100% Uptime
- User Productivity and Mobility

To find out more contact us
+44 (0)207 847 8700
www.mimecast.com

SECURITY ARCHIVING CONTINUITY

in a realistic way – allowing fee earners to do what they need to do, but providing sufficient assurance so we can't be deemed to have been negligent," says Nicholl.

Information security is another area likely to come up in client procurement guidelines. Hogan Lovells is accredited against the ISO 27001 information security management standard, but Nicholl says the real challenge is to understand clients' concerns and demonstrate the ability to address them.

As with over-promising, lawyers might need some help here. He says he doesn't want to "risk offending any lawyers", but some "might not be as well versed in some of the business management disciplines that are running parallel to their work".

And then there's the risk of people behaving really badly, on purpose. One data threat readers might not have thought about (but certainly up there in the USA, says Nicholl) is unwitting involvement in the next big case of insider trading.

"Firms are party to lots of very sensitive information. It mightn't even be a fee earner involved in the transaction, but a clever IT support assistant or billing officer who has realised a document management system gives them access to material in the M&A department. There have already been instances where that has been identified, and people have been prosecuted accordingly."

Age of uncertainty

What becomes clear is that the very practices and tools that can create a competitive edge for Hogan Lovells also create corresponding risks.

Control of knowledge sharing, for instance, needs to strike a balance between risk of inappropriate data use and leveraging collaborative, connected working with precedents across an international network.

And then there's the paperless transition. "A traditional hard copy file had a lot of secretaries around to ensure it was well documented, and archived so it could be quickly retrieved," Nicholl explains. "That was straightforward, and in 10 years' time I'd like to think the process would be relatively straightforward again.

"The challenge at the moment is we are in transition. Inevitably we have a mix of hard copy files and a variety of electronic documents, whether in email inboxes, systems, network drives, or data rooms. We have a host of sources that combine to create our complete file."

"Bright people make some very obvious mistakes surrounding confidentiality – and one main weakness we all still have in terms of overall security is simply people."

Of course, this all takes place in a legal services market that seems to be changing apace whatever your specialism. **Briefing** says outsourcing models and other channels for reconstituting legal work are here to stay – and Nicholl agrees. Inevitably, the more hands on a piece of work, the higher the risk one of them will err. And complex global supply chains can be disrupted by changes to local regulation. "A local bar with quite a protectionist approach might begin to regard something as unauthorised practice of law locally," he says.

Making the difference

A whistle-stop tour of the gamut of global and internal risk is all very well, but it's Nicholl's job to make sense of this with structure and systems that stop things before they snowball – if not spot them before they strike. So where to begin?

Given the regulator's new approach and the legal mind's tendency to find (and possibly exploit) loopholes, he says the main changes he has introduced have concerned improving awareness of risk and influencing everyday behaviours.

"One issue is ensuring people know when to escalate something, but without being too prescriptive, and allowing partners and practice groups a certain degree of autonomy to work in the way most sensible for them.

"We'll form a risk profile – and use that to decide and articulate risk appetite. We work to understand relationships between risks, so we can focus resources on those with potential to cause most damage. But the crux is to ensure 800 partners each understand the firm's risk tolerance."

Local engagement and learning is particularly important. London's appetite will look rather different to that faced by a new practice group developer opening up shop in less familiar territory, for example.

"All offices will periodically have a risk review to assure senior management that local risks are being appropriately controlled," Nicholl says. "I'll make recommendations to the office managing partner and others about any gaps – and then undertake regular monitoring to make sure any changes are having the desired effect." Similar audits could be scheduled for risks to which a particular practice group or project is exposed – a new IT system or business process, for example.

An important tool for checking that understanding is testing business continuity plans. Weak points in the armour are identified, leading to priorities for investment or future training. Plans are tailored to local office circumstances – both their most likely risks (earthquakes in Tokyo, for example) and the extent of access to technology and infrastructure.

To test resilience, Nicholl's exercises place special emphasis on the unknown – testing staff judgment as well as procedures and resources. "We drip feed parts of a hypothetical scenario to simulate how an event evolves. Rather than knowing everything at the outset, people have to think without access to the full facts. We can assess how well they respond and what could be done differently.

"It's also often only when you test a plan you realise there's an unrealistic assumption, or that a key contact detail has been overlooked."

