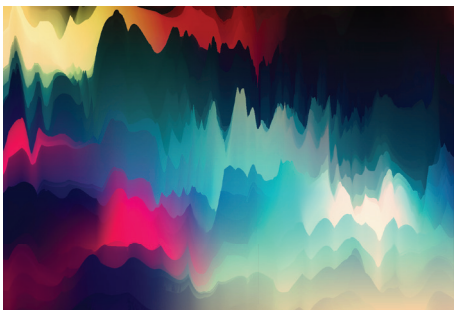
SUPPLEMENT: FEBRUARY 2022

LPM

LEGAL PRACTICE MANAGEMENT

PRACTICE HEDGING

What more can SME law firms do to manage endemic risks?



With any luck, the waves of business risk that characterised the last two years will ease up in 2022 – although new challenges always seem to be around the corner. For now, a clear(er) idea of what the current threat landscape looks like has allowed law firms to gear up against risk and ask themselves key questions – about the effectiveness of their current protection mechanisms, and what new challenges might be around the corner.

This supplement analyses some of these puzzles – featuring a range of expert insights from within the SME legal ecosystem. Read about the multifaceted risks posed by unpredictable human behaviour, and see what experts are saying about mitigating these risks.

Accesspoint's Martin Lynch highlights the power of visualisation when it comes to security, and Sam Dobson of NetDocuments suggests a switch to legal-specific data storage solutions to hedge against the sector's nuanced risk profile. Plus, Chris Giles from LegalRM discusses how SME law can increase its focus on data retention and disposal.

Flip through this issue, and take a deep dive into some of the technology – both well-adopted and emerging – that you could be using to make your law firm more secure and sustainable going into what we can only hope is a post-pandemic era.

Aftab Bose, editor
@LPMmag | aftabb@lpmmag.co.uk

WHAT'S INSIDE?

About us

Aftab Bose is LPM's editor. He takes care of all content SME legal-specifc. He enjoys a good open mic night, too. **aftabb@lpmmag.co.uk**

Emily Nash is head of client services – and resident musician. Want to advertise in LPM? Contact: **emilyn@lpmmag.co.uk**

Richard Brent is Burlington Media's head of content, overseeing publications and events. Contact him on: **richardb@lpmmag.co.uk**

0800 014 2445
LPM@lpmmag.co.uk
Burlington Media Group
20 Mortlake High Street
London, SW14 8JN

ISSN 2398-9734

Living with risk

Many SME law firms have systems in place to manage a range of risk factors, finds Aftab Bose, though mitigating people-related challenges seems to be the focus in all areas of management – from compliance and cybersecurity, to strategic pillars such as client and talent retention

Pandemic-related changes to operating models intensified the complexity involved in compliance and risk management, but, as we cross the two-year mark of living with Covid-19 in the UK – with a subtle expectation of prolonged normality – SME law firms are starting to comprehend everything entailed by the post-pandemic risk landscape. As such, many have upgraded systems and processes to monitor the standard array of risk – including anti-money laundering (AML), compliance, cybersecurity, professional indemnity insurance (PII) and data protection, among others.

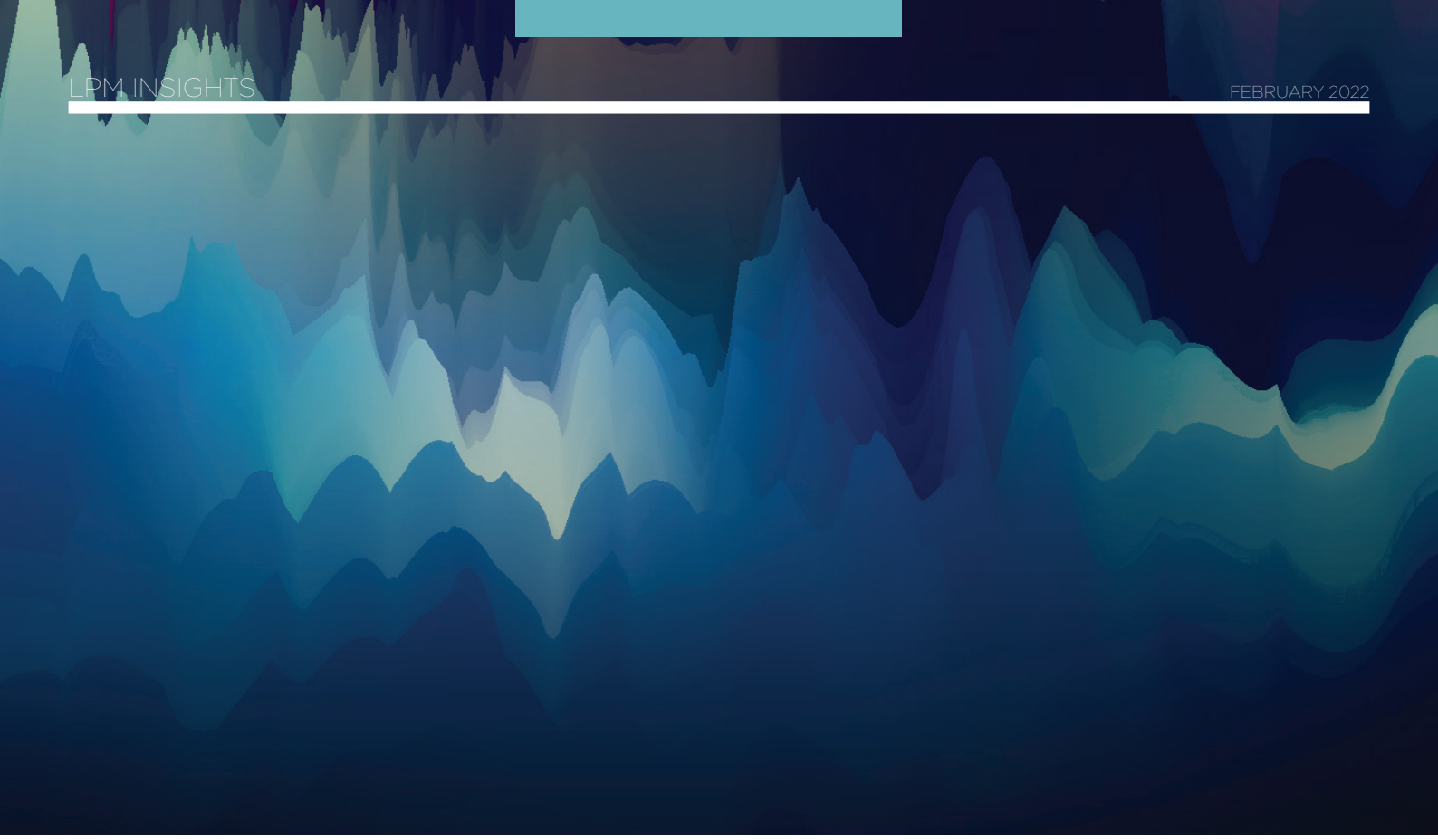
That said, a common realisation taking shape in each of these areas is that the most elaborate of security systems is vulnerable to the unpredictability of human behaviour – a core pressure point that is also surfacing in more fundamentally disruptive factors facing the sector, such as client and talent retention.

COMPLIANCE NOT CONVENIENT

A good starting point is the intensifying AML compliance landscape – as laid out by Susan Humble, regulatory specialist at West End London law firm RIAA Barker Gillette (RBG). Having recently returned to private practice as a solicitor and regulatory expert, Humble is in the unique position of having worked for eight years as the chief executive of the Solicitors Disciplinary Tribunal (SDT).

She recalls a recent meeting with the Financial Conduct Authority's Office for Professional Body Anti-Money Laundering Supervision (OPBAS), where the observation up for debate was that law firms don't provide as many suspicious activity reports (SARs) as other professional services segments, such as accountants.

"My perception is that, under pressure to remedy this gap, the Solicitors Regulation Authority is sweeping the SME law market – to



find that risk assessment on client matters lacks the rigour required to detect suspicious activity, which then affects due diligence. The body is also looking to intensify enforcement, using encouragement from OPBAS to push again for higher fining powers up to £25,000 and administrative sanctions for AML and other Standards breaches," she says.

Expectations in the AML space have been growing for two or three years now, and many law firms – particularly larger ones in the SME market – are well prepared. "Perhaps the biggest changes for us in 2021 were the updates in the Legal Sector Affinity Guidance," says Grant Sanders, compliance officer for legal practice (COLP) at south-east law firm Stephen Rimmer. The update included expanded stipulations on understanding and evidencing sources of funds and wealth, among other advice on AML governance and internal controls.

"The guidance also states that just verifying a person's existence is no longer enough. We will be expected to seek assurances that the person claiming a particular identity is in fact the person with that identity. We've introduced a new stack of solutions for digital onboarding that records ID and biometrics, scans passports, and – with the client's permission – can sift through online banking data to verify both source of funds and source of wealth," he continues.

Richard Hill, chief executive at London-based commercial property law firm Stepien Lake, is also now onboarding clients using biometric digital tools that manage the entire verification process – extending to source of funds – while the same technology focus is reported by Alison Lobb, managing partner at Liverpool-based Morecrofts, and Jacqueline Watts, director at A City Law Firm.

