November/
December 2020

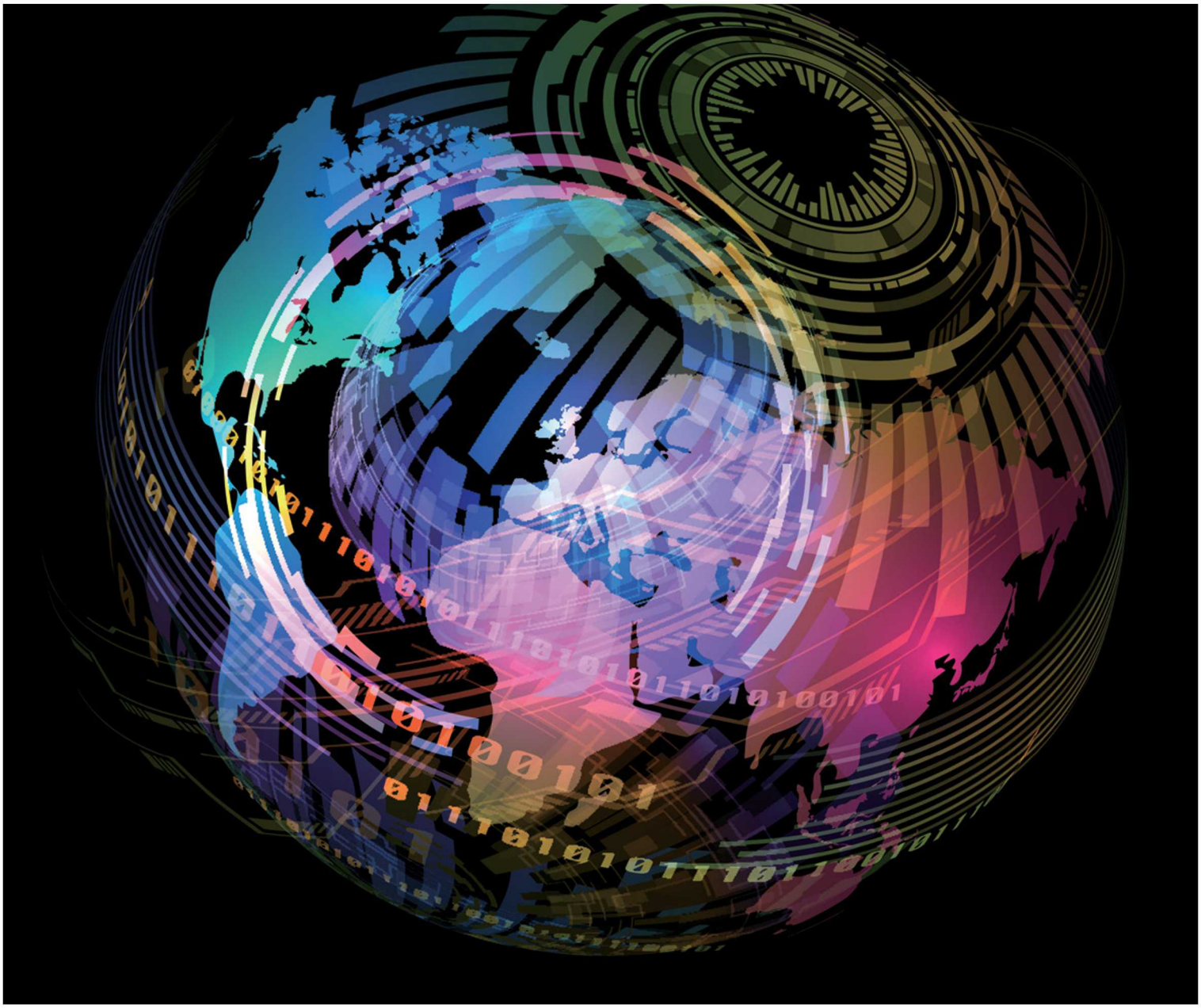
Briefing

SMARTER LEGAL BUSINESS MANAGEMENT

SPECIAL INSIDE
BRIEFING 5P 2020

BRAND PLANS
Sarah Walker-Smith, CEO of Shakespeare Martineau, on liberating lines of business

DISTANT BEHAVIOUR
Tom Bedford at DAC Beachcroft on client due diligence during Covid-19



Alert to change

How has a global pandemic changed the business of risk awareness and management in law firms?

INDUSTRY INTERVIEW

The strength of unobtrusive security

Cybercriminals are seeing advantage in a time of heightened fear and uncertainty. Even before the pandemic, client calls for insight into firms' security strategies were rapidly on the rise. And employees now present a potential further risk – the avoidance of approved systems and processes when working from home. The solution needs to be comprehensive and pervasive, but also unobtrusive, says Ian Raine, vice president of product management at iManage

As lockdowns return in autumn 2020, all organisations must consider the complex combination of risks they present. At the same time, many have strongly indicated that significantly more frequent agile working will remain in the picture even when social distancing hopefully no longer does.