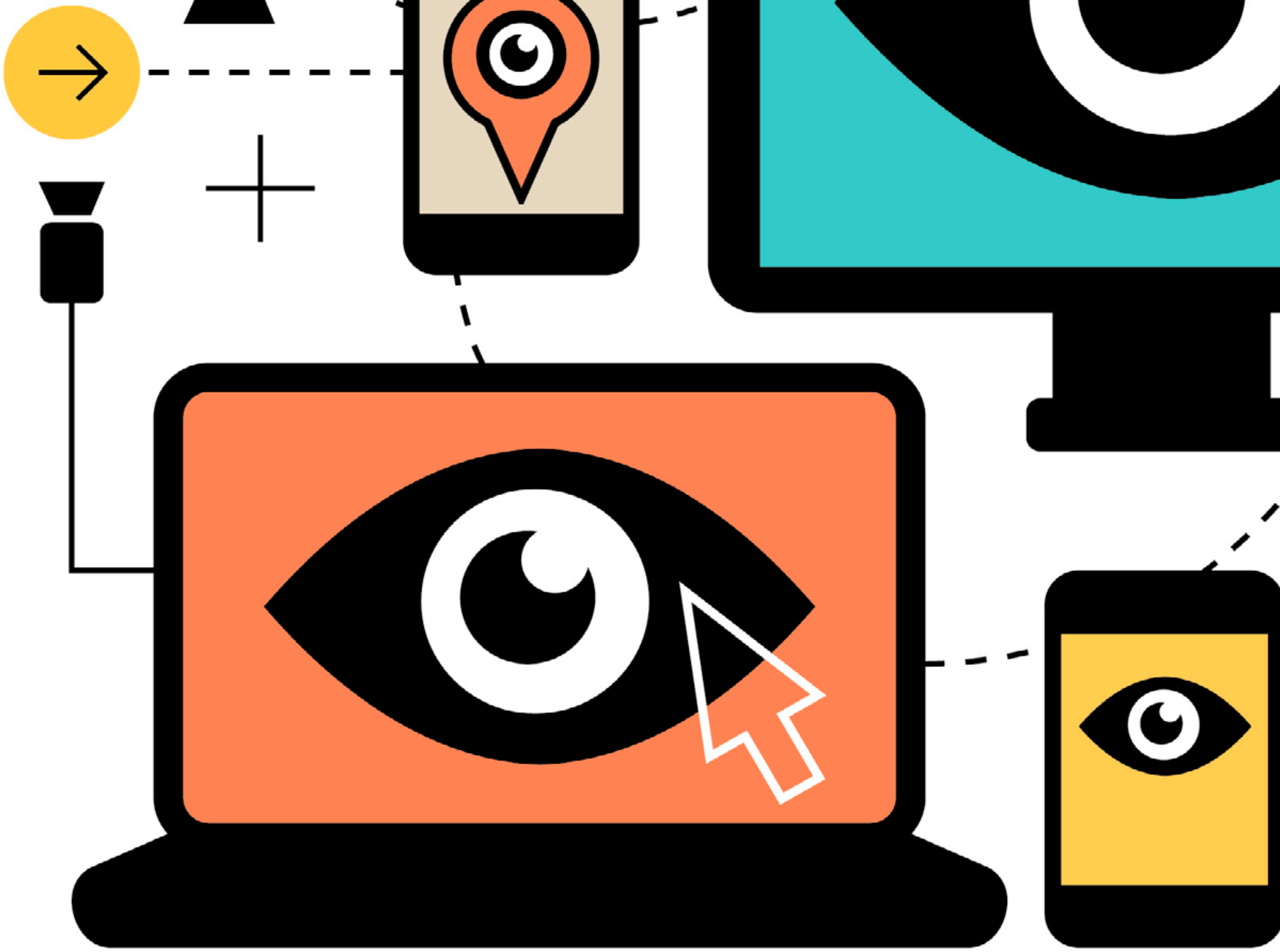
Nicholl's office reviews check the right plans are in place, that they've been updated and tested, that they're available in several locations, and that people are competent to action them.

In general, his business continuity planning also evolves as new risks rise up the register. For example, in London he recently scripted a scenario where the firm was targeted because of work for a controversial client. Protesters turned up on the street outside, but 'hacktivists' had also managed to deface the website in a bid to inflict reputational damage. As the morning unfolded, some protestors also managed to access work computers, testing not only how employee safety was managed, but whether the intruders could log on and access confidential data.

"We need to recognise that the ways we could be interrupted are changing," says Nicholl. "In many scenarios our offices could be fine physically, but a cyber attack might damage hardware. A pandemic might mean people aren't able to work at an office, either because they're ill or if they can't or won't travel."

But day-to-day risk-management culture is just as important as how you act in crisis mode. After all, like insurance, it's PR and brand power built up in good times that can have a buffer effect if serious trouble does ever darken your door. "There have been a number of cases where how a company is perceived publicly in advance has enabled recovery or lessened damage after an incident," explains Nicholl.

The right risk, well managed, can also present an opportunity. Risk needs to work with marketing to leverage their skills and dynamic in full – without letting them tamper with the brakes, of course! ●



Eyes everywhere

Whether expanding overseas or running a UK-only business, exposure to an ever-shifting range of natural and criminal shocks can cause serious damage. Richard Brent goes looking for some lessons for law firms when preparing for the worst

The headlines and hashtags stamping the first month of 2015 reveal a world both volatile and vulnerable.

A British nurse, cleared to travel across the UK from Morocco, was later diagnosed with Ebola and admitted to a London hospital. The Economist Intelligence Group flagged up potential for "political earthquakes" after polls across Europe – in the now firmly anti-austerity Greece, as well as Spain, Germany, Ireland, and indeed the UK. Over in the USA president Obama has again outlined proposals to help track down cyber criminals (a day after military command's Twitter account was successfully hacked). He will now embark on cyber 'war games' with the UK, simulating attacks on financial services businesses lining Wall Street and the Square Mile. North

Korea, meanwhile, may or may not be at war with Sony Pictures.

And – of course – business vulnerability to geopolitical and terrorist risk was horrifically highlighted in the tragic attack on a small Parisian publishing company.

Such threats to stability are regularly assessed and ranked by interested organisations – and in an increasingly connected business world, every law firm needs to consider its exposure, and plan how it would respond if affected by a major incident. In legal service delivery, specifically, as new markets are assessed and work becomes more globally distributed to drive down costs, risk profiles require regular updating – striking a careful balance between the comprehensive and the concise.

Registering responsibility

It's telling that alongside "fiscal crises in key economies", "greater incidence of extreme weather" and "profound political and social instability", one of the 10 top risks in a World Economic Forum report in 2014 was "global governance failure". Poor risk management is itself one of the biggest dangers we face.

But improving isn't just about adding to an ever-growing list of threats. Andrew Cheung, general counsel for the UKMEA region at Dentons, says the firm revised its approach to risk to become more "dynamic" in 2012 – by slimming down a risk register to the 20 "top risks for the board to address in any given year". Each has a "risk owner" so accountability is clear and ensuring the firm is engaged with the most business-critical.

"Responsibility forms part of each risk owner's job description. They have to sign off on risk control sheets, certifying their effectiveness to management, as part of their annual performance appraisal," says Cheung. "It's quite a big change, but we realised engagement around risk is challenging if you don't properly incentivise people and make it clearly business relevant.

"We recognised that at the heart of good risk management is transparency and effective governance – and we found some of the biggest risks to the organisation were ones that weren't clearly owned by a single person or department, but fell between the stalls.

