CONFERENCE REPORT

10TH OCTOBER 2017

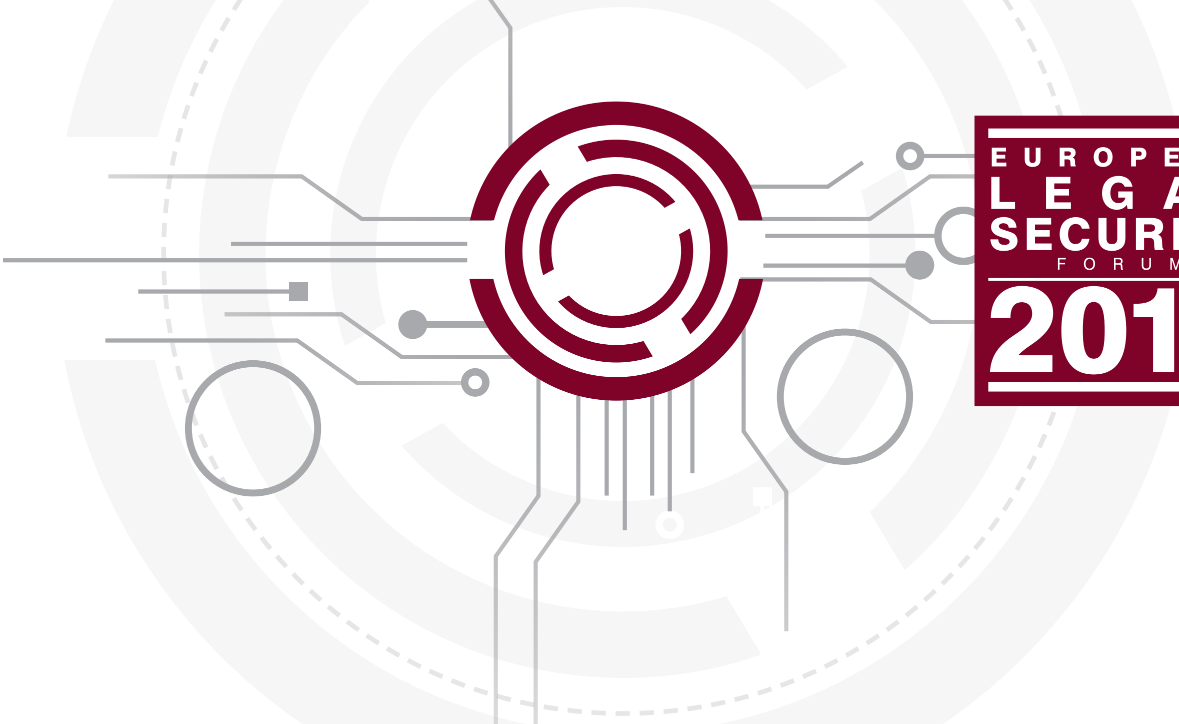
OLD BILLINGSGATE • LONDON

EUROPE'S LARGEST LAW EXPO JUST GOT BIGGER
EUROPEAN LEGAL SECURITY FORUM
2017
LONDON LAW EXPO
2017
TS, 1 VENUE, 1 DAY
CTOBER 2017

An EVENT BY

NetLawMedia

EUROPEAN LEGAL SECURITY FORUM 2017



EUROPEAN LEGAL SECURITY FORUM 2017

Bigger and better than ever before

In October 2017, Netlaw Media, the legal conference organiser, held its largest ever event – the combined London Law Expo and European Legal Security Forum.

More than 2,000 delegates from 35 countries descended on Old Billingsgate in London for a packed day of presentations, demonstrations and discussions, held across six stages. Over 60 speakers from the legal, academic, government and vendor communities took part in the proceedings, with enthusiastic discussions ranging from the future of legal services delivery to IT security, and law firm branding to GDPR compliance. This report offers a taster of the day's highlights. By Richard Parnham.

Is your firm an easy target for cyber attacks?

The cyber security threat to law firms is real and attacks are commonplace. These were the key takeaways from the recent European Legal Security Forum (ELSF).

> Cyber attacks on law firms have increased by 60 per cent in the past two years

Not one but several European Legal Security Forum speakers made it clear that the IT security community regards the legal profession as a soft target for cyber attacks. Speaking at the event, 'Lucy', a representative from the UK government's National Cyber Security Centre (NCSC), offered several sobering statistics.