But, there's another risk emerging around AML compliance – and a significant reason behind the adoption of such technology to improve the efficiency of compliance. This is that extra authentication hurdles can negatively affect the client experience. "Painful processes do cause alienation with clients," says Watts, who suggests that firms should look to the banking industry for inspiration about how to redesign AML processes.

"With large volumes of transactions, banks have the same, if not more, risk when it comes to money laundering – but they have very slick, integrated processes to onboard clients while monitoring it," she adds.

Beyond having the right technology in place, SME firms are doing their best to accommodate clients on the due diligence journey in other ways. Sanders says: "Each client will have different needs, so we offer three options. Either they can complete their verification online – where lawyers still have to ask questions for risk assessment, but the heavy administrative burden for both sides falls to technology. Second, clients can arrange to go to a local solicitor, have their ID certified and sent to us. Or they can come into the office if they want a personal touch."

Still, it's challenging to find the balance between due diligence and a positive client experience. Hill's team at Stepien Lake provides a similar degree of flexibility, but there are some limits: "We've trained our people to manage expectations right from the start – source of funds has to be verified and payments can't be made via unrelated third parties. Clients can't treat us as a bank, or request that we make payments for them. All this has to be verified and cemented right at the start, so there are no surprises for anyone later.

"Another challenge is familiarity risk, or what I call 'existing client syndrome'. Solicitors pride themselves on their relationships, so they can be hesitant when going to long-standing clients to carry out full AML verification. But it has to be done, and we've been training staff to ensure complacency doesn't set in. The advantage is that verification is less complicated when it's a

LPM FIRM FACTS

RIAA Barker Gillette

Revenue: ~£5m

Corporate status: LLP

53 fee earners, 72 total staff

Offices: central and north London

LPM FIRM FACTS

Stephen Rimmer

Revenue: £7.5m

Corporate status: LLP

47 fee earners, 100 total staff

Offices: Eastbourne, Hastings

LPM FIRM FACTS

Stepien Lake

Revenue: £4-5m

Corporate status: LLP

30 total staff

Office: London

known and trusted client, as we already have their information and understand their business and funding models."

RISKY CLICKS

As such, firms have structures and processes to manage AML compliance, but people – mainly clients, and in some cases staff – may create a degree of vulnerability. The same could be said of cybersecurity, another area that has been climbing the risk management agenda in recent years.

Firms have fortified themselves from an infrastructure perspective. "We keep up to date with our servers and firmware. We have a secure VPN for our remote desktop server, and there are other checks in place such as multi-factor authentication to log in. We also have a good IT management company that handles our network," says Sanders.

Others report similar efforts to stay on top with technology – "we have a good relationship with our IT providers, who keep us advised on new cyber risks. We have email security, file security and blockers in place for certain websites," says Lobb at Morecrofts.

"It's like trying to run around plugging all the gaps, and a new one is always opening. Even if we have the most rigid possible processes in place, we can't police every single email that comes in and out of the office."

Alison Lobb, managing partner, Morecrofts

But leaders say the real risk lies in the behavioural space, with ransomware attacks rampant and phishing emails soliciting sensitive information – firms need to ensure their staff vet links before clicking on them. Stephen Rimmer, Morecrofts and Stepien Lake are among several law firms running phishing simulations among their employees, to analyse click rates and find risk areas within their businesses. This approach runs hand-in-hand with learning: "We do online training regularly, where we simulate different situations through various exercises. We repeat these periodically to keep people's minds focused on security," says Lobb.

That said, what she has realised – through a recent close shave in a data protection incident – is that people risks are extremely challenging to manage. Emails containing sensitive information are flying in and out of a law firm every second.

"It's like trying to run around plugging all the gaps, and a new one is always opening. Even if we have the most rigid possible processes in place, we can't police every single email that comes in and out of the office. All we can do is try to ensure all our staff are trained as well as possible and we've got the best possible processes to prevent it happening," she says. Her experience is that regulators also take the challenge of behavioural risk into account during enforcement – provided that every process and decision is meticulously documented.

According to Humble, the same is true of many people-related risks in the compliance space. "As long as law firms have thoroughly documented their thought processes, they should be okay in the majority of cases," she says, drawing on her experience at the SDT.

COST OF COVER

There is a financial incentive for meticulous record-keeping too. Much like behavioural risks, the high cost of PII is a reality that law firms must live with. Documenting risk management

processes is a widely used strategy to control insurance costs – a method that is particularly effective when it comes to cyber cover, which, according to Sanders, doubled in cost last year. "Being able to report the frequency and results of our simulated phishing campaigns helps with insurers, who are demanding more information about every aspect of the business," he says.

And satisfying these demands is a full-time affair, according to Hill. "You can't just present a package of good behaviour for one renewal. You have to try to encourage reporting and documentation throughout the year to present a business that is addressing risks genuinely at the firm level, rather than just packaging up and finessing it to try and look better than you are. That's what underwriters are looking for," he says.

But the risk around PII goes beyond costs – there are structural market factors to contend with, brought about by an exodus of insurers willing to cover SME firms during the pandemic. "We're more concerned with the stability of the PII market now, to ensure we can always have insurance because we have to have it," says Hill.

One way that firms, including Stepien Lake and Stephen Rimmer, are tackling both cost and stability is through collaboration. "We've joined the LawNet Group, which gives us the purchasing power of 56 firms and has really added stability to our renewals," says Hill. According to Sanders, being part of the LawNet Group has also led to a lower increase for Stephen Rimmer, compared to other firms that are going to brokers themselves. Humble's firm, RBG, is also a member of the same collective.

At Morecrofts, the strategy has been to cultivate a strong relationship with the firm's broker and collaboratively work on renewals between March and October each year. Other actions have also helped, says Lobb. "We engaged an external business to come and audit our conveyancing practices, because that's the highest-risk area. They did a remote audit of some files, interviewed our conveyancing fee earners and surveyed our wider staff about how they'd react to certain situations. They wrote this up into a report, which really helped insurers to identify the major risk areas."

With similarly tailored strategies employed from firm to firm, the SME segment seems to have responded well to the 'standard' suite of risks that have dominated in recent years – barring the ever-present people-related vulnerabilities. Puzzles that firms are finding it trickier to solve relate to restlessness – among both the workforce and clientele.

PEOPLE PROBLEMS

Salary inflation at the top of the legal market has made it difficult to attract – or retain – people at SME law firms. Rising pay demands are putting pressure on smaller firms, expected to be further exacerbated by the spiking in the cost of living in the UK. And in a virtual working paradigm, larger City firms are finding it easier to poach professionals from other regions and cities too.

The result is a talent roulette, and an extremely challenging recruitment landscape. "People are scheduling interviews and not turning up. Or, they put their CV out there just to line up some offers so that they can leverage a pay rise at their own firm," says Sanders.

One aspect of strategy at Stephen Rimmer has been to focus on growing its own talent, recruiting fresh graduates and integrating them over two years. But this is not always a viable strategy – as explained by Lobb. "There seems to be a lack of the two-to-five-year qualified person moving around between firms. There are a lot of great graduates coming in as paralegals and becoming trainees, but most firms I know are incredibly busy at the moment, and would like to bring some more experienced people in," she says.

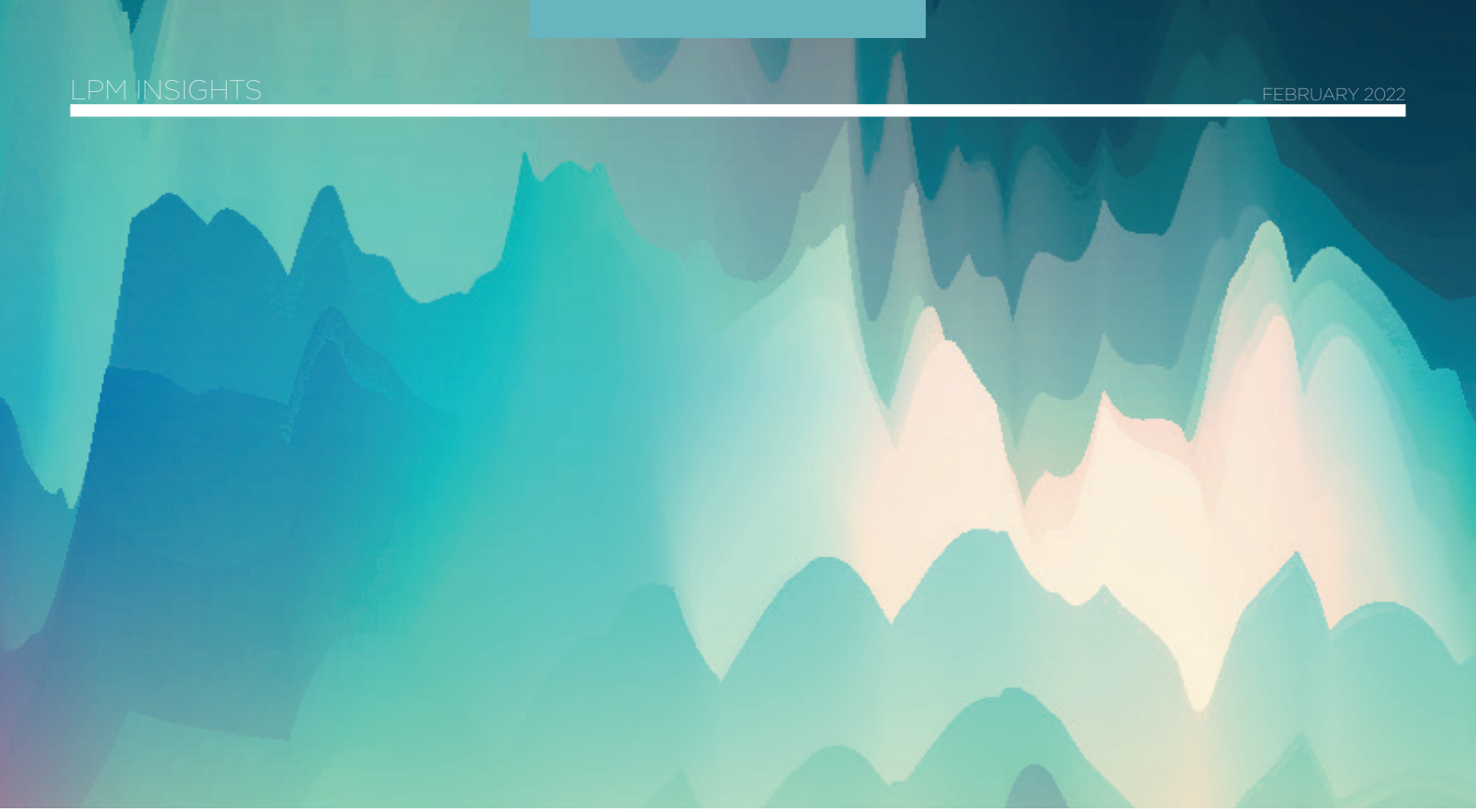
Firms are faced with the challenge of creating a workplace attractive enough to counter market forces such as rising pay, mainly by leveraging changing employee expectations around work-