"It's particularly relevant in times of rapid change. Assumptions can be made about who's responsible for what, but these may not necessarily reflect reality, giving rise to gaps. The worst outcome is if executive management or the board assume something is being dealt with when it isn't, or isn't being done in the way everyone assumes."

"Another example's cyber security – often handed to IT, but something that is multi-disciplinary, requiring input from HR and regulatory compliance, and involving leadership. Without a joined-up, clearly accountable approach, factors will be missed and the organisation won't be able to respond to risks effectively."

Brian Gray, chief of business continuity management at the United Nations, says a related risk of not having a system-wide approach is "unintentional risk transfer".

"You could also take an action that reduces your risk in one area but risks increasing somebody else's. For example, reducing IT infrastructure to save money can increase risk elsewhere if business-critical processes can't access systems during an outage."

Gray – named public sector business continuity manager of the year at the Business Continuity Institute global awards last year – led development of the UN's Organisational Resilience Management System. This ties a wide range of risk programmes together, from security and business continuity to contingency planning for humanitarian disasters, across multiple geographies with dramatically different risk profiles and resources.

"Previously we had an approach where each programme was run independently of the others, but where there were overlaps, with the result that who was responsible for what wasn't clear," says Gray.

Board talk

A 2014 report from the Institute of Directors, Responding to Global Risks, also found responsibility was a key issue – but that while significant strategic risk monitoring ought to lie with board members, they often struggled with non-company specific, or systemic, risks.

Dr Roger Barker, director of corporate governance and professional standards at the IoD, recommends clearly splitting responsibility for macro and operational risks between the board and specialists respectively.

"The board needs to recognise it's more involved in oversight than direct risk management – making sure control mechanisms are in place but not necessarily undertaking them itself.

"The boardroom should directly engage with big picture political risks – the fundamental things that can sink an organisation. In the case of the banks, for example, what to do when they couldn't access the wholesale money markets? Or what's going to happen to the oil price over the next six months?

"Of course, that will draw on other people in the organisation to give background briefings so the board can debate them properly. They may also look to external experts to provide input. But they're too important to be delegated to a risk manager."

It's also important for a board to have direct lines of communication with risk managers and activity at the coalface. "There can be a tendency for a CEO or CFO to manage all information flow from employees on up to the board," Barker says. "It can place a board in quite a vulnerable position if everything has the potential to be controlled by management."

The IoD's report recommends "breaking the risk management glass ceiling", nurturing a "no blame" culture of trust and communication with all employees, including potential whistleblowers.

"In the financial crisis a lot of the banks had very sophisticated risk management systems. The problem was the information didn't get up to the board – or when it did, it wasn't presented in a digestible way to allow appreciation of the true risks," explains Barker.

He says an ideal corporate board will also have either a risk or an audit committee. The internal audit department would supply it with findings separately to the CEO. The audit committee would comprise chiefly non-executive directors – and the dual reporting line makes it crystal clear internal audit isn't just serving the interests of senior executives.

Emma Dowden, operations and best practice director at Burges Salmon, also agrees risk management demands both clear responsibilities and effective communication to all corners of a firm. As well as introducing new roles to support her risk committee's COLP (the managing partner) and COFA (the finance director), she has a network of lawyers, senior associate representatives, responsible for driving risk awareness within each practice.

"They're a point of contact to communicate key messages and feed any issues back. They have a job description, I meet them monthly, and they are measured against performance as part of their annual review," she says.

"We've also recruited an internal auditor, where previously we were predominantly using outside specialists. We've found it beneficial to bring that function in-house."

The firm's risk committee also meets monthly – more frequently if there's a new matter referral – and refreshes the risk register at least annually, with partner representation from each practice.

Online experience

As businesses where decision-making is complicated more by multiple owners, a good governance model is critical to law firms' consideration of their risk appetites. But they need people with a broader knowledge base as risks change. A number have now appointed non-executive directors to benefit from greater breadth of business experience. However, PwC's annual law firm survey has also since found internal audit functions are generally under-strength when compared to similar sized businesses.

In the wider business world the gender diversity of boards has been a particular focal point. The Davies review seeks to increase the number of women on them in the UK using a voluntary approach rather than quotas. But Barker stresses that experience in emerging risk areas should also be a recruitment priority.

"Cyber security is a big issue," he says. "It's a growing vulnerability for companies, but often people sitting on boards don't have much experience or knowledge of the area. We're in a transition period where they're scrambling to try to identify the people who could join and provide input."

Increasingly reliant on digital business in a more connected world, PwC's survey identified law firms as a "weak link" for sophisticated cyber criminals – 5% dealing with staff-related security incidents every week. In its July risk outlook the SRA also highlighted cybercrime and information security as a new priority risk. And in August last year the Information Commissioner's Office singled out law firms for a one-off public warning about protection of client data – and the SRA points out confidentiality breaches are probably under-reported, as firms won't know they've been affected.

"Cyber security is an immediate and serious risk for firms," agrees Cheung. "There is civil liability that can flow from these sorts of attacks, there's loss of business through denial of service, and huge potential damage to brand. And we're not just a direct target – we can be indirectly hit through attacks on clients and suppliers."

John Verry, risk director at TLT, has recently established both an internal audit team and a raft of new information security procedures in line with international standard ISO 27001. The first – to help it adapt to the world of outcomes-focused regulation, where risk assessment must be tailored to a firm's client profile. "Risk has had to become more proactive – policing how people behave and what they achieve for clients, rather than, perhaps, waiting for something to go wrong," he says. Certification to the security standard has been driven by greater awareness of likely breaches at TLT, but also by clients. "They have expectations you'll function in a way that allows them to meet their own regulatory requirements," says Verry.

In addition to more complex firewalls, a comprehensive security breach register and regular reviews, his changes have focused on reformatting behaviour.