Research suggests that cyber attacks on law firms have increased by 60 per cent in the past two years; ransomware and phishing email fraud were the most common methods of attack, although theft of client data is also a problem. In financial terms, the value of cyber-fraud thefts from law firms reached £3.2 million in the first quarter of this year alone – a threefold increase on the same period in 2016.

To help mitigate against some of the more common cyber security challenges facing the sector, Lucy drew the audience's attention to the government-backed Active Cyber Defence (ACD) programme – a suite of largely automated security measures that aim to tackle a significant proportion of the cyber-attacks hitting the UK.

'Tina' another NSCS speaker, encouraged those attending the ELSF to consider joining CiSP, the NCSC's Cyber Security Information Sharing Partnership, which offers an early warning service, as well as its Cyber Network Reporting (CNR) programme, which includes a free tool for detecting malicious network activity. 'We're also working with the Law Society to set up a private [CiSP] group specifically for law firms,' she said.

Throughout the day, numerous speakers described the legal profession as a soft target for cyber attacks, particularly when compared with banks and other financial institutions. This seems to be because law firms tend to spend less on IT security than these other sectors, even though they hold highly valuable – even potentially stock market impacting – client data.

Illustrating this point, security analyst Graham Cluley put forward the example of a Canadian law firm, whose network was compromised over a period lasting several years. This low-key attack enabled hackers to sell access to the firm's confidential data. 'On the dark web, you could actually take out a monthly subscription to get all of the firm's latest updates,' said Cluley. Compared with ransomware, this form of infection is far more insidious. 'At least ransomware is obvious because your computers stop working,' he said.

Elsewhere in the conference hall, one person with a first-hand experience of cyber security risks was Jason Plant, head of lawyer innovation at DLA Piper. Over the summer, the firm was memorably caught up in a cyber attack, which left some of its IT systems crippled for weeks. Speaking at our parallel London Law Expo event, Plant explained that the attack didn't happen because the firm had failed to patch its software. Rather, the attacker had compromised a third-party solutions provider the firm relied on. When DLA Piper installed this vendor's software patch, its own systems were affected.

Plant insisted that law practices should actively evaluate their IT solutions providers for their cyber security vulnerabilities. Just as law clients are increasingly subjecting firms to such evaluations, so should law firms, in turn, scrutinise their IT suppliers. 'Supply chain management is becoming critical in this area,' he warned.

> ”
> **Law firms spend less on IT security than banking and financial institutions**

Human error

Unfortunately, not all the attacks on law firms' IT systems depend on sophisticated software-based hacks. Speaking at the ELSF panel discussion 'Why are law firms a target?', Mark Leiser, a cyber law expert from Leicester University, emphasised that it's possible to access a firm's network with nothing more than a mobile phone and a plausible story.

He went on to describe an experiment he conducted on several law firms based around Glasgow's criminal court. After making a note of each firm's publicly accessible Wi-Fi box name, he phoned each practice office, pretending to be a BT engineer. Claiming that he was testing the firm's phone line, he asked them to read out all the details on the back of their Wi-Fi box – including the router's password. Amazingly, he said, of the ten firms he was able to speak to, three willingly provided him with this information, thereby rendering their networks vulnerable to an attack. Leiser admitted that his experiment was probably 'ethically and morally wrong', but his point was well-made.

In a separate presentation on the psychology of cyber hacking, Jenny Radcliffe – aka 'The People Hacker' – claimed that 'praise and flattery work really well' in getting people to drop their IT security guard. Demonstrating how easy it is to persuade someone to click on an email link, she offered the scenario of a spoof message from a fake magazine, in which 'leaders in their industry' were sent a list of questions and a request for an interview. Within the email was a link, supposedly to the magazine's website; in fact, Radcliffe said, anyone clicking on it would instantly infect their computer. Needless to say, this type of press interview request is commonplace in the legal sector.

So, given the gravity of the situation, how should individual firms respond? Clearly, IT security technology – including many solutions being promoted at the ELSF – can help protect against the vast majority of common risks. However, as the speakers repeatedly made clear, technology can only form part of any firm's defensive armoury; humans also play a vital role in ensuring the security of legal practices.

> **IT security is everyone's job – not just the person that's got the words in their job title**

Making this point, Sue Diver, head of information security and data protection at Clarke Willmott, offered a blunt message regarding how she herself approaches this issue. Although the firm has numerous IT security measures in place, including an ISO/IEC 27001 accreditation, she told the ESLF audience, 'I go around my organisation saying that information security is not my job.' This is because she sees her role as helping others to do their own job securely.

