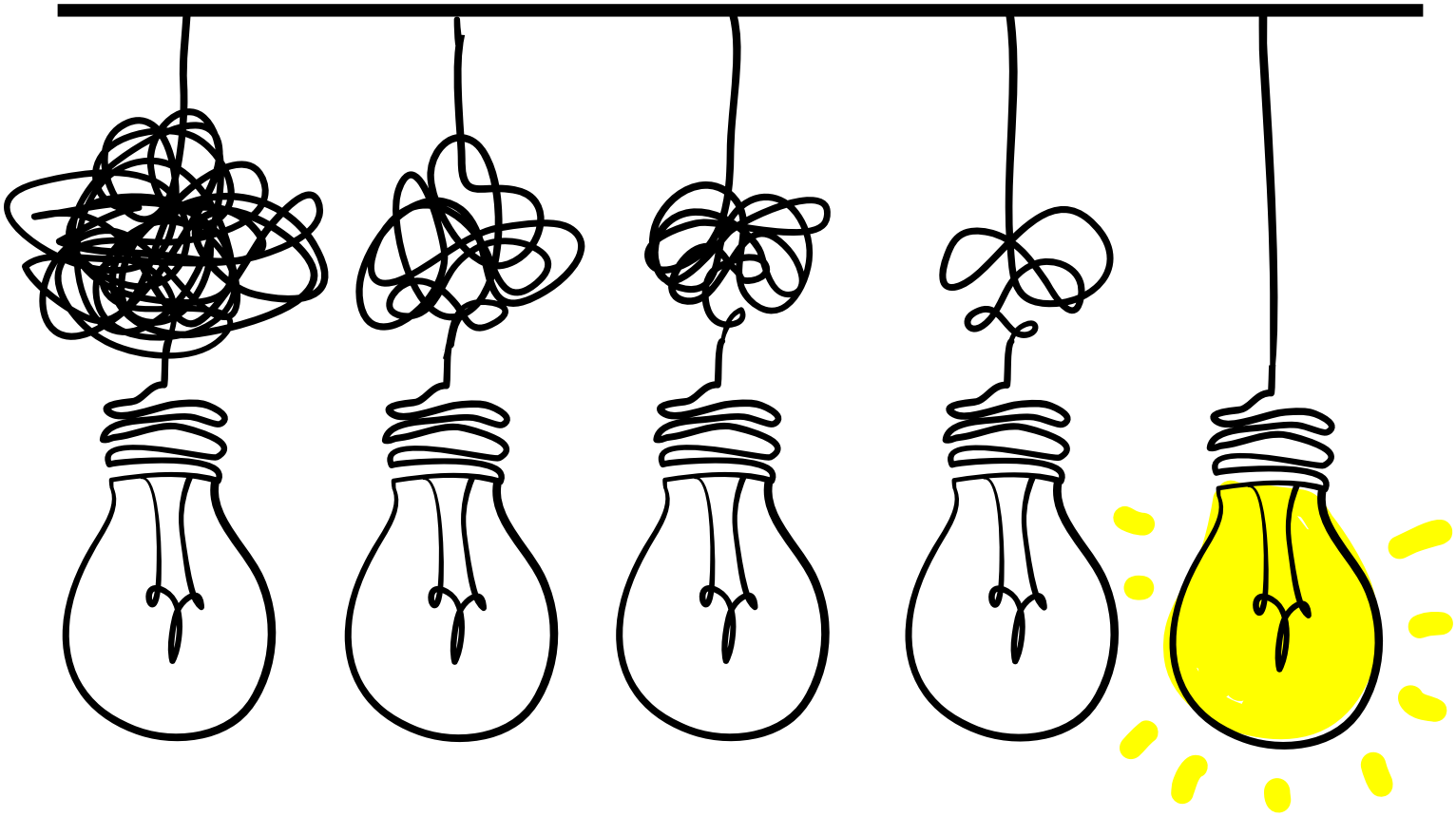
SUPPLEMENT APRIL 2020

LPM
LEGAL PRACTICE MANAGEMENT

KNOT RISKY?