"People will now challenge any strangers on the floor. One risk is third parties – anyone from cleaners to security guards – having sight of sensitive information. They are far more focused on security as a personal responsibility," he says. A clean-desk policy also encourages all hard copy work to be locked away at night – and recognises security is just as much about protecting paperwork as petabytes. As well as encryption, the ICO's warning to firms highlighted paper file storage, as well as people taking client information when leaving a firm.

Growing pains

Cleaners and paperwork illustrate that risk is no respecter of size. You don't need offices in conflict zones, or multiple outsourcing arrangements on the go, to be in trouble – although risk profile inevitably shifts as a firm grows.

At Birketts, for example – which now has four offices and a new policy on scam emails (another risk in the SRA's latest outlook is 'bogus firms' – criminals robbing firms' identities in a bid to dupe consumers).

"Asking for £10,000 to send to Nigeria doesn't work so well now, but law firms tend to be trusted. People often won't question it," says risk and compliance director Sarah Ralph. Birketts is therefore regularly checking the firm's and individuals' names online, as the SRA suggests.

Sarah arrived at Birketts from Lloyds Banking Group in 2010 – coinciding not only with the arrival of OFR in law, but also the dramatic realisation of a lighter-touch regime's limits in financial services. She says much of her role is driving greater risk awareness, often with a smattering of 'war stories' from her days in banking.

"I came across accustomed to a highly regulated environment – but here a lot of it's about changing the mindset of the fee earner," she says. For example, she runs roadshows dedicated to key risks, touring around the offices and specifically bringing fee earners and secretaries together for holistic and hands-on training.

"That works much better than just sending an email for people to roll their eyes at," she says. "Induction training is also important."

Most recently she compiled a roadshow on money laundering – yet another current SRA priority risk owing to a high proportion of poor quality suspicious activity reports filed with the National Crime Agency.

"Initial money laundering targets, such as the banks, are now a lot harder for criminals to get past – so they're focusing elsewhere," she says. "There's also a danger that regional law firms think it's really a City issue. Our intranet sets out some key examples of where firms have been caught out."

Burges Salmon has embarked on a programme of cross-firm training on money laundering too. "It occurs to us that secretaries are often gatekeepers to clients, assisting with filling out file-opening forms or helping with queries," says Dowden. "They do need to be alert to the same things as the lawyers."

Sarah Ralph stresses risk is just as much about tackling behaviours that may be second nature – on email, social media, or even in person. "Chatting about a client on the bus home is a security threat," she says. "Even if you don't use the name, the wrong person can put two and two together."

Chain reactions

It's a good example of how risk managers really need to consider the widest chain of outcomes possible. Business continuity plans activated in the event of an incident then need to factor this in to create a certain degree of organisational 'resilience'.

"Risks can seem to come from nowhere," says the IoD's Barker. "It's obvious we don't have perfect foresight. While there are 'black swan' events that have a potentially huge impact but are very unlikely, as a general rule you also want to build some margin of error into an organisation.

"With diseases like avian flu or Ebola you can have a policy in place – but often you have to wait and see what happens," says TLT's Verry. "You need to be flexible. A good business continuity policy ought to include ensuring people can work seamlessly from home."

But then there's the question of how employees are really likely to behave in the event of a mass panic as a situation escalates. One tool being used more for events that couldn't be prevented is scenario planning. "There are a range of possible outcomes, and a likely gap in the organisation's ability to deal with the most extreme," Barker says. "You then have to consider how to mitigate them, either with some control mechanism, or possibly by exiting an activity or trying to insure yourself.

"It has become more common in the financial sector in particular – stress testing, for example, to see whether a bank has sufficient capital reserves to cover potential liabilities in extreme circumstances."

Wayne Behrens, vice president of enterprise business resilience at Franklin Templeton Investments, says: "We draw upon our strength as a global organisation, where understanding our options for shifting work to alternate sites is key. Franklin Templeton won the Business Continuity Institute award for team of the year. "With a few exceptions, we take an 'all risk' approach. Our plans are designed to work no matter what the cause.

"In crisis management and business continuity we have assigned planners by region. Regional risk committees help ensure we are looking at the right risks and that our mitigation plans meet not only local business unit needs, but also address regional and local legal entity concerns. We vary exercise scenarios to keep it engaging and tailor them to ensure it's appropriate to the site. In 2014 Ebola was top of many people's concerns and had 'ripped from the headlines' appeal. We used an Ebola scenario in our table-top

> *"Chatting about a client on the bus home is a security threat. Even if you don't use the name, the wrong person can put two and two together."*
>
> Sarah Ralph, risk and compliance director, Birketts

exercises to ensure local emergency management teams understood the issues."

But is knowing and testing your own risk exposure even enough? Business continuity best practice now also often extends to considering key risks and relative resilience in your supply chain. Dowden, for example deliberated about contractors returning to affected areas such as Sierra Leone for Christmas. "We made sure our suppliers set up appropriate controls to avoid any outbreak in the building," she says.

"Malware can be present [undetected] for many months, perhaps a year – potentially impacting many businesses that work together," says Dentons' Cheung.

Law firms could possibly take a leaf out of their clients' books here. "There seems to be a trend for clients not only to probe information security, but to perhaps hire a third party organisation to visit and audit systems to see for themselves," says Dowden.

Verry says TLT's business continuity has been beefed up as part of ISO 27001, including external penetration testing. "Clients want to know when and how we test – and sometimes even to be present at a test. And quite right too – to check a main supplier could continue to provide service in the event of an adverse incident."

A simpler system

Business continuity rose up the agenda at the UN during the pandemic threat of 2006 – but it was the Haiti earthquake in 2010 that really made the organisation realise it needed to revise its approach to risk.

"The huge loss of life and impact on survivors made us realise we needed to dedicate more policy and support to those affected, not just by natural hazards, but also by malicious acts," explains Gray.