LPM FIRM FACTS

Morecrofts
Revenue: £5m
Corporate status: LLP
57 fee earners, 115 total staff
Offices: Liverpool

LPM FIRM FACTS

A City Law Firm
Revenue: undisclosed
Corporate status: Limited company
10 total staff
Office: City of London



life balance. "Partners in the firm and I personally check in with all our staff regularly to make sure everyone is ok – a practice that we intensified during lockdown but have continued in person. We're trying to understand people's pressures, and to keep things as flexible as possible – we haven't forced anyone to come into the office. We make sure that when people do come in there's a lively environment so they have a chance to connect, and we organise nights out and other activities to take people away from their desks," says Hill.

"Beyond having a supportive culture, training, career development, exposure to higher-quality work and learning opportunities can all be of equal, if not more value, than pay – so we need to constantly work on improving those areas."

According to Watts, the salary inflation at current rates is unsustainable. "Where is the money coming from to fund these salaries? Rising costs of living, coupled with the economic fallout of the pandemic and unfolding effects of Brexit mean that clients' ability to afford fees might also be affected in the medium- to long-term. The legal sector is likely headed for a 'boom and bust' scenario – and if the need to cut costs arises, the talent market will equalise again.

"It'll be interesting to see the direction the market takes. Either the value of traditional legal services will fall, or it will be even higher than before as a premium addition to more normal, automated processes."

Jacqueline Watts, director, A City Law Firm

We just have to wait and see how things pan out," she says.

One problem that pay equalisation wouldn't necessarily solve is the growing restlessness in the talent market. "The belief in today's workforce is that people should be changing jobs every five to eight years. So, even growing your own talent could potentially be a futile investment if people move on once they're brought up to speed. That's always a challenge small firms face with limited resources, although niche firms like ours have the advantage of offering high quality work in a small firm environment," says Hill.

And while this is an imminent challenge when it comes to the talent market, it also speaks to one of the persistent long-term risks faced by the SME law segment – that of succession. He continues: "Closing down a law firm is a huge cost – with dilapidations, redundancies, run-off cover and several other considerations. SME firms rely on the relationships and expertise built by their partners, and having the right people is crucial to ensuring their business can continue. At the moment, the right people are hard to come by, and even harder to retain for succession purposes."

Priming young equity partners for succession is one option according to Hill – albeit with the critical risk of losing those people when the time comes – while the inorganic route of a merger is another. "Both are good options, although there is urgency here. Even if succession isn't two or three years around the corner, both avenues require a significant time investment – either to build up the firm from within or find a suitable M&A prospect," he says.

ALTERNATIVE DISRUPTION

The underlying issue remains restlessness, which is causing just as much trouble when it comes to client retention, according to Watts. Clients are demanding faster service, and more flexibility in fee structures and payment options. "There are scores of digital-only alternative solutions

emerging to meet these needs, automating large chunks of legal work and delivering value-added services," says Watts, who specialises in innovation and disruptive technology.

"Some solutions compose documents, or obtain advanced assurances from the HMRC – steps that lawyers wouldn't traditionally take. Others will make disputes, small claims, wills and divorces as easy as pressing a button. For me, that is one of the biggest risks this industry faces, and imminently," she adds.

While Watts sees the challenge of client retention very much in the context of digital disruptors, Hill suggests that a range of bigger law firms, consulting firms, multi-disciplinary firms edging into niche areas such as property, and tech-savvy peers all pose a threat to retaining your client base in the SME market. "People are more price-sensitive than ever, and they want to consume legal services like they do other online services in their day-to-day life – cost effectively and with the click of a button, but still with personal interaction when needed," he says.

"New entrants in the market are potentially more open and transparent than law firms. They might not be doing things better, but they're more adept at presenting their services, selling them and being more visible than traditional law firms."

For Watts, the future of law could be a hybrid model of digital solutions, paired with personal advice at a premium – much like the banking sector in its current form. Hill suggests the same, positing that while making the most of technology is important for law firms, there is no substitute for quality of service and expertise. For him, pre-empting what clients want from their experience, and investing in delivering it will keep SME law firms afloat.

Watts adds: "But there is significant cyclical change to navigate before reaching a balance between tech and service delivery, and law firms could lose out to alternative solutions in the short term. It'll be interesting to see the direction the market takes. Either the value of traditional legal services will fall, or it will be even higher than before as a premium addition to more normal, automated processes."

TO THE FUTURE

Beyond internal efficiencies and competencies, attracting and retaining talent and clients alike could also become more deeply entwined with understanding what people value – which increasingly falls within the wide remit of environmental, social and governance (ESG) considerations. "Having a mix of backgrounds is important. Many in our profession will have gone to similar universities, have completed the same examinations, and have similar ways of thinking as a result. It's important to bring in a diversity of mindsets so a firm can think differently," says Sanders.

Pressure to stay abreast of these values is intensifying from every direction – including from a regulatory standpoint. "Firms must be equal and must be diverse, and that is an area where the SRA is going to conduct a thematic review over the next 12 months, to find ways of better enforcing these principles," says Humble.

According to her, a significant portion of the SME law market might be caught unprepared. "There are many firms that have come to be very diverse, although there are also those that continue to have very homogenous workplaces of a certain gender, age group and ethnicity. The idea of having a diversity, equity and inclusion policy is quite shocking to them – I can say that with some confidence, from looking at the below-the-line comments in the Law Society Gazette in particular, whenever any issue of diversity is mentioned."

The good news is that, for now, having some ESG policies in place is a reassuring starting point for the SRA, which according to Humble remains process-focused rather than outcomes-focused when it comes to many areas of compliance. And with systems set up to manage other key threats, much of risk management is now a matter of mitigating the unpredictability of human behaviour. LPM

Innovation for P4W Firms

Your next move matters, make IT Count with Mozaique

Mozaique is fully integrated with your P4W platform and other innovative software, providing a fully automated, joined-up platform.

What can Mozaique offer?

- **Seamless Digital Onboarding**
  Make onboarding as easy as possible, as clients can securely enter their information via online web-forms, with the data being sanitised and auto-inserted into your P4W.

- **Automated Client Portal**
  Fully adaptable settings to publish client matters, what and when you want to share in real time from P4W. They can access live and archived matters, case milestones, notes and share documents.

- **Synchronised Client Payments**
  Receive secure, online payments from clients through the portal, which are automatically synced as posting slips in P4W, reducing admin time and improving accuracy.

