

Briefing

PROTECTIVE POWERS

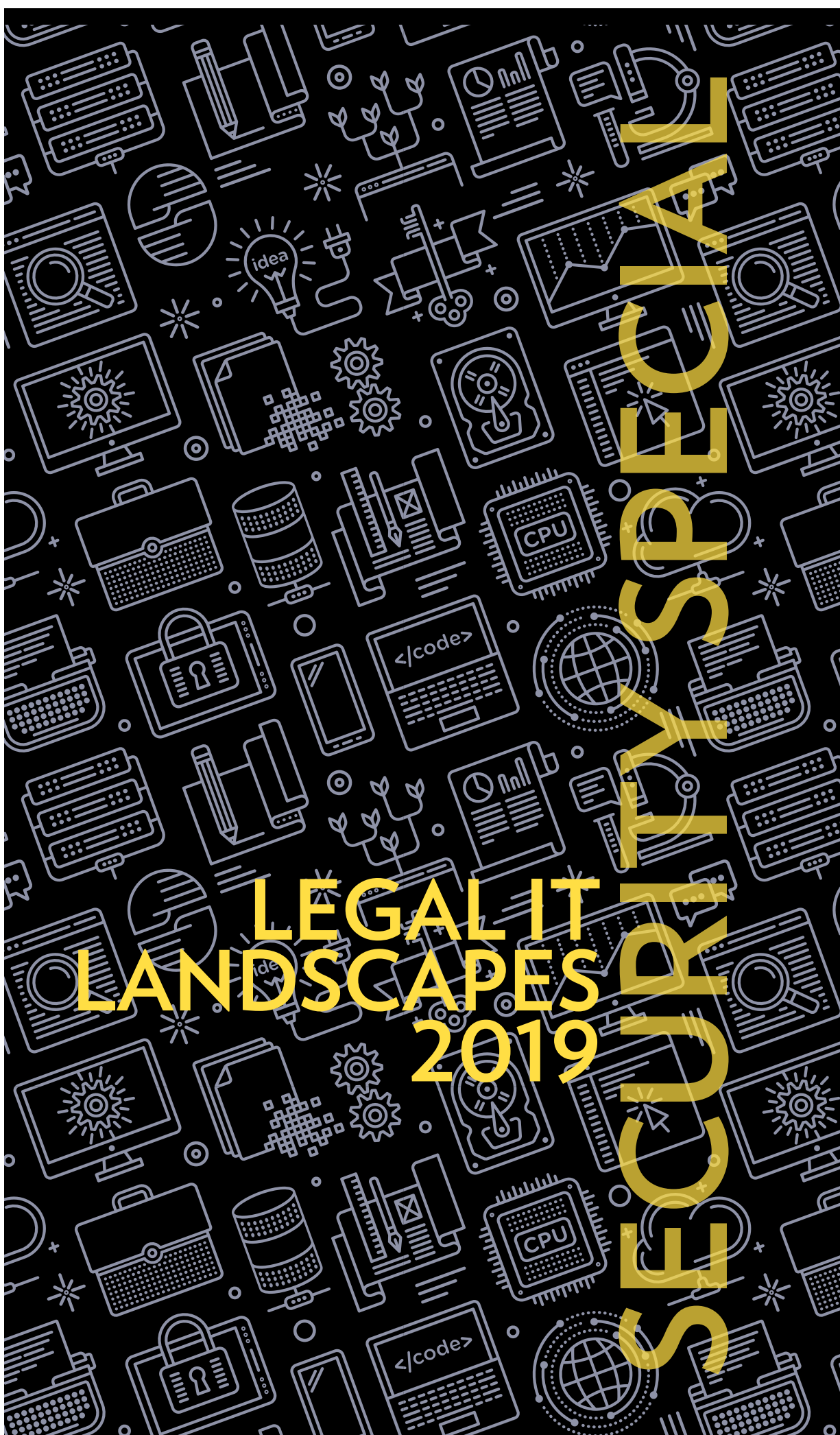
From client audits to chief information security officers, law firms explain what's on the agenda for managing the risk of cyberattack

EzeCastle
INTEGRATION

Secureworks

DVV
solutions

SMARTER LEGAL BUSINESS MANAGEMENT



**One Global Cloud.
Complete Solutions.
Trusted Partner.**

EzeCastle
INTEGRATION



In an ever changing technology and cyber risk landscape you need a technology provider you can trust!

Eze Castle Integration is a leading managed service provider to over 660 professional services firms worldwide.