Are SME law firms getting in a twist, or successfully unravelling current and upcoming challenges in risk?



Night light

A switch has been flipped and challenges in the market only continue to rise. What are SME law firms shining the light on in terms of risk and compliance? Kayli Olson reports

Challenges in the risk landscape only continue to grow. With changes around the new Solicitors Regulation Authority (SRA) handbook in place, as well as the anti-money laundering (AML) fifth directive, and an increase in threats to cybersecurity, 2020 was already destined to be a risk-filled year. And the professional indemnity insurance (PII) market was already very volatile.

At this point in time, Jayne Kendrick-Jones, head of client care at Nockolds says, the number one concern is, of course, the Covid-19 pandemic. "We must make sure we look after our staff and clients to minimise the impact of this outbreak on our business.

"In this fast-changing situation, with travel restrictions and office and school closures in place, our business continuity team is regularly reviewing and testing our plans and procedures – ensuring that we can continue to deliver the highest levels of client service, whether that be from our offices or with staff working remotely."

Sarah Charlton, legal practice tutor and examiner at the Institute of Legal Finance and Management (ILFM), agrees that the current pandemic is a big concern: "A lot of SMEs are going to struggle, some might even close, as they'll be unable to resource the working capital needed to ride the storm."

Kendrick-Jones adds that the resulting effect on the global economy is also of huge concern and remains uncertain. But it doesn't stop there, Brexit uncertainty continues to impact many of her firm's service areas.

"We have experienced people holding off engaging legal services during the transition period, and we expect this to continue until the government announces whether a deal has been negotiated and ratified with the EU."

A CAN OF WORMS

Charlton says, in terms of regulatory pressures, AML is by far the greatest area of concern. "Fraudsters will use client information for anything from selling houses that don't belong to them all the way through to providing banking facilities to someone." There are so many ways fraud can find its way inside a firm.

Alison Lyman, compliance manager at Peace Legal, recalls a money laundering situation that was caught at her firm – where client's grandparents refused to hand over bank statements showing the origin of their gift money, which was being used to purchase a property.

She says it's important to follow up on things that don't sit quite right. Afterall, SME law firms don't have the luxury of not paying attention – one accident could land a firm in a serious situation, which would damage the firm's reputation as well as incur a fine.

LPM FIRM FACTS

Peace Legal

Revenue: Undisclosed

Corporate status: Ltd

6 fee earners, 21 total staff

Offices: Barnsley

LPM FIRM FACTS

Nockolds

Revenue: £9.5m

Corporate status: Ltd

64 fee earners, 156 total staff

Offices: Bishop's Stortford, London

LPM FIRM FACTS

Rix and Kay

Revenue: £6.5m

Corporate status: LLP

58 fee earners, 110 total staff

Offices: Ashford, Brighton, Seaford, Sevenoaks, Uckfield

Kendrick-Jones says AML also remains a concern for Nockolds – as it does for most other law firms. "The fifth AML directive has required us to reassess our procedures, and we train our staff regularly to ensure we don't unwittingly open the door to money launderers.

"As we have a large conveyancing department, it's essential that we have appropriate risk-based systems to prevent money laundering, terrorist financing and breaches of the financial and economic sanctions regime. We've independently opted to implement these risk-based practices across all our non-regulated legal services to ensure consistency but this, of course, increases our compliance burden."

She says, from a compliance perspective, there's certainly a lot of pressure that comes from the SRA. The new SRA rules aim to drive higher professional standards and set out what regulation stands for and what a competent and ethical professional should look like. Although shorter, they place more responsibility on the shoulders of individual solicitors, as well as firms, and those working for legal practices particularly in relation to integrity and breach reporting.

Though this may be true, Charlton at the ILFM stresses that the core principles remain unchanged and therefore, "if you weren't lying to the court and third parties before, and you have kept client money and assets safe, then you're likely to be good. The detail within the handbook has changed but the core message behind it hasn't, so I don't think SMEs need to worry or see too much more risk here."