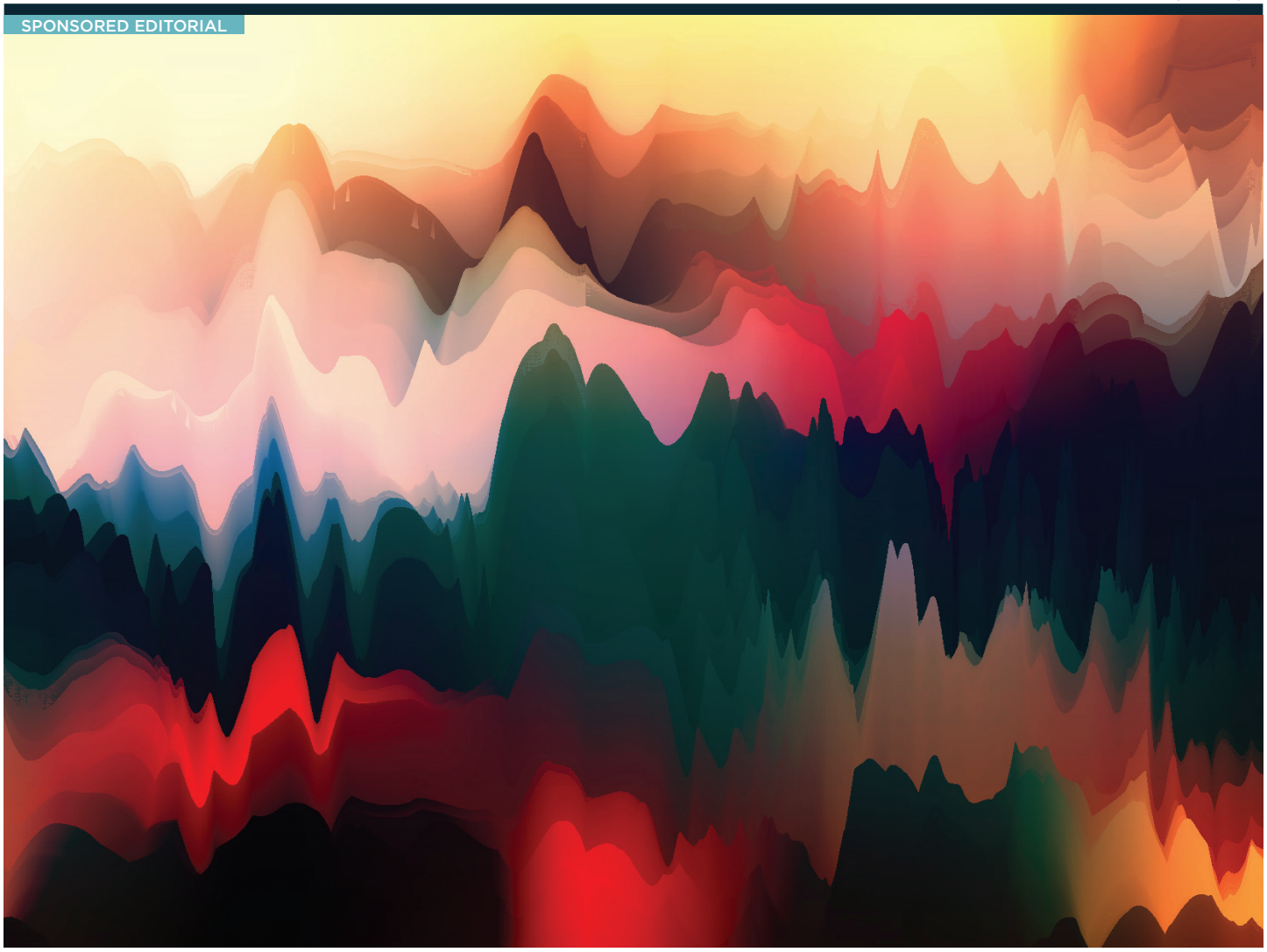
View all our modules at mozaique.legal

Brought to you by: Accesspoint Legal Services — Where knowledge makes the difference

t: 0203 189 2645 w: accesspoint.legal

mozaique — enabling legal intelligence

SPONSORED EDITORIAL



VISUALISING SECURITY

Martin Lynch of Accesspoint traces how the structured, visual elements of the company's custom-developed cybersecurity platform have laid the foundation for more secure infrastructure, processes and behaviours among SME law firms

Most law firms understand the importance of security, but it's hard for many to fathom the time, resources and processes that go into having a truly secure tech stack. This, coupled with the much-cited cultural inertia in the SME legal space when it comes to adopting new technology, manifests in significant barriers en-route to comprehensive cybersecurity – and consequent chinks in a law firm's armour.

"As managed legal IT service providers, we tend to have unrealistic expectations of practice managers and other law firm leaders as to their ability to understand technology and all the risks therein. It's the same as if they spoke to us in technical legal terms – we would need some extra help," says Martin Lynch, head of service delivery at Accesspoint.

Without a full understanding, it's hard for leaders to drive adoption of security measures within their organisation – given the existing people barriers. "There is a fine line between usability and security, and most lawyers are primarily concerned with the former. They want to just be able to click one button and carry out tasks as quickly as possible, so things like multi-factor authentication, for instance – which requires them to take their phone out and type into an app before proceeding – are viewed as unnecessary obstacles," he says.

And while simplifying these processes is important, Lynch draws on his experience to suggest that the best way to drive adoption of secure infrastructure and processes is to truly convince law firms of their necessity. The company's visually sophisticated legal technology platform – Mozaique – has been a big help in making this argument.

STOP AND GO

Using data gathered on a law firm's security infrastructure across more than 100 metrics, the platform distils a firm's security status into a single numerical score, which forms a cumulative of percentage scores across five key areas – domain security, cloud security, mail security, device and mobile management and phishing awareness.

Specific metrics include the status of Sender Policy Framework (SPF) records at a firm, or whether its domain has been secured with Domain-based Message Authentication, Reporting and Conformance (DMARC) – both of which fall under domain security. In the cloud security space, a firm is assessed based on whether antivirus is installed on all platforms, whether remote access is encrypted, and the level of complexity in their passwords. Protection on hardware such as phones, tablets and laptops is evaluated too – under device and mobile management – and similarly detailed assessments are carried out in each area of security. The score for every metric is presented in a visual dashboard that uses a 'traffic light' system of colour coding – with red, amber and green indicating performance from poor to good, respectively.

> *"Based on what we're hearing from our public network – especially the SME segment – ransomware attacks are emerging as the most intensive and increasingly frequent cyber threat in law."*
>
> Martin Lynch, head of service delivery, Accesspoint

According to Lynch, the dashboard has facilitated a stronger argument for action among law firms. "Verbally conveyed recommendations over a phone call or a meeting tend to fall down the priority list for our clients. But when we actually sit down with them and present this visual display, they can clearly see, marked in red, where their firm is in danger. And the way it's broken down into various areas gives them a detailed overview of their tech stack, and all its vulnerabilities."

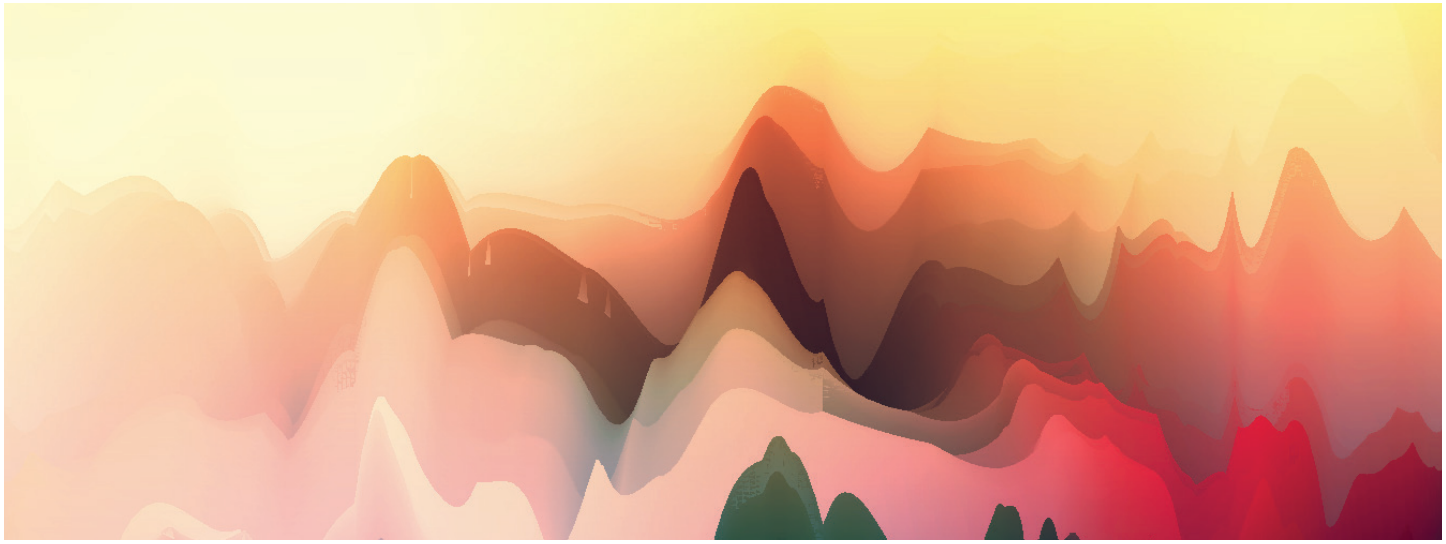
Using the platform, Lynch reveals that his team has successfully fitted the majority of its clients with the basic technical infrastructure required to be secure – evidenced by a 98% adoption rate across its client base. From this point onwards, the underlying goal is to continually improve the simplicity and usability of security infrastructure, while the next key challenge is to educate users at law firms in secure behaviours and protocols.

Simplification is an ongoing journey – Lynch uses the same example of multi-factor authentication (MFA), as cited above, to illustrate some improvements that have been made. "We've introduced a push authenticator, which allows users to log in or authorise a task by simply clicking an approve button that shows up on their smart phone or watch – rather than having to log in to an authentication app and type in a code.

"We've also consolidated different types of MFA codes that you may need across multiple platforms such as Google and Microsoft into our approved authenticator app, which means users don't have to go into each platform to log in. This makes roll-out easier, it makes support easier, and creates an overall better experience for lawyers," says Lynch.

STOKING VIGILANCE

Cultivating secure behaviours among law firms is more of a challenge – particularly in light of an intensifying cyber threat landscape. Accesspoint partners with the National Cyber Security Centre (NCSC) and other third parties, and closely



monitors information channels such as newsletters, forums and peer networks to keep up-to-date with changes to the threat landscape.