- ✓ Complete Cloud Services
- ✓ Cybersecurity Protections
- ✓ Disaster Recovery
- ✓ Global Private Network
- ✓ Outsourced IT Support
- ✓ Voice Solutions

Contact us at:

**0207 071 6802 (UK)
852 3189 0101 (HK)**

**800 752 1382 (US)
65 6622 2300 (SG)**

Visit us at www.eci.com

LONDON | BOSTON | CHICAGO | DALLAS | HONG KONG | LOS ANGELES | MINNEAPOLIS
NEW YORK | SAN FRANCISCO | SINGAPORE | STAMFORD

WHO WE ARE...

Briefing is published by Burlington Media Group, the only media and events business focused on legal business services



Richard Brent is editor-in-chief of **Briefing**. He likes to get out and meet as many readers as possible, so contact him at richardb@briefing.co.uk



Kayli Olson is **Briefing**'s assistant editor, in charge of gathering stories and data. Want to contribute? Contact: kaylio@briefing.co.uk



Josh Adcock is **Briefing**'s editorial assistant. He rolls up his sleeves on everything from interviews to production. Contact: joshad@briefing.co.uk



Chris Cardon is **Briefing**'s client services manager, responsible for managing all our supplier insight. Contact: chrisc@briefing.co.uk



Rupert Collins-White is creative director at Burlington Media. Contact: rupertw@briefing.co.uk



Sarah Cox is Burlington Media's client services director. Contact her at sarahc@briefing.co.uk

TALK TO US

Briefing on Twitter
@Briefinglegal

Email us your thoughts
editorial@briefing.co.uk

Find all our back issues online
www.briefing.co.uk

Join the **Briefing** LinkedIn group
bit.ly/BriefingLinkedIn

Write us a letter (remember those?)
Briefing magazine
Burlington Media Group
20 Mortlake High St
London SW14 8JN
DX36356
EAST SHEEN

SPONSORED BY

EzeCastle
INTEGRATION

Secureworks®

DVV
solutions

Racking up threat

Cybersecurity was one of two new 'priority risks' to make the Solicitors Regulation Authority's set of 10 in its 2018/2019 risk outlook. It is, of course, hardly a new risk. "But we recognise that this is of increasing concern to the profession, so we have set it out as a separate risk," the SRA said in its foreword to this regular report.

The regulator itself received 157 reports of cybercrime back in 2017, up 52% on 2016 – and of course, the nature of attacks continues to evolve. In 2017, for example, it says that email fraud fell to an average of just under half (46%) of those crossing its path; in the first quarter of 2018 this had shot up to 71%. Email modification, or so-called 'Friday afternoon', fraud is the most common of the scams that hit law firms, where criminals falsify emails from a supposed client, (or the firm itself) leading to new bank details being handed over by one or the other. And of course, there are the likes of phishing/vishing activity and malware/ransomware – both of which were also singled out in the UK National Cyber Security Centre's first report on the threat level facing the legal sector specifically in 2018.

In its outlook, the SRA also puts the rise of remote/flexible working under the spotlight – all well and good for employee retention and engagement, I expect most would now agree, but also coming with a less bright side. The 'bring your own device' movement requires all the right updates to maintain access fully securely. This shouldn't come as a surprise, but that isn't to say it always happens. And malware is also now targeting videoconferencing setups and smart connected devices that play into process improvement initiatives such as internet-connected printers.

To turn now to our own research in this spotlight supplement, a whopping 82% of law firm business leaders see the cyber threat facing them as no more or less intimidating than that lying in wait for that firm over the road (14% reckon they're a higher risk, only 4% say lower). With a 'positive' gloss, we might say that means they know they're pretty much all in the same boat – at risk, right now. But cybersecurity doesn't just cost if you do a bad job of it. It also costs to implement it. It seems there are no easy answers as to how much to invest, but firms certainly need to figure out what to prioritise for themselves.

RICHARD BRENT EDITOR-IN-CHIEF

Contents

04 Mindset the gap?
Dean Hill, executive director at **Eze Castle Integration**, says there's always more to do on cybersecurity, so it makes sense for firms to find a trusted partner

06 Place your threats
The **Briefing** Legal IT landscapes 2019 research found that technology for cybersecurity was yet to prove itself. So, what exactly are law firms doing to manage their risk?



Mindset the gap?

Dean Hill, executive director at Eze Castle Integration, says cybersecurity is a particularly challenging area for firms to invest in, but they can't afford to be ill-prepared for the worst

Law firms today are becoming increasingly knowledgeable about the range of cybersecurity attack they could expect to see targeting their systems. The area of management that they most need to improve is addressing their risk profile and exposure proactively. Proper incident response to mitigate the impact of an attack continues to be business-critical – but certain actions can also reduce the likelihood of a successful attempt in the first place.