CONTINUING CHALLENGES

Tracey Sullivan, quality and compliance manager at Rix and Kay, says with more regulation comes more pressure on how SME law firms allocate resource and time. "When the General Data Protection Regulation came into force, it was a massive task to review our processes and roll that out across the firm."

Kendrick-Jones says data protection is something Nockolds worries about. "GDPR and data protection are a day-to-day pressure – an email or document sent to the wrong client by mistake can result in both a data breach and an SRA serious breach. Nockolds' reputation and the health of the business depends upon it keeping clients' information and money safe."

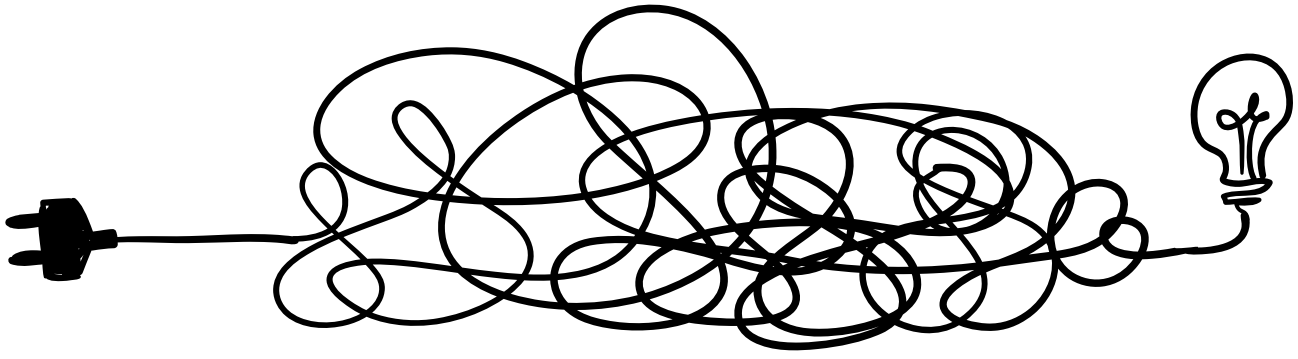
After GDPR deadline, unlike what some people thought might happen, there wasn't a flood of data subject access requests (DSARs) that hit the market – and depending on the practice areas and type of clients your firm instructs, you may not get many even these days. But the ones that do come through, can be awfully time consuming – according to those who attended the compliance clinic at LPM South conference 2020.