"Based on what we're hearing from our public network – especially the SME segment – ransomware attacks are emerging as the most intensive and increasingly frequent cyber threat in law," says Lynch. Rather than targeting individual transactions for small sums of money, these attacks target a law firm's data repositories – jeopardising sensitive and confidential information, while also demanding exorbitant sums to keep the data safe and private.

According to Lynch, ransomware exemplifies the type of cyberattack that puts the human side of security into sharp focus. No doubt, the technical side of things is important – data needs to be encrypted, systems need to be equipped to detect suspicious emails, and MFA needs to be in place to secure processes. These can shore up against a certain inevitable degree of human error. But there are some behaviours that can render even these systems ineffective. "An IT person could help out a lawyer who has lost their phone by removing MFA for a one-off login, and then forget to replace it straight away. Or, a highly complex and optimised password can be written down on a post-it note and left lying around. And then there is the threat of phishing emails – often the starting point of ransomware attacks – which could successfully solicit login data," says Lynch.

"Lawyers want to spend their hours fee-earning, so convincing firms to invest their time in security training is very difficult."

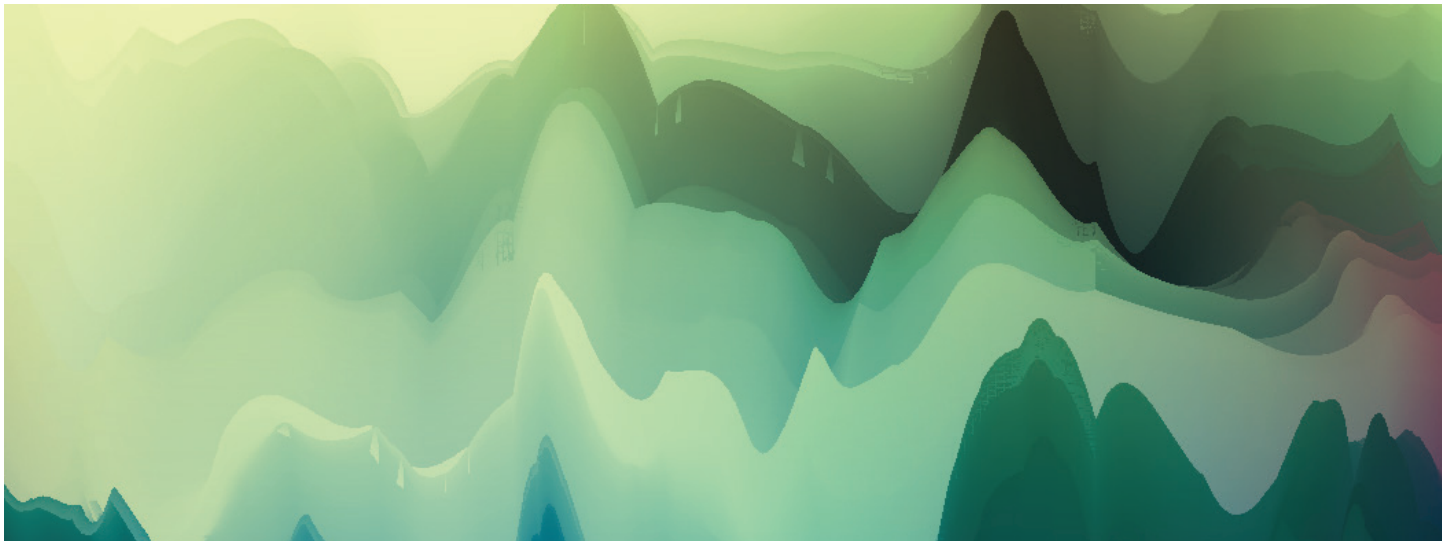
Martin Lynch, head of service delivery, Accesspoint

As such, technical security demonstrably needs to be paired up with training, although attitudes pose a significant hurdle here too. "Lawyers want to spend their hours fee-earning, so convincing firms to invest their time in security training is very difficult," says Lynch.

Again, it's the visualisation of threats that helps create learning momentum. Accesspoint partners with third parties to organise phishing campaigns – simulated phishing emails that can identify and record risky behaviours. "These campaigns give us information on the number of emails opened, the number of links clicked on, and all the way down to how much data has been entered. Presenting this to management executives in a visual format allows them to benchmark their firm's security status, and understand how much of a risk is posed by behaviours.

"Once this is established, we can start to roll out training, and follow it up with repeat simulations. At regular intervals – three months, six months, and so on – a trend emerges in reporting where the line representing number of clicks gradually starts to come down. We can keep reminding people of the risks but to a lesser degree, and firms have a visual on the progress they are making in user training and education. The end goal is to reach a point where people doubt every single email that comes in, rather than being suspicious of just a few," says Lynch.

Separate protocols are in place in case of a breach – an immediate report is in order, which can trigger an investigation to find out where a law firm was found exposed. Accesspoint conducts this investigation, and can use a visual representation to convey the vulnerability to its clients, relating it to the overall picture of the firm's security dashboard.



OMNI-COMPETENCE

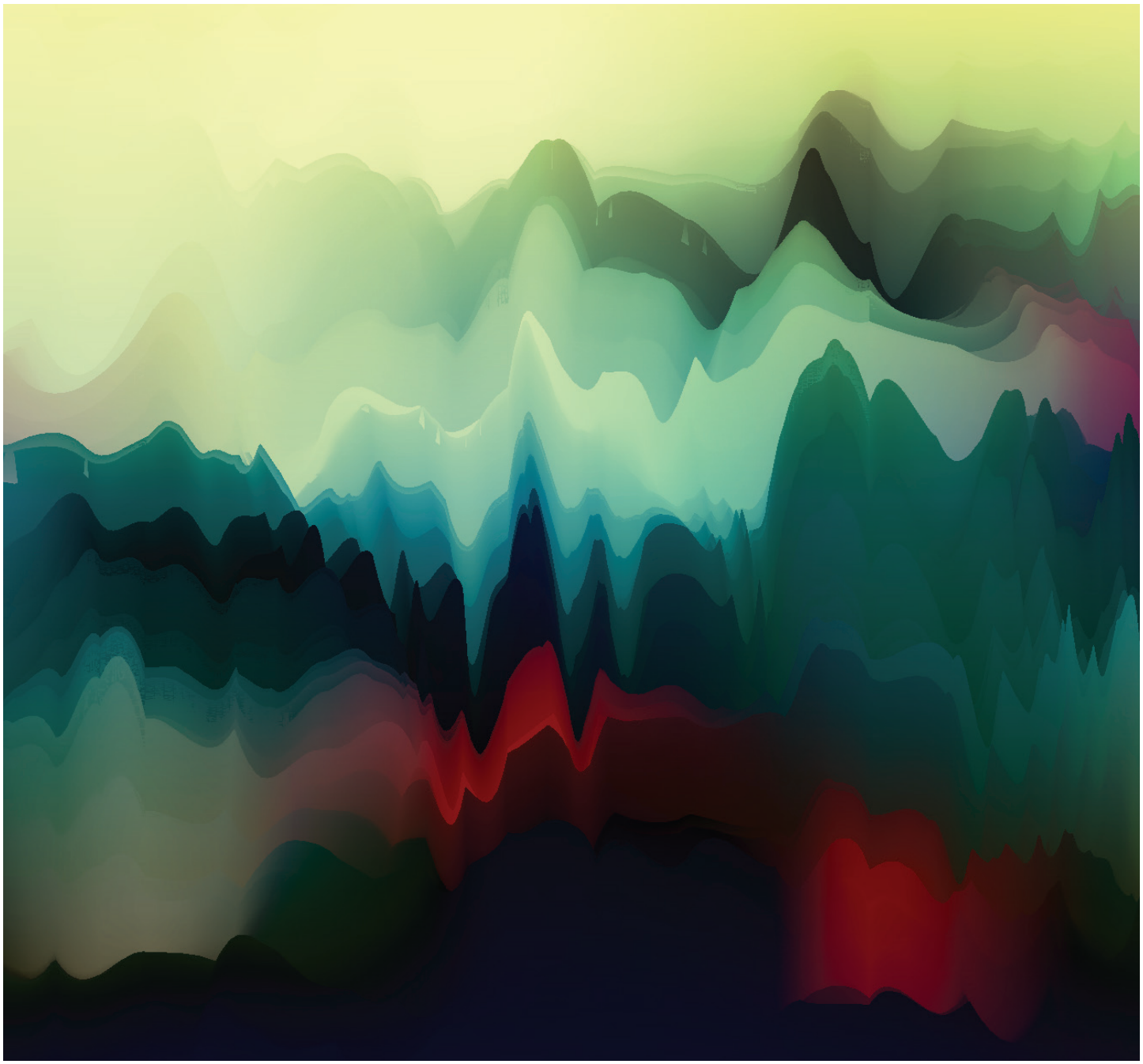
In some cases, where a law firm doesn't necessarily have a well-resourced, internal IT team, Accesspoint conducts security training amongst staff. According to Lynch, having a full overview of the security infrastructure – as presented in Mozaique – helps overcome key cultural and technical obstacles at every step, forming a strong foundation to meet its clients' security needs.