In fact, businesses need to be as assiduous as those behind the growing threats they face. Cybercriminals in 2019 are doing due diligence of their own: more detailed research on the

vulnerabilities of both software and the people in organisations who use it – practising and honing their skills to increase their own chances of success and ensure they're only spotted late in the attack.

Finding the resources to meet that sizable effort can present a challenge. Large global organisations like top law firms will have strong, hard-working IT teams, but even then, running a 24/7 information security monitoring operation may present a significant burden. Instead, it may make more sense to partner with an outsourced specialist in threat management, highly trained to track emerging types of attack and their modus operandi, as well as the best ways to see them off.



For more information, visit:
www.eci.com

Client concerns

It's unsurprising that only a minority of firms have so far recruited or appointed a chief information security officer. The remit for this role is wide – encompassing networking, process, remediation and event management. And there's a market shortage of the skillset needed to take that on, even before considering whether the workload is manageable.

However, another problem when it comes to making strategic investment may be one of mindset. There's a tendency for people to think terrible events simply won't happen to them – so, the reasoning goes, why pay for the most expensive insurance policy? Of course, they could end up paying out more to recover once hit – not to mention the impact on a carefully guarded reputation that could cost a few profitable clients.

Those same clients' levels of interest in firms' security decision-making and practices is a trend that's only going in one direction. Requests for proposal now often include specific questions about information security preparedness, and companies will potentially conduct their own audits before awarding work. Some clients even want to know about the processes in place at firms' supplier partners. Of course, if firms are well prepared, they should arguably be prepared to pass that information on with confidence.

It also appears that some firms don't appreciate that their sensitive documents and data are as attractive to criminals as large sums of money that might be available in other infrastructures. Cybercriminals will pursue whatever generates money, and one of the biggest things in that category is data. Ransomware, for example, has the potential to threaten individuals and organisations with repercussions for their data if they refuse to pay. Data can also be used to go after clients' money more effectively.

Moving targets


The bottom line here is that complacency and/or denial is likely to cost more than investment in a cybersecurity strategy – and the factor that places firms at most risk. However, both sensitive documents and data are also at greater risk with

Another problem when it comes to making strategic investment may be one of mindset. There's a tendency for people to think terrible events simply won't happen to them

the rise in remote working patterns. More devices means more possible points of entry, and of course these can be left on a bench or train. Firms must invest in technology to protect files, but people also need the training in behaviours, policies – and yes, the technology – to prevent them from becoming a significant part of the problem (never mind helping with the solution).

Fortunately, some categories of technology are also coming forward to help with these very human security challenges. Machine learning or automation software, for example, may be in a position to support aspects of education. Tools might issue the timeliest reminders or prompts to take (or not take) specific actions, and use past and present data to better predict the shapes and times of future attacks.

However, isolated implementations of security technology and one-time employee training sessions are not enough. The risk landscape is changing rapidly, meaning today's technology update or top lesson may no longer even be relevant in a few months' time as the attackers start on a new route. Rather, firms must adopt a security-first mentality and create a culture of security, where personal responsibility, awareness of consequences, strong communication skills and the regular knowledge updates are standard.

Finally, culture needs consistent work itself, even at the best of times. The top tier of business leadership should be visibly backing the communication and reiteration of security messages – leading by example, and sharing knowledge regularly for it to filter through to the defensive 'front line' effectively. And whether the board is investing in a CISO any time soon, or seeking the support of a close specialist partner, an information security culture – as with much of management – benefits from having a recognisable human face. 