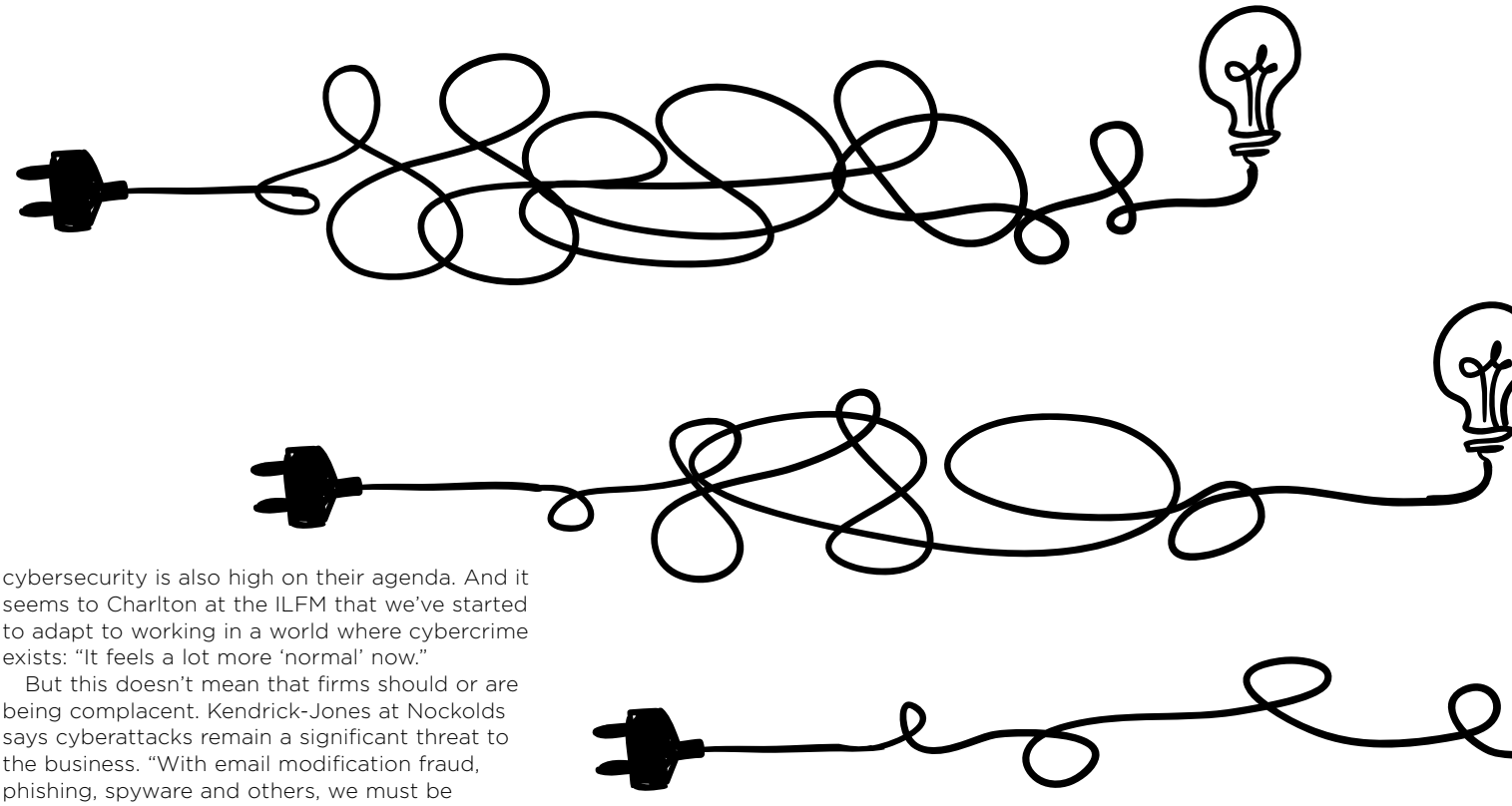
Speaker Gemma Garen, head of quality and compliance at Ellisons Solicitors, mentioned at LPM South that there are two types of motives behind a DSAR – genuine requests for data, usually for a file transfer or auditing purposes, and requests that come via unhappy clients looking to, for lack of a better term, make a fuss.

Sullivan at Rix and Kay adds that DSARs are 'purpose blind' and therefore the reason for which a DSAR is being made is not a valid basis to resist the request. Recent cases make it clear that a DSAR remains valid notwithstanding that the data subject's motive may be to obtain documents or information to assist with ongoing or contemplated litigation.

She also points out that there can be competing interests around handling data – and firms need to look out for these when drawing up a risk and compliance policy. "GDPR says you shouldn't hold on to any data for longer than you need, but our insurers want us to keep it for a certain amount of time so that we can defend a claim should we need to."

Data handling isn't the only area where insurers are putting pressure on firms,





cybersecurity is also high on their agenda. And it seems to Charlton at the ILFM that we've started to adapt to working in a world where cybercrime exists: "It feels a lot more 'normal' now."

But this doesn't mean that firms should or are being complacent. Kendrick-Jones at Nockolds says cyberattacks remain a significant threat to the business. "With email modification fraud, phishing, spyware and others, we must be vigilant, keep staff informed, and IT systems and equipment up to date. This comes at a cost, but we can't afford not to take this threat seriously."

Sullivan says Rix and Kay uses the ISO 9001 policy standard, has a Cyber Essentials accreditation, and recently made a big investment in IT – including a rollout of Mimecast secure messaging – as well as separate cyber protection insurance alongside PII.

And because the firm is a member of LawNet, Sullivan feels Rix and Kay is well connected and engaged in terms of IT. And with the membership, there's huge group buying power for PII. "The cost of just one mistake with a phishing email can be devastating – and building up awareness can be the hardest thing because most breaches are due to human error."