"If a staff member or family member is killed or injured, we need to support the family and integrate recovering staff members back into the organisation." The UN General Assembly set up a new emergency preparedness and support team to handle such issues – and arrived at an emergency framework that more clearly articulated interrelationships and responsibilities.

At the same time, the devastation wrought by storm Sandy in 2012 has since ushered in a new initiative to optimise crisis communications.

"You need to dedicate specific thinking to crisis lifecycle – and therefore which sort of messages should be sent at which stage, and how," says Gray. "For example, people may pick up information in different ways when under extreme stress."

Such flexibility runs through the Organisational Resilience Management System. Risk assessment, for example, is static – potential disruptions in a given location are assessed for prevention and mitigation measures annually. But it's also dynamic, as a core group (comprising business continuity, IT, HR, facilities and security) continually assesses emerging risks and presents a recommendation if a new action is needed.

The same goes for exercises such as disaster recovery and business continuity testing and awareness campaigns. "New technology comes in, and people change jobs. You need to maintain the plan and constantly exercise and update things," says Gray.

He also stresses that, to be successful, emergency plans need to be woven into business as usual. Home working, for example. "There are many reasons telecommuting makes business sense day to day, and if you really can't come into the office it should be a way of working staff are used to.

"We're constantly trying to find ways to integrate our messaging into what the organisation does every day."

Another key UN innovation is using informal networks as well as formal channels to share practices and lessons as part of what Gray calls an emergent rather than top-down strategy.

"We have a collaborative platform, and anyone who wants to can be involved and share experiences and ideas about how to make something better locally. We can then make changes quickly if somebody comes up with a simpler format, for example."

And for all the complexity of risk registers and varying appetites, ultimately management also has to drill down into something resembling simplicity. Crisis management can, after all, be as much about saving lives as business – and time is also of the essence in saving reputation.

"If you have 50 critical processes, that's 50 separate tests to run, which carries some consequences," says Gray.

"What I need, especially if I'm in a smaller country office with fewer resources, is a checklist of the essential things to do that I can easily use when I'm running out of a burning building!" ●

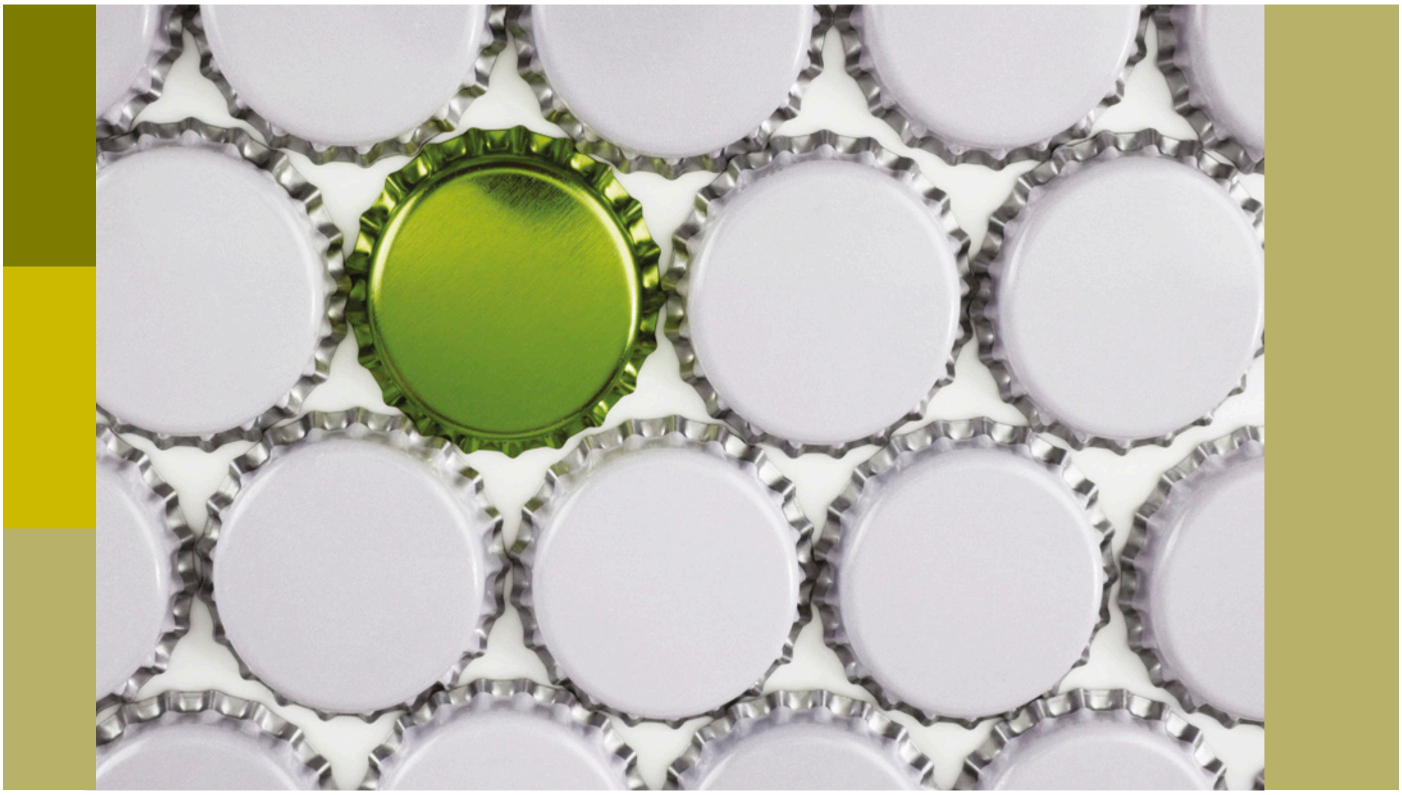
informance.co.uk | See Informance at @BritishLegalIT

WHAT WILL YOU DISCOVER?

Improve risk management throughout your firm and take a structured and consistent approach to compliance with QlikView Business Discovery.