RESEARCH

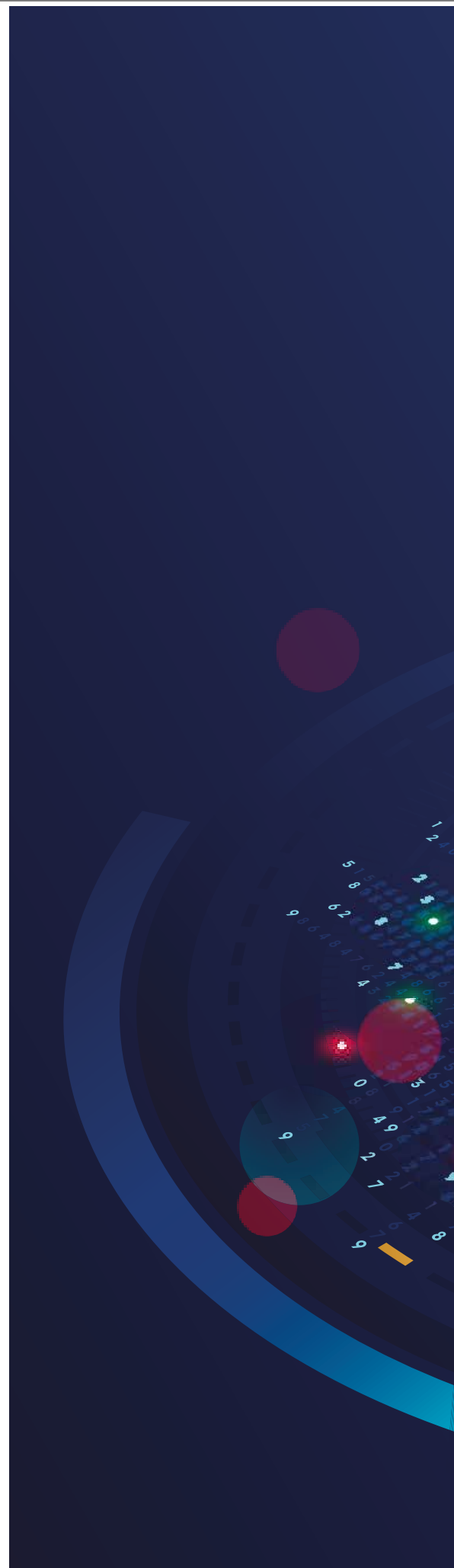
Place your threats

The number of law firms reporting information security incidents is on the up. **Briefing** Legal IT landscapes 2019 enquires what, if anything, can be done. Richard Brent reports; additional reporting from Andrew Muir

In July 2018, the National Cyber Security Centre (NCSC), part of GCHQ, published its first report on the extent of the cyber threat facing the UK's legal sector specifically. The research found that 60% of law firms had reported some form of information security incident in 2016–2017 – an increase of almost 20% on the previous 12 months. The most significant threats faced by firms were phishing, data breaches, ransomware and supply chain compromise – and the Solicitors Regulation Authority estimates that over the same period more than £11m of client money was reported stolen by cybercriminals.

A NCSC spokesperson says: “Cybersecurity is all too often thought of as an ‘IT issue’.” Rather, the NCSC would “encourage business leaders to understand cyber risk in the same way as they understand financial, or health and safety risk”.

A year earlier, in August 2016, the NCSC had already published its ‘10 Steps to Cybersecurity’ (see box, p12). Now, it says, it has further launched a private ‘legal sector’ group within its free Cyber







You're only strong as your weakest link

DVV Solutions deliver a comprehensive approach to Third Party Risk Management:

- ✓ Managed services - on-demand assessments to total program management
- ✓ Third Party risk framework development and maturity
- ✓ Assessment automation, reporting and remediation tracking platform
- ✓ Continuous monitoring across 5 key data and business risk domains
- ✓ Evidence sharing networks to accelerate your TPRM
- ✓ Risk advisory and remediation consultancy

**Take the pain out of
Third Party Risk Management.**

Contact us on 0161 476 8700 **or**
Learn more at dvvs.co.uk



“Investment in cyber defences should be decided by the stakeholders – owners or the management board – as it needs to meet each firm’s specific needs.”

*Chris Simmons, IT director,
Bates Wells Braithwaite*

Information Sharing Partnership (CiSP) – the latter a “joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business”.

But the NCSC’s ‘step one’ of 10 is “defining and communicating your board’s information risk management regime as central to the organisation’s overall cybersecurity strategy”.

A challenge of solutions?

In spite of no let-up in high-profile incidents – including some that have hurt high-profile law firms – **Briefing’s** latest Legal IT landscapes research into how firms’ technology leaders view the potential of different categories of technology (plotted for efficiency against competitiveness) did not identify cybersecurity solutions as ‘one to watch’. The question is, why?

Chris Simmons, IT director at Bates Wells Braithwaite, says that the market for technology products offering help with something everyone admits is a continuous battle – as attackers keep shifting to exploit new weaknesses – is probably still too immature.

“As demand for cybersecurity services grows, many new companies will spring up overnight,” he says. “Some will sell fear, while others will offer high-quality advice and support. The sector will then consolidate and knowledge will spread, until finally acceptance of the need to embed cybersecurity becomes commonplace.

“However, investment in cyber defences should be decided by the stakeholders – owners or the management board – as it needs to be balanced against what the firm can afford and meet each firm’s specific needs. Matching measures to the overall budget is a skill that differentiates IT professionals.

“At BWB the topic is regularly discussed at board level – with both the CIO and compliance officer for legal practice viewed as gatekeepers and process specialists.” He says that this voice on the board is not found in all firms however, and the size of organisation doesn’t appear to be the deciding factor.

I need a CISO?

Is that ability to assess and decide exactly what needs to be done to prepare perhaps the difference that a chief information security officer (CISO) job title makes? If so, it’s a skillset yet to find its way into legal. In Legal IT landscapes 2019, only 15% of law firm leaders report that somebody with the specific title CISO is the most senior person responsible for information security in their firm (p9). At three-fifths of firms it is a CIO or IT director, and at a quarter of firms it’s somebody else entirely.