JUST ROLE WITH IT

Charlton says that prior to all of the current uncertainty in the market, even the SMEs that are very progressive in their ideas and strategy still risk talent being snapped up by the bigger players.

"The larger firms are likely to be in a better position to provide salary packages as opposed to just a wage. Any historical perceptions of big law lacking a work-life balance, undervaluing employees and so on has changed. Larger law firms have done an awful lot to change this image and therefore appeal to those who might have stayed within SME firms."

Therefore, resource is scarce – not just generally throughout the firm – but in positions needed to ensure quality and compliance. Charlton adds: "Often, business owners at SME law firms will wear too many hats and lack the processes that flag non-compliance or risk."

This can be aggravated by the fact that only a solicitor can be a compliance officer for legal practice (COLP). Rix and Kay has a hierarchy of support in place to alleviate the 'many hats' problem. As deputy COLP and money laundering reporting officer (MLRO), Sullivan deals with any daily issues – from enquiries around ID, to source of funds, conflict of interest and so on.

If she feels that the issue needs to be escalated to the COLP or MLRO then she will liaise with them. The firm also has this hierarchy in place to support the compliance officer for finance and administration.

Compliance is being recognised as an important function in and of itself, as opposed to being a solicitor that wears an extra hat

Tracey Sullivan, quality and compliance manager, Rix and Kay

She says the compliance profession is definitely getting more recognition. Rix and Kay sponsored Sullivan to get a professional qualification. "Compliance is being recognised as an important function in and of itself, as opposed to being a solicitor that wears an extra hat."

Lyman at Peace Legal has also gone into training: "I'm now a Lexcel-accredited consultant and find that we now have a more proactive way of dealing with risk and compliance."

THERE'S A PROCESS FOR THAT

Technology is a significant challenge for SMEs as they don't often have the spare capital to invest in – or the time to source and implement – the tech needed to make them competitively priced, says Charlton at the ILFM.

"I think we'll see an increase in smaller firms being priced out of the market simply due to a lack of IT investment and nothing else. IT investment isn't just a one-off payment, it has to be continuous year on year, complete with regular developments and upgrades."

She says firms can still have a presence on the high street and provide a very client-facing

Clients' needs must

Jayne Kendrick-Jones, head of client care at Nockolds, says in recent years the firm has really focused on improving the service it provides clients. "We have used the Customer Service Excellence Accreditation to help us achieve this. We intend to use the standard as a driver to ensure that we continuously engage with clients in order to provide the type of service they wish to receive."

And in terms of issues raised by clients, she says, the compliance team is always available to speak to clients – whether this be to complain, make an observation about the service or to give feedback.

"We have recently subscribed to Trustpilot to make it easier for clients to give us feedback – whether good or bad – and we analyse the information shared and follow up on all negative comments." LPM

service, while utilising IT in the background to the max.

"The small firm I work for has three directors and around 23 fee earners and support staff; we have just advertised for a part-time IT person as we recognise how much of a part IT needs to play in the service that we provide going forward. And we need to make this investment now."

And, of course, it isn't just the technology that you have but the way you use it that makes the difference. Process is everything, especially when it comes to risk and compliance.

Sullivan at Rix and Kay says it can be hard to get staff to change their ways once new regulation hits the market or new technology is rolled out across the firm. "You can get push back, even in the most compliant of firms; there are characters wanting to do things their way. The way we combat this is by having an ideas forum within our intranet so people can swap ideas, make suggestions to increase efficiency, contribute to improvements and feel listened to.

"If someone has found a quicker way of dealing with something, they can make a suggestion on the forum and others can engage with it. This is regularly reviewed by our management team and we roll out things off the back of it – sometimes it might only be saving two clicks of a mouse, but it makes such a difference to everyone because they can see their ideas being considered and taken on board."

STRAINED TO TRAIN

Ultimately, it all boils down to people. Are staff adequately trained to identify and deal with risk issues, whatever form they might take?