'That's the message we have to get through,' Diver insisted, wrapping up the debate. 'IT security is everyone's job – not just the person that's got the words in their job title.'

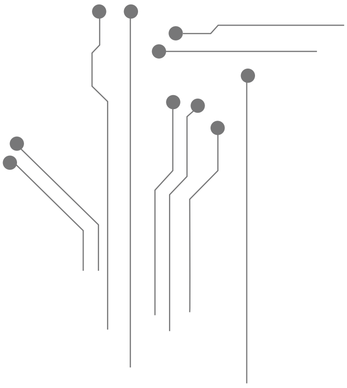
17 +

Netlaw Media's 17th sold out Law Event in succession

GDPR – a challenge and an opportunity

Promising huge fines, the pending GDPR data protection provision is a legal framework that will have a massive impact on UK law firms and their client security.

Emerging from the parallel London Law Expo (LLE) and European Legal Security Forum (ELSF) conferences was a single regulatory development that speaker after speaker returned to – the forthcoming General Data Protection Regulation (GDPR). Due to be adopted across the EU by 25 May 2018, GDPR will touch on numerous aspects of the business of law. These include the way in which law firms market themselves, how they store and process client data, even the insurance policies they take out. So all-pervasive was GDRP at the proceedings, one speaker pointedly joked that they had managed to get through their entire talk without mentioning 'those four letters'.



The GDPR will have a significant impact on the UK legal sector, Brexit notwithstanding. This is because GDPR applies to any organisation that holds data on EU citizens, irrespective of where in the world that firm is based. Therefore, UK law firms will fall within the regulation's provisions post-Brexit, even if they have just one EU client. What's more, the UK government aims to give effect to the GDPR's provisions via an act of parliament, up to one year before Brexit occurs.
For one event speaker, the advent of the GDPR is unquestionably a good thing. Speaking at the LLE, Chris Butlin, director

of professional services at Pitney Bowes, observed that the current UK data protection regime – in essence, the Data Protection Act 1998 – predates much of the 'data volume explosion' that has since taken place. The GDPR is specifically intended to reflect the new data reality, he argued, placing the need for data security, accuracy and informed customer consent at the heart of its protections.

By forcing organisations to comply with the regulation's requirements, Butlin said the GDPR will encourage them to go on a 'digital transformational journey.' Firms that are able to consolidate, standardise and link together different pieces of customer data will end up with a 'golden record' and 'single view' of each of their clients. This, in turn, will allow organisations to offer their customers a consistent experience, no matter what platform they use to contact them.

That said, several speakers acknowledged that the process for moving towards GDPR compliance should not be underestimated. Lee Fisher, EMEA security lead at Juniper Networks, told the ELSF audience, 'I'm not going to stand in front of you today and pretend there's a technical answer,' he said – particularly since there is no industry standard checklist that firms will be able to rely on, or a software version they can install. 'You're going to have to look at the entire ecosystem of how you capture, use, process, store, share, store, interactive with and dispose of data – all of it,' he said.

The GDPR is a legal framework, not a technical one. This means that the question of whether or not an organisation is in breach of its provisions will ultimately be a matter of interpretation. 'If asked "What could you do?" and "What did you do?", you're just going to have to stand up and justify your answer,' Fisher said.

First steps

Starting from first principles, Fisher suggested that firms should define what customer data they actually require, and why they need to collect it at all. By way of illustration, he questioned why so many websites ask for his date of birth, which has nothing to do with the service they provide. "If you have no reason for that data – get rid of it," he said.

> ”
> **UK law firms will fall within the regulation's provisions post-Brexit, even if they have just one EU client**

Firms should also be transparent about how they intend to use their customers' data and be able to prove that informed customer consent had been given. Here, Fisher offered the extreme example of pub company JD Wetherspoon, which recently deleted its entire email marketing database. Presumably, he speculated, JD Wetherspoon had been unable to demonstrate that its customers were sober – and therefore gave informed consent – when they signed up to the company's mailing list.

Elsewhere in the conference hall, Peter Wright, managing director of DigitalLawUK, discussed whether a cyber insurance policy might act as a catch-all form of protection, in the event that an organisation found itself in breach of the GDPR's provisions. 'Certainly, you'll want to have that safety net in place,' he said. 'But, don't forget it's insurance – insurers won't pay out if they can possibly help it.'

Cyber insurance policies tend to offer very different levels of cover, Wright said. As a result, a specific policy may not cover the type of GDPR-related loss that a firm might incur. For example, would a cyber insurance policy cover the losses associated with a post-breach resignation of key team members?