Shane Scott, information systems director at Shoosmiths, says: “First, you have to define what is meant by CISO. Many instances I have seen in play within law firms are still largely technical. The full scope would cut across technical, behavioural and information security frameworks – encompassing data loss prevention, risk management, and so on. For a multinational I think it is a relevant role, but for purely national firms I don’t think there is always enough of a role.” At Shoosmiths, he says, the areas described are shared between himself and the compliance director.

“Any structure also needs to reflect the risks and threats that are relevant to a firm’s commercial position. Our threats and risks are similar – from a generic perspective – but they can be quite different practically. We take security frameworks and implement the elements that are relevant for



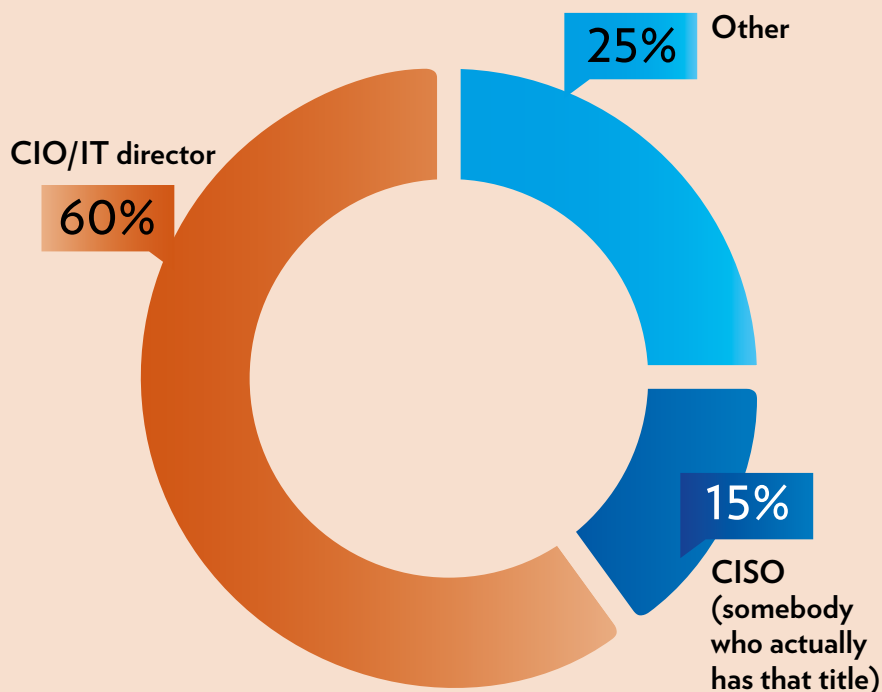
Cybersecurity. It's woven into our DNA.

Collectively Smarter. Exponentially Safer.™

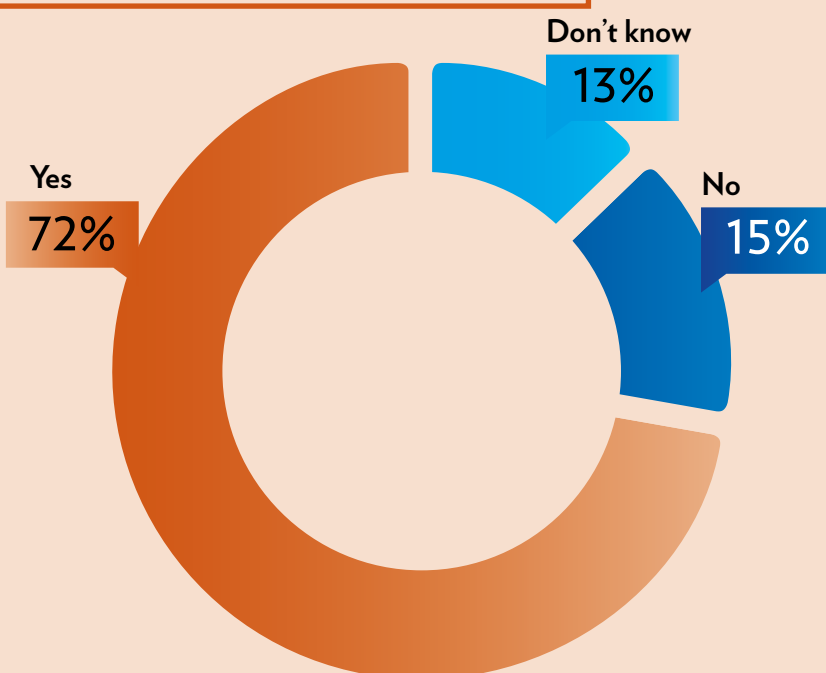
Contact us to learn more:
+44-131-260-3044, info@secureworks.com
secureworks.co.uk

Secureworks®

Which role is the most senior person responsible for information security within your organisation?