Lyman at Peace Legal says it needs to be an all-rounder approach: "We have a firm-wide risk assessment, risk data analysis, and other risk assessments regularly carried out on all files. We also have external and internal training for all, with regular compliance updates by email."

Nockolds also publishes monthly compliance newsletters sharing a summary of what the firm is focusing on for the month ahead. But this is just one piece of a wider solution to risk and compliance at the firm. The compliance team hold regular coffee mornings and training sessions focusing on particular compliance and client care issues.

And where there is a big regulatory change or a firm-wide training need, Nockolds engages with external training providers and arranges for consultants to come in and present on specific subjects.

Charlton at the ILFM says: "For SMEs, compliance is likely to vary a lot more between poor and adequate than it would in a larger firm. They're at a greater risk of not being up-to-date as they simply don't always have the time to read articles, attend training courses and so on. You don't know what you don't know."

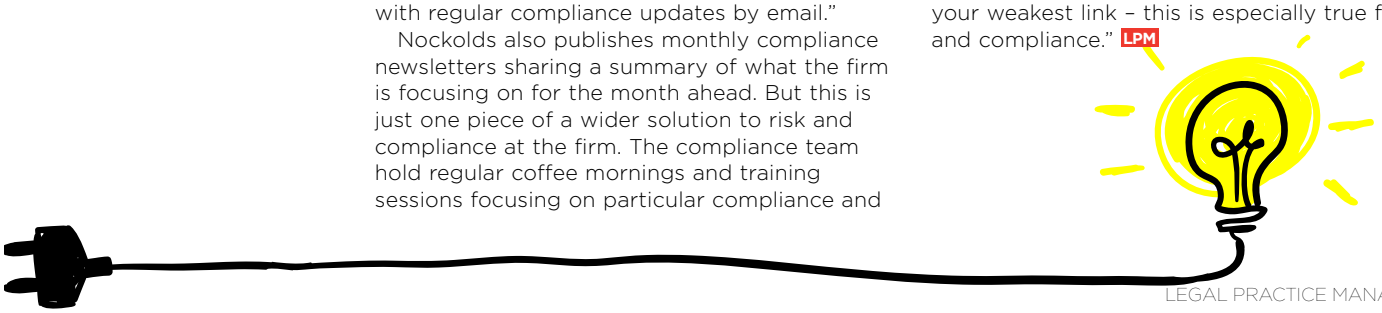
Kendrick-Jones recognises this issue, and, therefore, the firm subscribes to a compliance e-learning package, which has webinars on a diverse range of compliance topics. "All staff are allocated relevant webinars to watch to ensure there's rolling training. The webinar is followed by a test that needs passing – to make sure the training has been digested and can be applied."

Rix and Kay has a full subscription to Socrates online training. Sullivan says: "Staff have mandatory training for AML and data protection at induction and then refresher training every two years, or sooner if there's a regulatory change.

"I provide a monthly report to the strategic board that covers client feedback, supervisions complaints, claims, DSARs, internal audits and so on. I attend all monthly team meetings with a prepared, team-specific quality report and I circulate a mandatory-read compliance bulletin via our intranet every six weeks or so."

There's a huge list of solutions out there, Charlton says – it's important to take the time to listen. "If you don't listen, people will stop reporting things to you. Trained staff will increase the likelihood of a question having merit to it. Keep communicating and engaging with staff as other members may have the same question but haven't been so forthcoming.

"Like many things, you are only as strong as your weakest link – this is especially true for risk and compliance." LPM



STORMING THE WEATHER

Andy Bevan, cloud sales specialist at Pulsant, discusses mitigating risk – looking at the bigger picture and what SME law firms should keep an eye on

In the legal sector, reputation is everything. Without it, it can be challenging to get a foothold in the market and build trust.

In the same vein, once a law firm has established a reputation and presence in the market, any damage to that can have a devastating impact. It's not just about damaging customer trust, there's also potential loss of revenue, and compliance implications.

At the heart of all this is identifying and managing risk. Law firms are well versed in risk. And in today's business and technology climate, risk is everywhere. You see it in mobile working and the use of cloud services to boost productivity, and in the threat of data breaches and IT failures.