However, Wright pointed out that most organisations are unlikely to be hit by a massive fine in the event of a minor GDPR breach. Noting that the maximum possible fine under the GDPR is four per cent of global turnover or €20 million (whichever is greater), Wright observed, 'Today, the Information Commission's Office (ICO) can fine you up to £500,000 – and they've never done that.'

Even telecommunications firm TalkTalk was only fined £400,000 – the highest ever fine issued by the ICO. 'And what TalkTalk did was so wilfully ignorant of what they should have been doing that it beggars belief,' he said. In Wright's view, substantial GDPR fines will only be imposed on organisations if their regulatory failure amounts to a 'persistent, wilful and ignorant neglect of the law.'

The view from MI6

It's not every day that law firm leaders get to interrogate a former head of MI6 – but they did at the recent European Legal Security Forum

Sir John Sawers, who led the UK's main external security agency between 2009 and 2014, delivered a keynote address and took part in a follow-up panel debate. After providing a downbeat assessment of the global security situation, in which he feared ongoing upheavals in the Middle East and further terrorist threats in Europe, Sir John then turned to the issue of IT security.

Here, he expressed with wry amusement that Russia had been hit hard by the recent WannaCry ransomware attack – due to the country's widespread use of pirated Windows software, which hadn't been updated or patched.

Offering his opinion on the politically contentious issue of data encryption, Sir John echoed the recent views of former MI5 head Jonathan Evans, saying he was 100 per cent in favour of strong encryption. 'It's a really important part of preserving our security in this interconnected world,' he said. Later, in a straw poll on the issue, an overwhelming majority of the event audience indicated that they agreed with Sir John's position.

In the panel discussion following his keynote presentation, Sir John said he thought the Edward Snowden revelations marked the end of the – previously informal – working relationship between technology companies and the security services, where the former allowed the latter to access their services via a 'back door'. Nowadays, technology companies have moved to a situation where they're behaving more like safe manufacturers, unable to unlock their own products. As a result, there are now entire sections of the internet that Sir John described as 'no-go areas' – 'That's not a satisfactory outcome for me as a citizen, let alone as a former intelligence security chief,' he said.

A fresh outlook

So what's the answer? As back-door access to encrypted technology is politically impossible and it's unrealistic to expect technology companies to cease developing new solutions, Sir John suggested an alternative approach: bringing about the 'same sort of front-door access into the virtual world that you have in the physical world.' Just as warrants can be issued to search houses or tap into private phone calls, so broadly similar interception options could be made available to internet communications.