Are you seeing an increase in the number of clients performing security audits on you?



“Many instances I have seen in play within law firms are still largely technical. The full scope would cut across technical, behavioural and information security frameworks.”

Shane Scott, information systems director, Shoosmiths

60%

Of UK law firms experienced a cybersecurity “incident” in 2016-2017, according to the National Cyber Security Centre (NCSC), part of GCHQ



the threats and risks we perceive as relevant to our commercial circumstances. The review and reporting of these are tailored to what our executive wants and needs to hear.”

Nick Galt, IT director at Boodle Hatfield, sees business value in a CISO appointment. “The data that we hold is commercially valuable and, equally, is personally sensitive to our clients. Also, as a law firm’s systems become more complex and integrated, access is more difficult to manage and monitor. Practically, however, a smaller law firm cannot afford a CISO, so the responsibility devolves to the IT director or head.”

David Aird, IT director at DAC Beachcroft, agrees. “A CISO is definitely worthwhile, but it comes at a cost that may be too high for some. The value lies in the holistic nature of the role – focusing on more than just the technical points. And the best ones are very pragmatic, able to balance what the business sets out to achieve with the safest, most efficient way to achieve that.

“The role also needs to be well connected. As a sector, at times we can be quite insular – only looking at the legal market – but a CISO should have broad exposure to the full range of business challenges.”

He adds that the idea of ‘CISO-as-a-service’ appears to be gaining traction as one to help some firms resource themselves in the area, while Simmons says that BWB has reduced its need for a dedicated CISO by investing heavily in management areas such as repeated cyber-awareness communications and training.

“The need for a dedicated CISO depends on the

“A CISO is definitely worthwhile, but it comes at a cost that may be too high for some. The value lies in the holistic nature of the role – focusing on more than just the technical points.”

*David Aird, IT director,
DAC Beachcroft*

SPONSOR COMMENT

Share the security burden

Mike McLellan, senior security researcher, Secureworks Counter Threat Unit, says it’s crucial the board gets onboard with information security

Legal sector organisations face a unique blend of threats: from malicious insiders seeking to steal client information for financial gain, to organised criminal gangs extorting money in return for preserving the confidentiality and availability of data. Even sophisticated nation-state actors focused on stealing sensitive information, or exploiting trusted relationships to attack law firms’ clients, are becoming more commonplace. The impact that these attacks can have on the confidence and trust that clients place in their legal representatives can be huge.

Consequently, firms need to recognise that information security is a business risk, not just an IT one, and ensure that the topic has board-level scrutiny, coupled with appropriate resourcing and governance further down the organisation. Where possible, organisations should look for mechanisms by which they can share threat information and best practice with their peers, even if they are competitors. The goal for all law firms has to be to force attackers to work harder to be successful, and working together can have an amplifying effect on security across the board.

It’s interesting to note from the Legal IT landscapes research results that clients are increasingly focused on this area, and are actively auditing the information security standards of the organisations to whom they entrust some of their most sensitive information. It remains the case that fundamental security controls such as patching, logging, active management of user passwords and the use of two-factor authentication for internet-facing services will protect organisations against the vast majority of attacks. Do not place the burden of securing systems solely on the users of those systems. Train them, but also assume that some attacks will nevertheless succeed, and also focus on being able to spot and block those attacks through the application of layered security controls.

Do not place the burden of securing systems solely on the users of those systems. Train them, but also assume that some attacks will nevertheless succeed. Focus on being able to spot and block those attacks

www.secureworks.co.uk
Mike McLellan
Senior security researcher

What are your biggest 'threat vectors' for cybersecurity?

PEOPLE



EMAIL

FINANCE

PARTICULAR
WORK TYPES (EG,
TRANSACTIONAL,
PROPERTY)



DOCUMENT/
MATTER-LEVEL
SECURITY
WEAKNESSES

MOBILITY

SOME OTHER STUFF!

Largest letters/darkest red = most mentions!

Step by step



The National Cyber Security Centre's 10 Steps to Cybersecurity includes 10 'technical advice sheets', covering:

1. Risk management regime
2. Secure configuration
3. Network security
4. Managing user privileges
5. User education and awareness
6. Incident management
7. Malware prevention
8. Monitoring
9. Removable media controls
10. Home and mobile working

Source: www.ncsc.gov.uk/guidance/10-steps-cyber-security

size of the firm or size of the problem," he says. "Larger firms will have the resources to dedicate a specialist to this role, and firms working in an environment where they are a prime target will either dedicate someone to handle this responsibility, or outsource the role to another individual or organisation."