And the platform's applications are multifarious. Another key area of risk with which Lynch and his team support clients is security accreditation. Working with third parties, the team evaluates a law firm's tech stack, recommends specific certifications – such as Cyber Essentials, for instance – and then makes the application, handles all the paperwork, arranges for the technical audit and delivers the certification. Law firms can then check the right box for insurers and regulators alike.

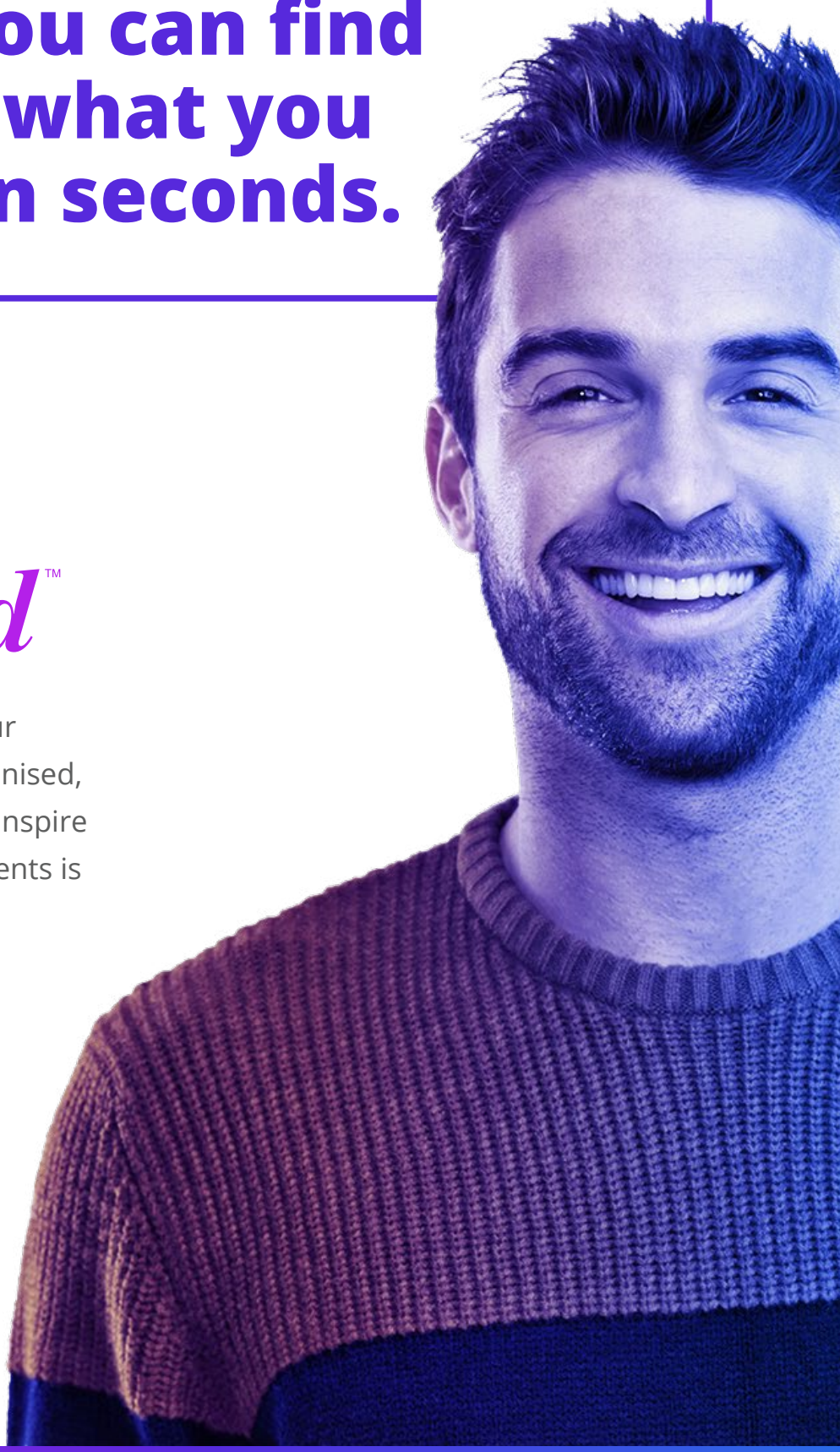
According to Lynch, while Mozaique doesn't yet play a direct role in accreditation, it currently helps facilitate many of the component processes, and has the potential to play a much bigger role in the future.

The portal is conceptualised as a single source of truth for billing, contracts, licenses, project plans and processes, which can offer a valuable insight into status and performance across systems. New features are being integrated regularly, to make Mozaique a competent enabler of cybersecurity for all of Accesspoint's clients.

LPM



When you can find exactly what you need—in seconds.



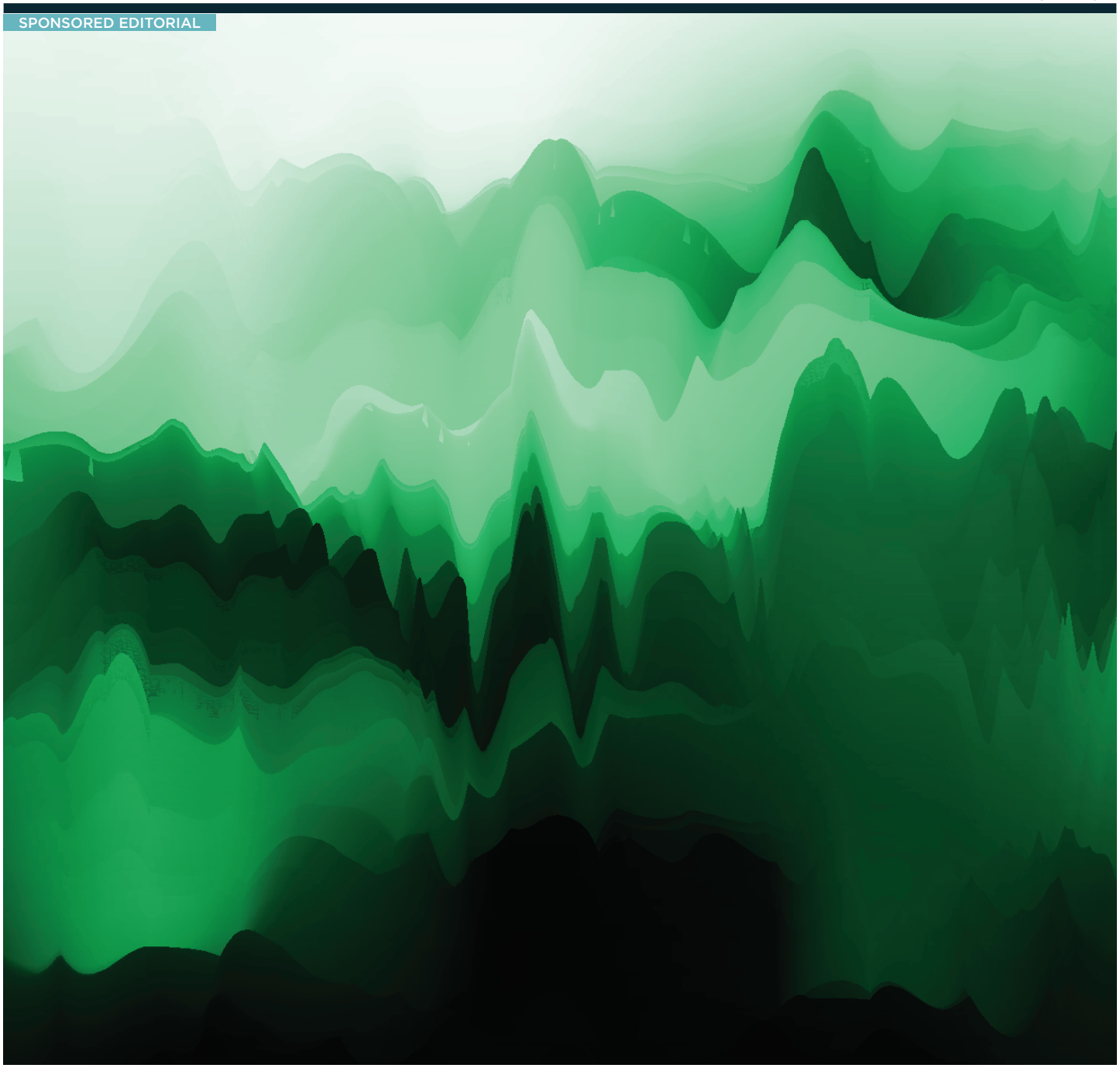
That's Work Inspired™

Imagine a future where your content is always safe, organised, compliant and available to inspire your best work. NetDocuments is ready to take you there.

Talk with us today to learn more.
+44 (0)20 3129 9324 | netdocuments.com

netdocuments®

SPONSORED EDITORIAL



PURPOSE BUILT

A data storage solution designed specifically for legal has a range of risk management benefits for law firms, according to Sam Dobson, account manager at NetDocuments

There are many cloud based data storage, document management, and file sharing solutions that law firms can use to streamline their day-to-day operations. Unfortunately, not all platforms are well-suited to the needs of legal work. This can be especially risky when it comes to maintaining the level of security and governance that the legal industry requires, in order to keep client information confidential.

Common 'freemium' cloud based storage solutions like Dropbox and Google Drive can seem like an attractive option for law firms on a budget, but they're not without their risks. Here are a few steps that law firms of all sizes can take to avoid making costly security mistakes when choosing legal project management tools and technology.