One area of risk revolves around data. As the lifeblood of a law firm, data needs to be carefully managed, stored and protected. Legal businesses also need to understand the flow of that data – how it's used and shared – and the impact on risk mitigation. The key requirements for data are security and availability – and these pose a challenge to law firms, especially the IT team.

BEYOND CYBER THREAT

News headlines tend to focus on data breaches and ransomware attacks, but law firms must focus on the bigger picture when it comes to understanding and mitigating risk, especially around data.

Risk is inherent in all operations, so managing it is about more than your security position or having a cybersecurity strategy. Yes, mitigating the impact of cyber threat is a critical part of business, but law firms and their IT departments also need to consider wider issues such as business continuity, disaster recovery and even workplace recovery.

The best way to mitigate this risk is by ensuring the right staff have access to the right information, that the data is secure, and staff can continue to work seamlessly.

In the event of a disaster or disruption, a business continuity plan enables staff to continue operating like business as usual until the issue is resolved. A disaster can be anything – network disruption, loss of power, weather event, road closure, cyberattack – that stops staff from getting physical access to their office, or accessing the systems or documents they need.

BROADEN THE ECOSYSTEM

Third-party providers are a significant external component to managing risk. Law firms don't operate in isolation; they depend on service providers to assist with operations. Whether these vendors are hosting data, such as cloud, or offering managed hosting, or providing another service, data could be compromised. Internally, data is protected via segregated networks, firewalls and encryption, but what assurances are there that these vendors can keep data safe? What service level agreements do they have in place to ensure data or infrastructure availability?

Hosting providers should, as standard, be ISO 9001 and ISO 27001 certified. Depending on the types of business they deal with, they'll have a host of other accreditations such as PCI DSS. While this doesn't necessarily help law firms directly, it does demonstrate a commitment and adherence to risk-management frameworks.

A disaster can be anything – network disruption, loss of power, weather event, road closure, cyberattack – that stops staff from getting physical access to their office, or accessing the systems or documents they need

These types of providers are also well positioned to dispense guidance when it comes to protecting data, networks and systems, and have the expertise to help in-house IT teams stretched for time or lacking the skills.

Cyberattackers could use other service providers, such as a managed print solution, as a gateway to access bigger, more attractive targets, like a law firm. Law firms must have the right processes, procedures and risk frameworks in place to mitigate risk, but also ensure that their technology partners do. Cyber Essentials or Cyber Essentials Plus, for example, goes a long way towards strengthening security and mitigating risk. While law firms give assurances to their clients that they can protect their data, law firms need to seek these same assurances from their own suppliers.

NOT A TICK-BOX EXERCISE

Risk mitigation needs to be owned and sponsored across the business. While this might be easier for large law firms with a dedicated chief information security officer, it's more challenging for small companies. Importantly, risk mitigation mustn't get lost in business as usual. It's a continuous lifecycle that assesses the likelihood and impact of threats, looks at mitigation strategies and ensures the business can get back to normal as quickly as possible should the worst occur. This affects the business from both an operational and an IT perspective, so both aspects need to be taken into account.

Risk is everywhere and mitigating it is an ongoing part of doing business. As the market changes, technology evolves, and staff requirements shift, the goal posts around risk also move. Plotting the best course forward then, involves clear ownership within the business, working with the right partners, understanding the latest threats, and having a continuous programme and the right processes in place. LPM