In the case of the latter course, he says, "they should be able to rely on the outsourced provider for cyber protection. However, some outsource providers may exclude this from contracts, so buyers need to be on their guard to make sure this is included as part of the service agreement, and that the provider has the necessary skills to introduce robust and lasting measures."

On top of the risks

However, whether it's CISO or any other title in charge, Karen Jacks, IT director at Bird & Bird, agrees that the person in these shoes doesn't simply need to know their technology – perhaps another factor behind why they are so hard to fill.

"You can throw plenty of technology at the situation, but a lot of the work is around risk analysis, mitigation, horizon-scanning, process, user awareness and behaviour, and even managing clients' expectations around risk profile. That's not such a natural fit for the technology team."

Indeed, Galt adds one aspect of employee

behaviour is probably the very top challenge faced in this area of risk management (note the very top 'threat vector' that Legal IT landscapes respondents cited on p11). "It's the growing use of applications such as DocuSign and Dropbox to spread malware, and educating fee earners on the dangers in not questioning the source of communications before clicking on a link or button. Our infosecurity training is covered on induction, and thereafter by alerts when phishing attacks come in. Policy updates are also communicated through quarterly meetings, email notification and intranet announcements."

Jacks also echoes the NCSC's main message mentioned above. "The key is less what you will invest or what somebody is called, and more the clear commitment of management at the very top. If security is seen as just an 'IT issue', I think that's when you really do have an issue. Whereas if you have the support of the leadership it will be significantly easier to make the necessary changes."

For example, as well as driving good behaviours, that support might help to soften the impact of some restrictions on ways of working. "We all want to operate as openly and freely as possible, so there are some actions you have to put in place that can be seen as prohibitive – you need support there as well," explains Jacks. "Fortunately, our CEO is very aware, and has good conversations on the subject. We also have a risk and audit committee, which isn't involved on an operational level, but does want to be assured we're applying the same level of attention to information security as we are to regulatory risks such as conflicts or money laundering."

Ticking lock?

In this year's Legal IT landscapes research, we also asked a question about one such potential restriction – do you currently use a 'need-to-know' security policy as the default when starting a new matter (p13)? Only 16% of respondents said they did this all the time, but more (18%) did not and another 16% simply didn't know. Almost a third



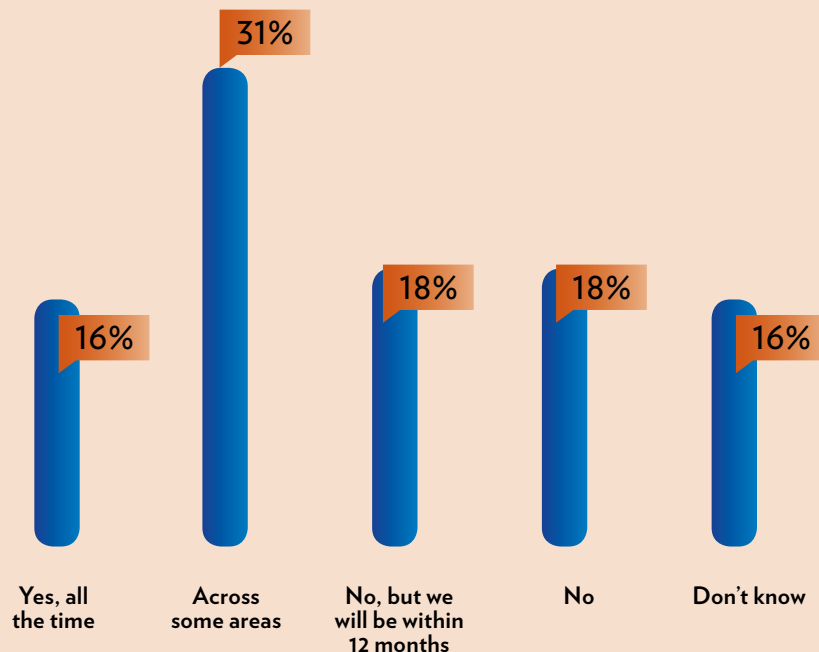
“The key is less what you will invest or what somebody is called, and more the clear commitment of management at the very top. If security is seen as just an ‘IT issue’, I think that’s when you really do have an issue.”