DRAWBACKS OF CONSUMER-GRADE COLLABORATION TOOLS

One of the key benefits of law firms transitioning to the cloud is that it's now easier than ever for teams to work and collaborate remotely, from wherever they happen to be. If there's an internet connection, legal professionals can quickly and easily access their files from anywhere and from any device.

As most legal work deals with documents, firms primarily use remote tools to share documents – often containing sensitive material – between colleagues and clients. That's why law firms should be extra cautious when utilising commonly used consumer-grade solutions designed for general user convenience, and not the rigorous compliance requirements of the legal industry. There are also other serious drawbacks to consider:

• **No standard organisation.** Consumer storage services allow each user to organise files however they wish, but if users aren't following the same standardised file management process, documents can quickly become lost, scattered and difficult to find.

• **Free versus business plans.** Commonly used file storage services often offer free plans with limited options, but these free options might not provide the necessary compliance assurances that law firms need to minimise security risks. Unfortunately, the same can also be said of premium business plans, depending on the provider.

• **Inconsistent governance.** With a focus on user flexibility, consumer storage options have a variety of access loopholes that may go unnoticed until it's too late. For example, if someone were to leave the firm today, would they still have access to any client files, whether on their machine or in the cloud?

The same advanced security controls and other restrictions that keep information safe can also quickly become a hindrance to employee productivity. This can unintentionally encourage risky workarounds that nullify all attempts at security.

Fortunately, it is possible to have both security and productivity, and it starts with asking a few simple questions during the consideration process.

FIVE QUESTIONS TO ASK BEFORE SELECTING CLOUD TECHNOLOGY

A law firm and its lawyers are obligated to understand what risks technology presents to client data. Asking the right questions about security and compliance prior to selecting any given solution can provide ample insight into whether a system will be the right fit, such as:

1. What encryption technology does this cloud application leverage? It's critical to understand if a service or solution encrypts information both on a device and also while it's being shared between devices and users. In addition, it is wise to ask whether files are encrypted individually or only in larger document groups.

2. Which compliance certifications does the provider maintain and how are they evaluated? The best file storage options will provide clear documentation regarding their compliance standards, which can then also be shared with a firm's clients as part of contracts and guarantees.

3. After working on a document, does it remain on my device or saved directly to the service? When files are returned to the service rather than being saved to a device first, it helps ensure all documents remain subject to the security controls set within the application.

4. To what degree can users control document access and actions? Having the flexibility to manage document access both on the individual file level as well as the user and group levels is critical to maintaining proper governance.

5. How does the service provider notify users, should issues arise? Asking what a provider does when things go wrong will help you gauge its maturity and transparency, especially for firms that have regulatory or contractual notification obligations.

While consumer grade solutions may provide satisfactory answers to some of these questions on the surface, don't be afraid to ask for detailed security and compliance information. When client information is on the line, it's better to be safe than sorry.

THE BEST OPTION? LEGAL-CENTRIC TOOLS

Simply put, consumer storage providers are not designed with the legal industry's unique security and governance requirements in mind, which makes these options risky for your LPM needs. While some solutions offer flexibility, the lack of controls can quickly turn document organisation into a nightmare.

Some of the additional features law firms should consider when selecting a document management system include:

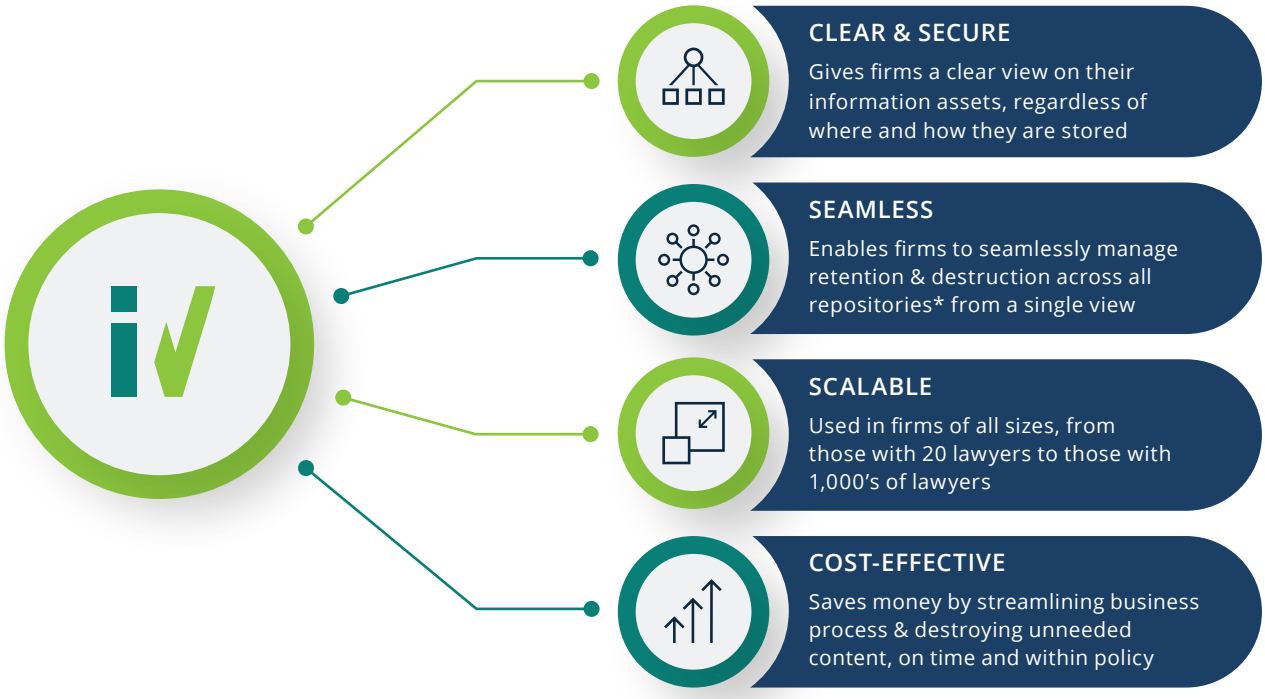
• Dynamic user profile permissions and attributes
• Version control
• Archiving and retention
• Backups and file recovery
• Data loss prevention
• Secure external collaboration
• Client and matter centric organisation
• Email management tools
• Desktop and mobile apps
• Built-in e-signature capabilities.

Whenever possible, it's best to select a technology that is specifically designed for legal teams with robust security features as part of the base offering. Avoid the security risks that come with relying on consumer applications for your legal project management needs – the right legal centric tool should enable productivity and inspired work without sacrificing on security and compliance. LPM

Privacy: Ignorance is not a defensible position

Whether information assets are paper or electronic or both; regulations, client demands, and sound business practice require firms to know what assets they have & where they are

iCompli offers seamless & secure management, retention & disposition of your information