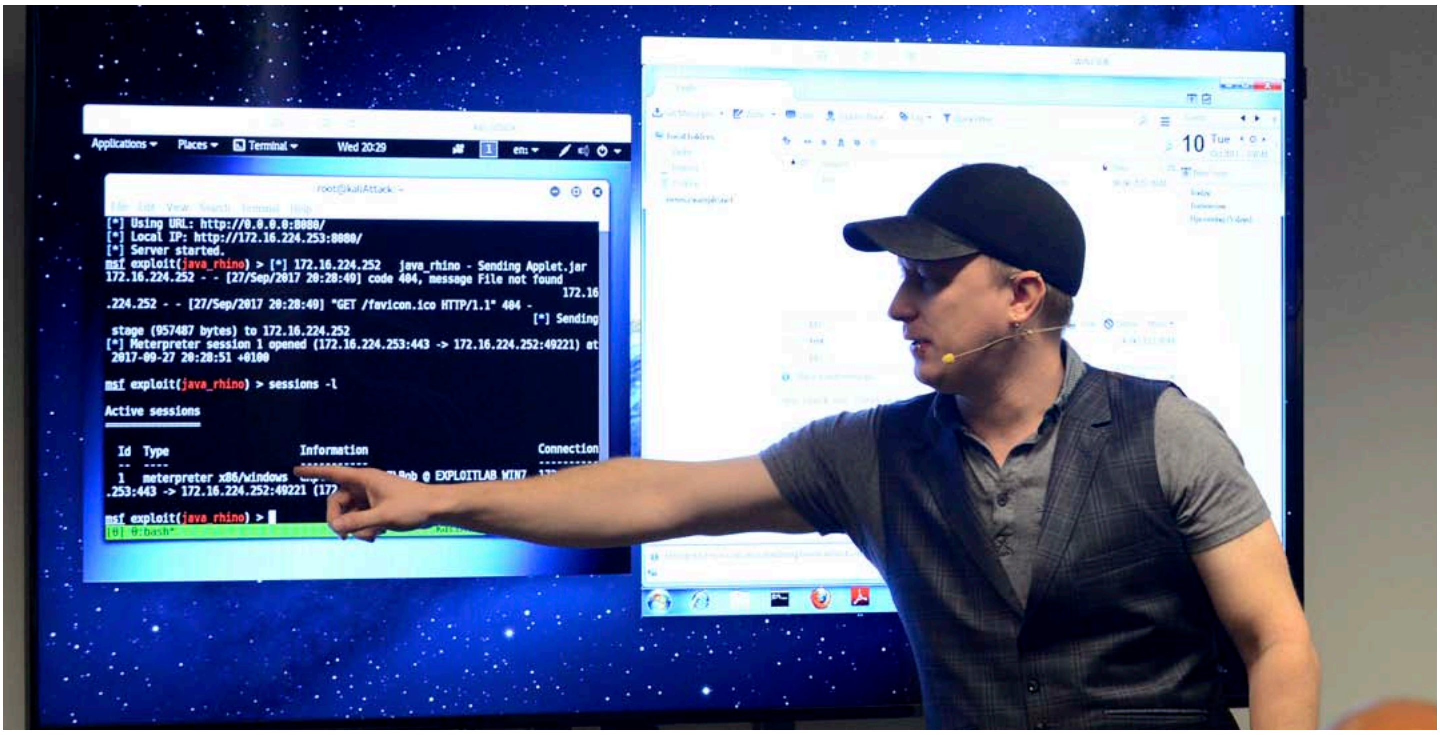
The rights of security services to intercept communications could be set out in an internationally-agreed legal framework, so that 'we all understand what is acceptable, and what crosses a red line.' He said that if an international agreement could be reached in relation to the treatment of nuclear weapons, for example, there was no reason why an equivalent cross-border consensus could not be reached between states regarding the balance between cyber security and data privacy.

Perhaps unsurprisingly, Sir John's endorsement of an albeit limited state intrusion into people's online lives sparked a debate between him and several members of the ELSF audience, who expressed disquiet about his approach on privacy grounds. However, Sir John insisted that the only alternative outcome is that everyone must accept a world 'in which law and order doesn't operate in great areas of our existence.' That scenario is far worse, he said, because 'law and order is the basis of our freedoms.'

" The likes of Google are softening their hard line on privacy to get into China and elsewhere

Sir John predicted that the leading technology companies will increasingly agree to provide the security services with access to their solutions, for two key reasons. 'What the technology companies really don't want is for some clever firm in Israel to break into their encryption system and then sell their solution to the FBI – which is what happened with Apple,' he said.

He also indicated that the likes of Google are softening their previously hard line on privacy and end-to-end encryption, 'because they're keen on getting accepted in China and elsewhere.' Wrapping up the debate, Sir John underlined that the commercial imperative for such companies to grow their businesses means they're now amenable to demands to comply with local laws.



```
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://172.16.224.253:8080/
[*] Server started.
msf exploit(java_rhino) > [*] 172.16.224.252   java_rhino - Sending Applet.jar
172.16.224.252 - - [27/Sep/2017 20:28:49] code 404, message File not found
                                                                         172.16
.224.252 - - [27/Sep/2017 20:28:49] "GET /favicon.ico HTTP/1.1" 404 -
                                                                     [*] Sending
 stage (957487 bytes) to 172.16.224.252
[*] Meterpreter session 1 opened (172.16.224.253:443 -> 172.16.224.252:49221) at
 2017-09-27 20:28:51 +0100

msf exploit(java_rhino) > sessions -l

Active sessions
===============

  Id  Type                     Information                          Connection
  --  ----                     -----------                          ----------
  1   meterpreter x86/windows              Bob @ EXPLOITLAB WIN7
.253:443 -> 172.16.224.252:49221 (172

msf exploit(java_rhino) > 
[0] 0:bash*
```

Law firm leaders given a hacking masterclass

Hacker Freaky Clown shows how easy it is for a novice to circumvent a firm's security system.

This year's European Legal Security Forum (ELSF) saw a welcome return of ethical hacker, Freaky Clown (FC). For his keynote presentation, FC showed just how easy it is for a non-expert computer user to break into someone else's machine - by overseeing a hack live on stage, using a volunteer from the audience and free, readily-available hacking software.