*Karen Jacks, IT director,
Bird & Bird*

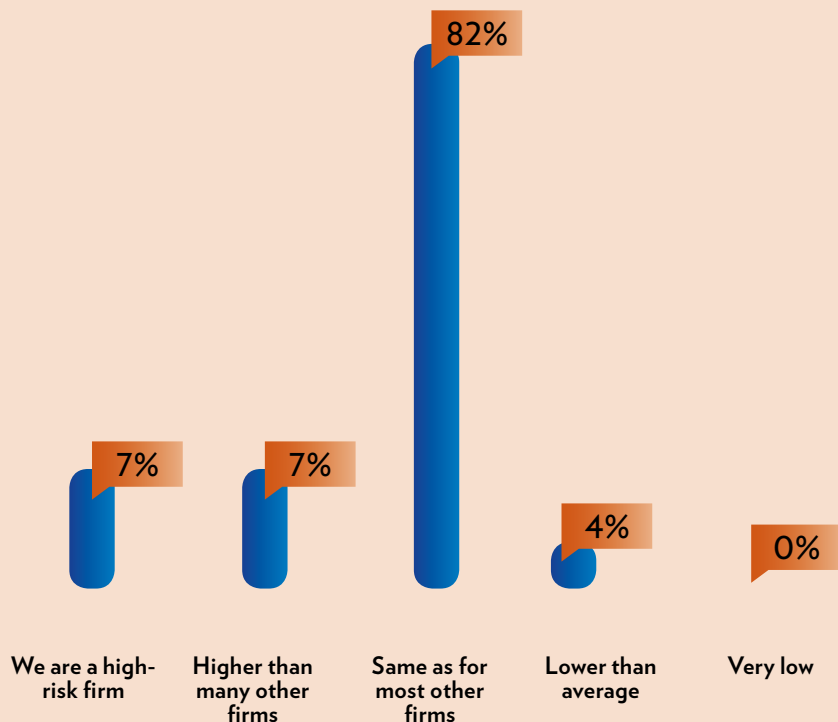
£11m

Of client money was reported stolen by cybercriminals in 2016–2017, says the UK National Cyber Security Centre in its first legal threat report (estimate by the Solicitors Regulation Authority)

Do you currently use ‘need-to-know’ security as a default policy for working on new matters?



Rate the level of threat against your firm ... right now



“One of the big security threats for an organisation is the potential actions of an ‘insider’, and you can’t leak something if you don’t have access in the first place.”

Anthony Stables, chief information officer, Forsters



(31%) said they applied something like this “across some areas”.

Jacks at Bird & Bird says: “We’ve embarked on a project to take the document management system need-to-know by client – it’s really quite a big change to make.”

Anthony Stables, chief information officer at Forsters, is in the midst of something similar. “We’re moving to a tight framework, with full role-based access control. After all, one of the big security threats for an organisation is the potential actions of an ‘insider’, and you can’t leak something if you don’t have the access in the first place.”

And Nick Galt, IT director at Boodle Hatfield, is exploring options in this regard, but has secured buy-in in principle to roll out the same across his firm. “Like many firms, we’ve historically operated an open system, with matters only locked down to ‘need-to-know’ by request.” The alternative may appear less convenient, he says, “but GDPR seems to have focused people’s minds a bit. Now they see this as the more risk-averse approach.”

Scott at Shoosmiths adds: “We have a continual process improvement programme (PIP) within three domains: cybersecurity (the technical aspects), information access (who has access to what) and information governance (what do we hold and why). Each domain is on either a weekly or a monthly review agenda.” He says that the priorities within each of these domains include:

- **Technical:** Contagion mitigation, “ensuring that any form of malware/infection/breach can be contained within a relatively small area of our network”
- **Access:** “Ensuring appropriate controls with regard to employee information access at the right

level for the role – effectively data loss prevention, records management and prevention”

- **GDPR review:** What to keep, why, and for how long.

Arguably, specific policies should also factor in what firms’ clients think about the balance between risk and efficiency. This year, Legal IT landscapes polled whether leaders were seeing an increase in the number of clients requesting security audits on the firm. For almost three-quarters (72%) the answer was a resounding yes – only 15% said no (p9).

Galt says Boodle Hatfield is among the 15%. “As a result of our specific practice areas, we rarely get a request for an audit,” he says.

Scott at Shoosmiths says: “The most common details interrogated are around our technical capabilities, such as security incident and event management, and technical mitigation strategies – Distributed Denial of Service, data loss prevention, firewalls, intrusion detection system, and so on. And of course, there are the various accreditation schemes such as ISO 27001 and the government-backed Cyber Essentials Plus.”

By all accounts, cybersecurity is a subject no more likely to go away than the internet or crime itself. As chains of law firm communication and command grow more complex, and systems such as artificial intelligence eventually bed in, the spectrum of risks will only shift in response. Law firms will continue to be ‘victims’ in some sense – and indeed their management teams ought to expect that. They can, however, take steps to manage risk more effectively and ensure their defence and response work is resourced appropriately. ▴