Our QlikView risk management dashboard informs compliance officers regularly on potential matter and client risk scenarios, enabling your firm to keep control of risk.

- Instant monitoring and management of risk compliance
- Clear understanding of risk integrated with daily operations
- Automated risk alerts and rankings
- Configurable and weighted risk analysis according to profiles
- Improved KPI compliance



Qlik™

informance®

Informance Ltd, Warwick Technology Park, Gallows Hill, Warwick CV34 6UW
Telephone: 01926 623456 Email: cathryn.hunter@informance.co.uk
www.informance.co.uk

Qlik Partner Solution Provider

Risk and reward

INDUSTRY ANALYSIS INDEX

Briefing Industry Case Study

Checks and balancing acts

New conflicts management software hasn't just cut down the risk of Eversheds taking on the wrong client, says head of operations, Kerry Kendal – it has lessened the risk of the firm losing the right one

Conflicts management is the cornerstone of compliance – and increasingly a critical element both in improving client service and profitability. When a lawyer begins a new matter – for a new or existing client – that always triggers a conflicts search, but all too often in larger firms this can happen without a solid 'big picture' view of current activity across the firm's relationships. That means that not only is business acceptance a due diligence risk, it could also end up stopping a firm taking on a client that could be very important to its strategic future.

Improving the process depends on detailed and accurate understanding of high-quality data – presented to people in the right form, and at the right time, to help them make the right decisions.

But until turning to new technology to assist, Kerry Kendal, head of operations at Eversheds, found she had both too much data and not enough refined information on her hands.

"The problem was we couldn't strip any information out of the conflicts reports we generated," Kendal explains. "Everything we found for one of our big clients had to stay in there for the next analysis phase. We could easily end up with 3,000 results, creating 300 pages for somebody to painstakingly sift through manually."

That "somebody" could often be a lawyer – and the process took valuable time that could have been spent developing more business, as well as posing a risk. Information presented to decision-makers needs to be as clean and as clear as possible to minimise the inevitable creeping risk of human error. The more irrelevant raw data included in a report, the greater the risk the most important warning flag is missed. "You can develop a false sense of security if the most important result has been pushed half-way down the list," Kendal says.

Worse, in process and efficiency terms, her team couldn't refer to details from past searches to see if similar checks had been undertaken. Everything had to be done afresh, with partners manually looking up client and financial data each and every time. "There was no record of our institutional knowledge from across the firm," she says.

What's in a name?

Eversheds turned to Intapp Open to get past these barriers to business acceptance nirvana. Now, the Eversheds conflicts and compliance team is able to create much shorter reports that automatically flag up the highest-priority results and issues for consideration, for lawyers to review.

"What made it a real winner was the way we can now create our own rules for searches – calling up everything that falls within certain sets of criteria but excluding others," says Kendal. As an example, she says, the team can cut out all closed matter data that is over five years old. "It might be useful to see that somebody else had run a search against a client in the last three months, but you probably wouldn't want to see that information from seven or eight years ago."

Another option is to filter by definition. Client entities can come under different guises – local authorities being one good example. "You might need data on a local council, a county council, a borough or a government entity. There are lots of different names. Previously one of my team would have needed to key all that in manually, but we have created a rule that stipulates every time we search a word like 'county', we automatically search the other 12 variations."

At the same time, the reports offer more instant management visibility into progress in an area, she says. "Each report has a useful summary section at the very top, stating which criteria were searched against and when. It's a lot more streamlined and efficient."

Raising up the ranks

Using Intapp Open also means Eversheds could change the way the risk department is structured to be more cost-effective. A new 'business acceptance unit' now focuses more energy on ensuring the firm is targeting the right clients in the first place – in line with strategy, as well as with the goal of keeping an eye on their basic financial health and possible future risk.

"Before Intapp, I had a team of four 'conflict administrators' whose job was purely to pick a search term and plug it into the database to create a report," says Kendal. "They did no stripping out or checking, but just sent it all back to the lawyer to assess and clear. I wanted to introduce a team of people who had core expertise in clearing conflicts and who could undertake that activity for the lawyers, but the data volumes we were previously experiencing made progress so slow, you would have needed a team of 20 or so. These days, there's just no way you could get that size of support model signed off."

Those analysts would also have been tied to spreadsheets, working to collate and manage their information, and the process would remain heavily dependent on individual memory of issues such as various exclusivity arrangements, conflict waivers and outside counsel policies.

The goal was for Eversheds lawyers to spend less time churning through conflicts data and more time focusing on the ideal clients to work for in terms of the firm's objectives. "We have a client strategy, like all firms, but often you can get caught up in lots of smaller instructions to an extent that can be counter-productive to that overall strategy," Kendal explains. "If you are looking to expand into a sector, such as healthcare, for example, acting for a regulator in the sector at the same time would be quite damaging. But if your focus is local government, a regulator as a client might be particularly productive. You want to know where conflict rules prohibit you from working, but also to maximise your opportunities for growth where they don't."

Project push

Intapp software helped Kendal demonstrate just what was possible with more efficient utilisation of resources. Feedback from the business was so positive that she secured senior management buy-in to expand her team of specialists to eight analysts, a conflicts manager and a new business acceptance manager in a matter of months.

The implementation has been so quick (from contract to live in a year), and insight so instant that the project has won Kendal an annual internal firm award too – for best overall project delivery.

Moreover, the business benefits have led to Kendal being charged with pushing both the technology and new team structure out into the Eversheds network of international offices to drive yet more efficiency.

"The feedback we've had from across the whole business has been fantastic," she says. "On the most fundamental level they love that the administrative groundwork of going through lengthy reports has been cut out. They don't need to go back to other partners in person to query conflict hits, or worry about what they need to do if a particular person isn't available.

"But most eye-opening has been how conflicts are at the crux of commercial decisions about the clients you want," she says.

"By getting a greater feel for connections in all the work we're doing, we have successfully engaged people in that conversation. They recognise conflicts isn't just an administrative compliance matter. If you take on the wrong piece of work, it can prohibit you from taking on the right one."