First, FC explained that non-expert hackers can learn how to break into someone else's computer by simply watching a YouTube video and following the hacking software's easy-to-follow, menu-driven, instructions. In his demonstration, 'Alice' – the volunteer ELSF hacker – was able to gain direct access to 'Bob's' computer. Crucially, the hacking software used was able to circumvent both the corporate firewall and antivirus software that was supposed to protect Bob's machine.

> **"A third of people click on links, even if they know it's malicious**

To engineer the security breach all Alice had to do was persuade Bob to connect back with her in some way. As she had discovered that he loved cats, her attack on his computer consisted of sending him an email suggesting that he look at a picture of a cat on the internet. As soon as Bob clicked on the link, Alice was able to take complete control of his computer – without him even being aware of it.

To any member of the ELSF audience who might have argued that 'no one today would click on a link to an unknown source', FC had this simple message: 'People click on links. It will happen. We've discovered that a third of people click on links, even if they know it's malicious, and even if we tell them it's malicious.' Often, they do so because they want to see what happens. But, as was the case with Alice and Bob, nothing appeared to have happened to his computer. In such circumstances, the victim wrongly believes that no hack had taken place.

FC then showed how Alice was able to change crucial bank payment details that were stored in a database that Bob was working on. This meant that when he processed a transaction based on those adulterated payment details, he was facilitating her theft from the company. However, as Alice's hack had penetrated far more deeply into his employer's network than Bob's computer alone, she had, in effect, gained system level privileges. This means she could frame Bob for both the initial hack and the subsequent theft. 'What a great way to get him fired,' FC said.

> **You will be hacked at some point. Recovery time is [even] more important than prevention**

Mitigate against risk

So how should law firms respond to this type of threat? In FC's view, the key to risk minimisation is to focus on the 'absolute basics'; namely, separating networks from each other and routinely patching software. Two stage-authentication can also help protect accounts from being comprised.

However, FC concluded that while education and a 'healthy level of paranoia' can help firms to minimise their risk of being successfully hacked, there is no technological solution that can guard against it entirely. For that reason, he recommended that backups are undertaken regularly – with the appropriate safeguards in place to ensure that those backups have not, themselves, been compromised.

'You will be hacked at some point, so you need to be able to stand up again very quickly,' he said. 'Hence, recovery time is [even] more important than prevention.'

EUROPEAN LEGAL SECURITY FORUM 2017

> An excellent event, in an excellent and central location. Having all notable legal suppliers and speakers under one roof made for a very productive and enlightening day!
>
> Regional Technology Director
> Clifford Chance LLP

Securing your legal practice – one risk at a time

Why the European Legal Security Forum (ELSF) is the place to learn how to protect your firm. Here's a round-up of the best of the crop of exhibitors at this year's show.

Law firms face a bewildering choice of security solutions suppliers, each offering to protect discrete area of their IT security. Many of the leading vendors who specialise in the legal sector exhibited at this year's European Legal Security Forum (ELSF); event attendees experienced an unrivalled one-stop-shop of products and services.

Several vendors, such as Juniper Networks and Darktrace, focused on protecting firms on a practice-wide basis via network monitoring services. By contrast, others, such as e-delivery communications expert RPost, offered niche solutions for individual desktop applications – in this case, email security.

Several exhibitors focused on disaster recovery. However, while Mirus and UDProtect demonstrated data back-up and recovery solutions, Yudu's product is targeted towards personnel. App-based Yudu Sentinel allows organisations to maintain two-way communications with staff, and access key firm documents, even in the event of a crisis or cyber-breach situation.

Secure hardware

In terms of security-focused hardware, Blackberry exhibited its newly-launched Blackberry Motion handset which places a heavy emphasis on user privacy. Staying on the smartphone theme, Wandera revealed its gateway architecture which scans phones for vulnerabilities or unusual behaviour and highlights apps that appear to have improper permissions rights.

Meanwhile, Apricorn showcased a simple, but elegant, method of making memory sticks and portable hard drives more secure. Its products are hardware encrypted and include a built-in lockable pin pad. A similar offering was also demonstrated at the parallel London Law Expo event by iStorage.

With many fee earners now routinely using multiple electronic devices, it's important that firms are able to keep abreast of the hardware that's allowed to access their networks. At the ELSF, Ivanti promoted a solution that does just that – Endpoint Manager. And, for anyone whose IT hardware is reaching the end of its useful life, Blackmore Ricotech was on hand to show its expertise in secure asset disposal, ensuring that firms' redundant IT hardware cannot become the source of a future data breach.