For law firms, this requires careful thought about how people work together effectively when they aren't sitting together – collaboratively producing and sharing documents that contain highly sensitive, valuable or competitive information. Companies' patent documents, for example, can be worth billions. **Briefing**'s Legal IT landscapes research for 2020 found 87% of firms' technology leaders had seen an increase in the number of clients requesting security audits to ensure compliance with their guidelines (and that was before the pandemic), and industry regulators also require timely, well-managed reporting.

As with all work, these requests must be completed efficiently, while of course minimising risk of a reputation-damaging breach and data loss.

Ian Raine, vice president of product management at iManage, says a single, comprehensive system is a critical part of the effort. "Content passing between parties is at the very centre of what law firms do – and now you suddenly have many more possible versions of that content on the move." It's one positive that this period has also seen a surge in content's digitisation, so documents can be searched for and consumed online, he says. But it all needs to be risk managed. "Sensitive client material needs to be top of lawyers' minds whenever and wherever they are working remotely, and it must be stored in secure repositories."

There is ever more potential for hasty email attachments in our new normal and, of course, collaboration tools such as Microsoft Teams are fast establishing themselves as the main form of communication. "Firms should embrace the technology – but that quick chat and share can suddenly lead to data out in the wild," explains Raine. So, they need to be that much more mindful of reinforcing the central position of their document management system. "iManage can

"The best storage solution is a secure system that's as easy as possible for people to use, and where the security and risk controls are as unobtrusive as possible to increase adoption."

Ian Raine, vice president, product management, iManage

govern content for client matters that is sitting in Teams channels, but the best storage solution is a secure system that's as easy as possible for people to use, and where the security and risk controls are as unobtrusive as possible to increase adoption."

What's the usage?

Whichever tools people are using, there's the risk of cyberattack. Even with two-factor authentication, people are inevitably more exposed outside the office environment, and phishing attacks have evolved to take advantage of the pandemic. Every respondent to PwC's annual survey of law firms said it had experienced a security incident this year, with a significant rise in ransomware attacks in particular. Nation-state intelligence services also increasingly regard firms as highly valuable sources of information they can leverage geopolitically.

Firms need sophisticated user-monitoring, says Raine – and iManage Threat Manager provides this by leveraging historical information in the system. "If someone enters the system with stolen credentials, it's likely they won't move around as a genuine firm user would. By monitoring users' activity, firms can compare current and past behaviour patterns, and trigger alerts for investigation where something appears anomalous."

Machine learning also helps firms to track typical use patterns in pockets of a firm, such as practice areas, to spot deviations from the norm. If some lawyers aren't using the DMS as much as they were, or are accessing documents at unusual times, they may be working in other ways at odds with the firm's security policy. "Usage analytics enable more targeted reminders and adoption training," says Raine. However, people may currently be working very irregular hours – with good reason, of course. "You can't trigger alerts for everything slightly unusual – too many false positives will keep security teams busy but away from the real risks."

Welcome delegation

Risk management is always a balance, and firms will also be mindful of helping remote working teams to access what they need easily enough to work productively. For example, some are now introducing default 'need-to-know' policies. Raine explains: "Preventing lawyers reusing appropriate content, even from work for previous clients, can make them less efficient and increase costs. And if a law firm experiences a data breach, while that's clearly concerning, need-to-know security ensures that it's a subset of content at risk, based on particular credentials." It's for iManage, therefore, to help law firms to make work as straightforward as possible for people, so they work with security, rather than trying to find ways around it.

"That's why we have enabled some roles to override security and search for anything – a head of knowledge management or GC, for example. We're also seeing firms moving further toward searching for the expert rather than the document. Lawyers can simply search for content they're permitted to access, but using iManage RAVN's AI technology they can also locate people most associated with documents that are locked down – people who may be able to grant permission. The user only needs to justify why they need access."

Using iManage Security Policy Manager, moreover, an approach like this can be scaled for the organisation's millions of documents more efficiently. "Previously, it would have fallen to the firm's central IT or risk function to decide, but today the system also enables targeted delegation," he explains. "You can pass the responsibility for security definitions and adjustments to a named matter partner." Firms could also choose to grant access to everyone working within one practice group, regardless of their role, potentially with some client-level security access layered on top.

Client concern about the specifics of law firm security policy like these – tracked through **Briefing** Legal IT landscapes – has only increased in recent years. Lockdowns are now back, while some firms are simultaneously parting ways with people. Secure document management with options for need-to-know access, threat detection and usage analytics, will be critical for keeping sensitive client information protected and professionals productive enough for client service to keep delivering results in these extraordinarily challenging times.

For more information, visit: www.imanage.com/product/security