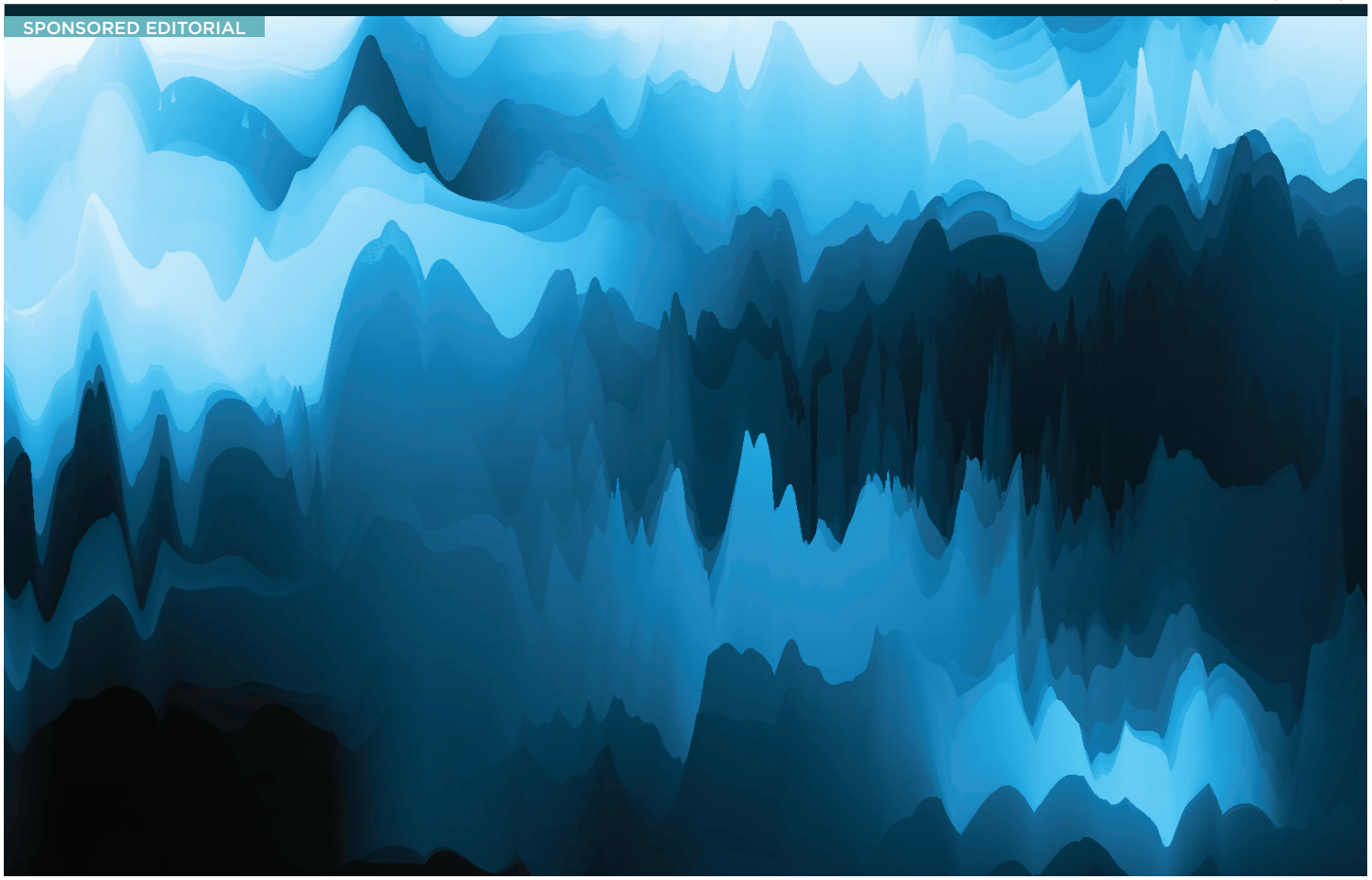
iCOMPLi by LegalRM

legal-rm.com

E: sales@legal-rm.com
T: +44 (0)208 289 8529

* Including iManage, NetDocuments, File Shares, Office 365, and many more

SPONSORED EDITORIAL



PENDING CONSIDERATION

With disparate data repositories persisting as a challenge for SME law firms, Chris Giles, founder and CEO of LegalRM, explains how his firm's solution – iCompli – is making a digitalised approach to retention and disposal more accessible for the SME legal segment

Holding on to client data longer than required is a significant risk for law firms – it runs at odds with the General Data Protection Regulation (GDPR), while data retention and disposal policies are among myriad factors examined by professional indemnity insurance (PII) providers when setting premiums.

"Law firms are data controllers according to GDPR stipulations, and they should only have personal data for as long as there is a legal requirement or legitimate interest – usually defined by a law firm's own retention policy. This could be seven to 10 years after a matter closes, for instance, after which the data should be destroyed," says Chris Giles, founder and CEO at LegalRM.

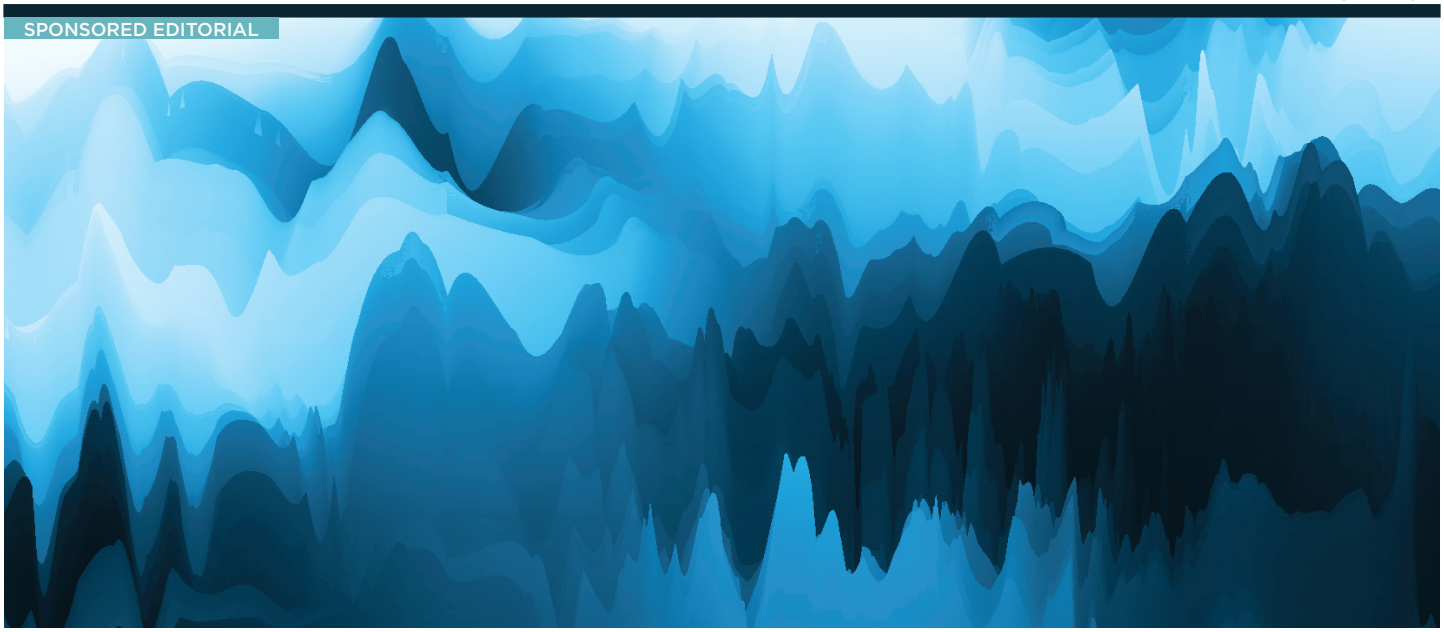
In most cases, having a policy – and the processes to back it up – is enough to mitigate the regulatory risks and pacify brokers, and large law firms have had these systems in place for years. Many in the SME market, on the other hand, are yet to take their first steps towards data disposal.

OVERWHELMED AND OVERWORKED

The process of building a retention and disposal policy falls into three phases, according to Giles – "knowing what you have, knowing where it is located, and then knowing when you should be destroying it." Most SME firms stumble at phase one. With myriad physical and electronic files stored in basements, offsite storage units, or in the cloud somewhere, taking stock of what firms have, and where, is a mammoth and obstacle-ridden task. "Disparate data aside, there are also people-related barriers to disposal – such as a decision maker who is wary of destroying old data for which they lack the context, or siloed decision-making from one partner to the next that prevents any coherent approach to retention and disposal. It can seem easier just to deposit the data in a form of storage, which builds up both cost and risk," he says.

The underlying issue here is a lack of resource. "Smaller firms are still preoccupied with savings, efficiency and automation – particularly since the pandemic – so the issue of information governance rarely gets the spotlight."

SPONSORED EDITORIAL



AUTOMATING COHERENCE

And while technology could help simplify retention and disposal – LegalRM's iCompli being one such proposition – most SME law firms are put off by the cost and excess administration of having to manage another system.

"Products like iCompli have traditionally been expensive to get up and running. But, building on years of experience with bigger firms, we've been coding into our system automated ways to make it self-sufficient. If firms don't want to use our professional services team to integrate the solution with their practice management system or convert old records systems, for instance, it's easy for them to perform these tasks themselves. We've really adapted our proposition to support the smaller firms," says Giles.

"Large firms have the manpower and resource to sift through their data and manage risk. Smaller firms could really benefit from having the process digitalised, and the cost advantages that come thereafter."

Chris Giles, founder and CEO, LegalRM

The solution pulls data in from finance systems, human resources systems (employee data), practice and document management systems (DMS), file-sharing platforms and other sources – to form a single dashboard of all matter and client related information within a firm. Paper files can also be digitalised with a single click and automatically assigned to the right matter in the system.

"Once we have the files in iCompli, we know the associated client, matter, author, owner, department, office, practice group, and area of law. We can then go about creating a policy for each practice area and department, which dictates the length of time that data is to be retained, and when that period should begin," says Giles.

The policy is then fed into the automated solution, which notifies decision makers when a file is coming to the end of its retention period – so they can give it one final look before triggering the disposal process with one click. "Disposal requests are sent directly to the DMS, file-sharing platforms, and offsite storage vendors, and iCompli verifies and updates the records system to make sure that the content has been destroyed in line with the firm's policy."

ACCOMMODATING NUANCE

There are complexities to contend with. Law firms suffer from poor process when it comes to closing matters in the system, which makes it hard to know when to kick off the retention period. In such cases, iCompli looks at other factors such as time lapsed since a client was last billed to infer if a matter is closed or not.

And flexibility within the solution allows for inevitable exceptions. "Certain matters might require a longer retention period than the policy, in which case the system can be geared to require extra levels of approval before it is destroyed. Or, in some cases where a child's data is involved, the retention period would only kick off once child turns 18. This level of complexity is hard to deal with manually, so having a malleable system helps" explains Giles.

There is flexibility in implementation, too. If a firm doesn't want to embark on the task of collecting and digitalising all its files at once, Giles suggests that data can be fed into iCompli over a longer period as and when cases are handled. In time, the firm will have a full inventory to work with, without putting additional strain on its already stretched resources.

But it's that very lack of capacity that makes it all the more important that SME law automates these processes as soon as possible, he says. "Large firms have the manpower and resource to sift through their data and manage risk. Smaller firms could really benefit from having the process digitalised, and the cost advantages that come thereafter." LPM

ABOUT US

iCompi, from **LegalRM**, is a modern, intuitive information governance platform for risk-savvy law firms looking to manage retention, destruction and overall compliance of records.

www.legal-rm.com

iCOMPLi by LegalRM