Industry Analysis

Content critical

Information risk management requires consideration of the complete content lifecycle, says Bryan Gilbert, enterprise account director at Konica Minolta

How do you deal with the risks associated with receiving, processing and managing information from a growing number of sources, particularly in today's complex global business environment? Indeed, how do you make informed decisions around risks, when the volume of information increases tenfold on a regular basis, and is stored in a variety of ways – email, SharePoint, desktop folders, and so on. Our advice to customers is to have a robust risk management strategy.

That's easy to say, but we've evaluated some of our recent engagements to understand the operational and strategic concerns clients experience that impact their exposure to risk.

In doing so, we've learned that many law firms are concerned with navigating their exposure to risk associated with accessing data and information sources, including those of clients and partners, particularly in global and mobile environments where offshoring and outsourcing is commonplace.

Also high on the list is the move to fixed fees rather than the billable hour, while ensuring matters remain profitable. And alongside this there's the challenge of retaining company processes as career mobility increases and partners move more frequently.

While information, data and document security is always paramount, how do you manage the associated risks that come from being exposed to these trends? Set against a backdrop of having to adhere to regulatory compliance and your clients' requirements in relation to data retention and destruction, this is no easy undertaking. Firms should therefore implement robust processes and workflow to deliver acceptable risk assurances.

This is caveated with the need to ensure autonomy for stakeholders to continue to operate effectively, when, where and how they need to. Firms need to apply the brakes quicker, and with greater intelligence, where risk parameters are breached – which is where having a risk management strategy comes into play.

Content with culture

At Konica Minolta we find enterprise content management (ECM) is a critical tool for helping customers to mitigate potential risk, ensuring compliance and governance. A well-defined ECM strategy can help any firm optimise internal and external communication processes. A strategy needs to encompass the complete content lifecycle – from document digitisation, extraction of key data, storage of content in a single repository and application of automated rules and alerts, to delivery of information at the right time, in the right place, and in the required format.

ECM aims also to improve business intelligence by providing a single portal where all information can be accessed regardless of where content originated or currently resides. This in turn speeds up the decision-making process. Many of our clients say speed of access to information is key to improving risk management.

A key reason many organisations are now looking to take a more holistic approach to ECM is that the benefits are wide-reaching – they don't address just one area of strategy, but the entire approach and culture.

But many find it overwhelming when initially embarking on an ECM strategy, usually due to the vast number of data sources and processes that need to be considered, as well as ingrained cultural practices, which are usually the hardest element to resolve. We address this by aligning our services with customer requirements through three levels of defined consultancy service – output analysis, document process study and business process optimisation. We work from output analysis, to comprehensive business process engineering. In doing so, organisations can break processes into manageable areas and address the most business-critical – not only offering the greatest return but also having the most immediate impact on other, lesser processes. This, in turn, drives quicker impact in addressing legacy culture and working practices across the entire enterprise.

There are five key elements to addressing your ECM strategy:

Capture: Whether information is in the form of hard copy documents or electronic files, you need to consider how to make capture and digitisation quick and easy.

Manage: Automate content lifecycles through workflow. Within the relevant process, define and map current workflow, and define the desired future state. Ensure relevant automated authority and sign-off is inherent in workflows so that authorisation is given before any document becomes part of the content repository.

Store: Consider what works best for your specific organisation. For example, do you want to manage your document repository in-house, take advantage of a cloud solution, or simply deliver a central portal that enables users to search and access multiple data sources securely and efficiently?

Preservation: As well as how documents and information will be stored and accessed, it's vital to consider how long you need to retain information for. Not only are there cost implications for storing ever-increasing amounts of electronic data and the obvious data protection compliance, but an increasing number of organisations need to show compliance with clients' data retention and destruction criteria.

Deliver: Access to information should be seamless, providing extensive search capabilities and link to line-of-business applications.

ECM should play a key role in law firm risk management strategy. It will help ensure faster and simultaneous access to mission-critical data. Content workflows can be implemented, inefficient and manual processes are automated and auditable, and meaningful knowledge must be made available from disparate systems via a single portal.

works within folder structure
Global Vs Local conflicts in orgs
Tasks - reviewing large docs letters to regulators calls to ext. lawyers
Fave apps Uber 'clever little gadget' password app Sky
Loves Uber efficiency cost saving 'clever'
iphone 5 ipad (work) laptop (work)
Has 20 deals on currently

Briefing Industry Interview

Information overload

Being drowned in email not only risks security and lost productivity, but also retention of the talent tasked with wading through it, says Workshare CEO Anthony Foy

Over the years that the credit crunch has dissipated into a new, more austere reality, firms have increasingly been trying to offer clients more predictable pricing arrangements that still keep them in profit – but this is only one way they may need to respond to the mounting competitive risk new players in the legal market pose.

"Every aspect of a law firm's business needs to be focused on efficiency as well as profitability," says Workshare CEO Anthony Foy. "Firms are challenged by new business models and ways to charge – and many services are being standardised and templated online. But creation and review cycles of documents also need to be more customer-focused, and quicker.

When things take much longer to complete, it just isn't acceptable to clients." For example, if a client demands to use a consumer-grade file-sharing application for their transaction, the result either exposes the firm to physical risk if it complies, or competitive risk when it fails to provide an intuitive alternative.

Technology to automate and make processes more efficient can help firms mitigate the risk of losing talented lawyers to the competition, says Foy.

"People spend years and a lot of money training as lawyers, but can find much of what they're doing is then pushing paper – trying to find multiple versions of different documents.

"They're really acting as highly paid administrators, which saps their interest and creativity. The imperative for legal businesses to become more efficient is also in the interests of their talent retention and long-term sustainability."

These are some of the reasons why Workshare has enhanced the Deltaview (redlining) technology in its new Professional 9 application, says Foy. When an email arrives from a client with a modified document attached, the lawyer is automatically alerted through Outlook.