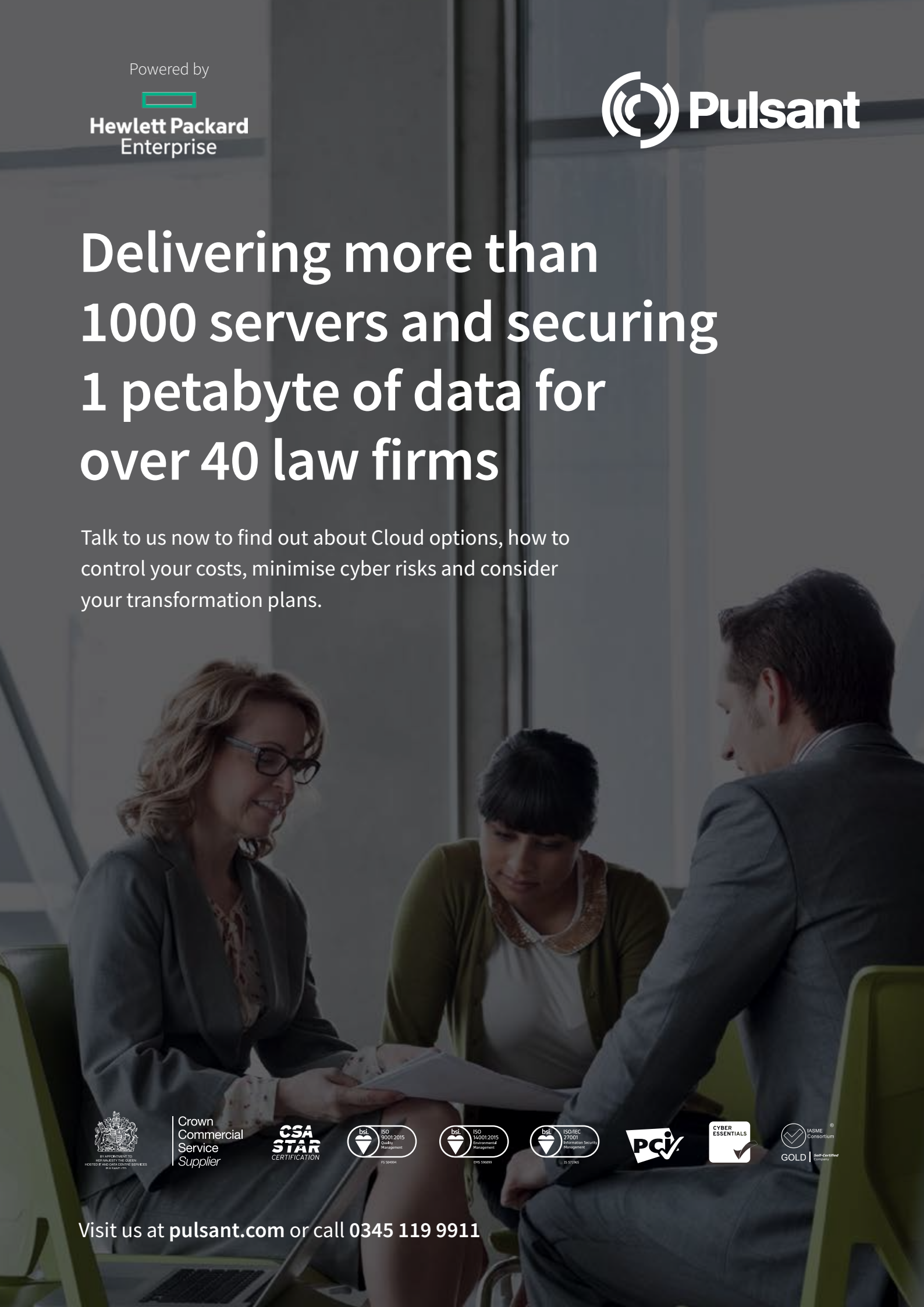
Powered by

Hewlett Packard Enterprise

Pulsant

Delivering more than 1000 servers and securing 1 petabyte of data for over 40 law firms

Talk to us now to find out about Cloud options, how to control your costs, minimise cyber risks and consider your transformation plans.



BY APPOINTMENT TO HER MAJESTY THE QUEEN HOSTED IT AND DATA CENTRE SERVICES PULSANT LTD

Crown Commercial Service *Supplier*

CSA STAR CERTIFICATION

bsi. ISO 9001:2015 Quality Management FS 594994

bsi. ISO 14001:2015 Environmental Management EMS 596999

bsi. ISO/IEC 27001 Information Security Management IS 571865

PCI

CYBER ESSENTIALS

IASME Consortium GOLD Self-Certified Company

Visit us at **pulsant.com** or call **0345 119 9911**