With a few clicks they can compare the new version right next to the original, instantly accept or reject changes, individually or in all instances, before safely checking the new document back into the system of record, or Workshare's secure online environment.

Where have you been?

Automating document amendment in this way also guards against error through inconsistency – another clear risk for businesses built around continually changing sets of knowledge and content.

One challenge is that however rigid your processes and monitoring, lawyers will inevitably have working habits that are hard to break. "For example, some people will love their file and folder structure, storing things away daily – but then there are people like me who just keep it all in the inbox and search," says Foy.

For international firms, of course, collating feedback becomes more time-consuming and complicated as more locations, emails and amendments fly in. Almost nine in 10 (87%) of respondents told Workshare's survey of 200 legal professionals they therefore needed strong visibility of a document's editing history – which pushed it to the top of Professional 9's development list.

"As soon as you send out a document attached to an email, you've lost track of it," says Foy. "We can track a document back through its entire lifecycle, into the document management system or inbox, or onto the lawyer's mobile, with clear sight of the whole audit trail.

"This connected document concept means you can see who has contributed, changed and deleted what – on which device, and where."

With that information, law firms can begin to analyse and refine internal processes to make future work more efficient. "For example, you can identify which key clause gets stuck in the review process most frequently, and the lawyer who can move it on to conclusion quickest.

"If you can identify the volume and velocity of activity, and the individuals contributing to it, you get a much richer view as a base for driving change."

Cloud cover

Foy maintains that sensitive data is far safer managed in the cloud than staff inboxes in various states of increasing disarray (Workshare also offers a hybrid cloud deployment, allowing for firm and client control over data storage location).

"If lawyers attach something to an email and send it out, who knows where it goes from there? How many are forwarded to people who shouldn't have their hands on it? You can't be sure where those documents go unless you enter into litigation and put in place a data hold and discovery process."

Ringfencing document-related communication in the cloud, therefore – with added process automation – reduces both the size of your email avalanche and the risk of losing sensitive data, or key content.

The cloud creating more security, not less? Now that's really doing things differently.

Industry Analysis

Presence dangers

Firms need to do much more to drive awareness of an evolving range of mobile security risks, says James Allen at Intercity Telecom

Technology is moving forward at an increasingly fast pace – and handsets are filling up with features. As the market evolves, users are demanding devices with access to a wide range of consumer services, not just email, on a business and personal level.

From a professional perspective, mobile technology is revolutionising the way many businesses operate – and all kinds, but particularly law firms, are now benefiting from the latest advances in mobile technology. The explosion of apps, for example, which cater for everything from time recording to document production, are making legal professional lives easier. But while it is important to be aware of the benefits, it's equally important to understand the risks in such a data-sensitive sector.

One of my main concerns is that this isn't taken seriously enough. For example, it's interesting to see that mobile data gateway Wandera's recent poll of 2,000 end users found only 7% of employees are being given any form of security guidance on using apps and smartphones in general.

App settings

So what are the risks? Is it just taken for granted that data is safe? From conversations I've had, it would appear the answer is 'yes' more often than not. Apps can gain access to company data and leak this sensitive information to the outside world, so if we're talking about sensitive legal documents and contracts, this could be potentially damaging. Leading apps have been seen to transmit passwords, email addresses and even payment information, including locations.

Many people use the same login names and passwords for personal services, so it's easier for criminals to gain access to financial and personal services. It's not surprising that Gartner predicts 75% of all mobile security breaches will be the result of mobile app misconfiguration or misuse.

Malware is a common word in the laptop/PC threat world and is now beginning to take hold in the smartphone arena (with total mobile malware growth of 167% in the past year alone, according to the June 2014 McAfee Labs Threat report). Mobile malware is malicious software designed to steal personal information stored on a device by silently watching what is happening, and in some cases even gaining control of the handset. Most mobile malware spreads via malicious apps on the device, gaining extensive permissions. Trojan malware has been seen to send SMS messages to premium mobile phones services, racking up very large unauthorised charges. Information is stolen, which can lead to phishing and fraudulent activity, including identity theft and banking fraud.

Danger from within

Mobile security threats aren't always external – they can be unknowingly created by employees themselves. For example, an employee leaves a business and resets their phone before passing it on to a colleague. This is a major risk many businesses aren't aware of. Once this happens a business has no visibility of the phone's usage when it belonged to its previous owner. Other unknown risks could be as simple as visiting another office and plugging a device into Wi-Fi, spreading potential problems further.

Mobile phone loss is one of the biggest risks for firms. Britain loses around 1.5bn gadgets each year, around 190,000 people losing their mobile in the back of a London cab. It's scary to think how dangerous that could be if phones aren't secured correctly and the device with business-critical information falls into the wrong hands.

I work with a number of law firms, helping to raise awareness of mobile device security. Most recently I worked with full service law firm, BP Collins, which wanted to provide employees with a choose your own device offering, with device options including Android, BlackBerry and iPhone.

With a diverse range of handsets on offer, the law firm recognised it needed to understand how to keep them all secure. After lengthy discussions, it chose the latest BlackBerry enterprise service, which allowed it to roll out Android and iOS smartphones with a secure and containerised email solution, ensuring client data wasn't accessible from private applications, such as Facebook. Not only does the BlackBerry Enterprise Service support BlackBerry devices, it also supports iOS, Android and Windows Phone 8 devices.

> *"Leading apps have been seen to transmit passwords, email addresses and even payment information, including locations."*
>
> James Allen, professional services manager, Intercity Telecom

Firms ensure PCs and laptops are secure, but it would appear we are yet to adopt the same measures for the smartphone and tablet, and I fear this is due to lack of awareness of the risks involved. Handsets are now being used for a wide range of services, from contactless payments through to opening a hotel room door. With such sensitive data at risk, the right solutions need to be employed – and quickly – as these threats are only set to increase as the use of the mobile phone evolves.