EUROPEAN
LEGALSECURITY
FORUM 2016

CONFERENCE REPORT

12th July 2016

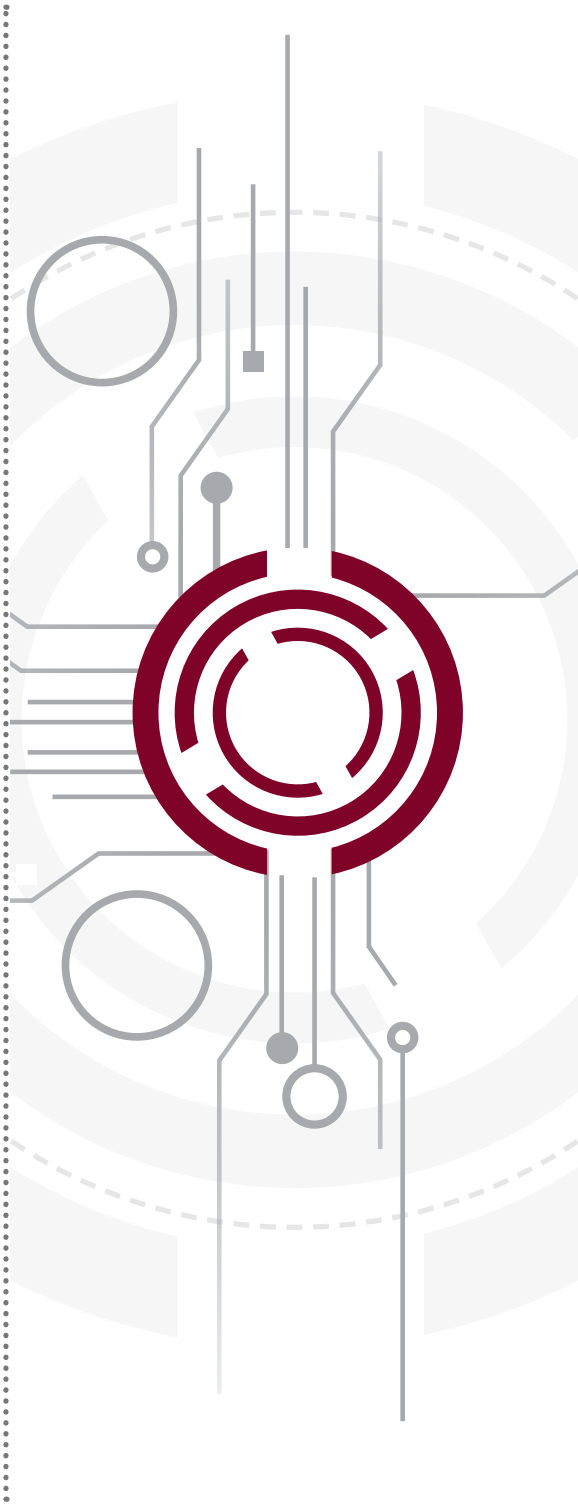
155 Bishopsgate • London

AN EVENT BY
NetLawMedia

Keeping Law Firms Safe

EUROPEAN LEGALSECURITY FORUM 2016

More than 500 senior executives from the world of law and legal technology attended Netlaw Media's inaugural European Legal Security Forum (ELSF), held in London in July. With more than 30 presentations across two stages, and 35 leading security-related suppliers to the legal profession exhibiting at the event, the day was packed full of advice and practical guidance for law firms seeking to minimise their risk of a security breach. Richard Parnham provides an overview of the event's proceedings.



Preparing for a cyber-attack

Law firms are increasingly being targeted by sophisticated cyber criminals. And, while technology can play a vital role in protecting firms from attack, the importance of people and processes should not be underestimated

There is now almost an established tradition at Netlaw Media's IT-focused events: Raj Samani, EMEA chief technology officer for Intel Security, takes to the stage and comprehensively spooks the assembled audience about current cyber-security risks. It was therefore fitting that Samani was one of the first speakers at the inaugural Netlaw Media European Legal Security Forum (ELSF), held in London in July.

On this occasion, Samani provided an update regarding the growing threat from ransomware – specifically, CryptoWall 3. This, he explained, had now generated revenues in excess of US $325 million for cybercriminals, by encrypting users' computer files and forcing them to pay a ransom before access to those files is restored.

Samani attributed the success of CryptoWall 3 to the high quality of its underlying software, coupled with the developers' effective use of established marketing techniques. This has had the twin effect of maximising infections, while also making the ransomware initially difficult to overcome.

"How many of you have a budget that's bigger than the bad guys? If you do, we have sales guys waiting for you!" he quipped.

Another hot topic of discussion at the event was the possibility that firms might suffer from

wholesale theft of their data in a manner similar to that suffered by Panamanian law firm Mossack Fonseca earlier this year. The first keynote presentation of the day, delivered by conference chair and cybersecurity veteran Graham Cluley, provided a detailed account of the security vulnerabilities to which Mossack Fonseca was exposed (cross reference to report, page 6). Perhaps inevitably, his presentation was extremely popular among ELSF attendees, and was a standing room only affair.

Firms fight back

In the discussion that followed Cluley's presentation, law firm representatives outlined the practical steps they've taken to try to ensure they won't ever be hacked like Mossack Fonseca. These steps include carrying out penetration and endpoint testing on the IT side, supplemented by compulsory security refresh training for all firm personnel. But, as Tracy Andrew, information security and compliance officer at Field Fisher Waterhouse acknowledged, until more is known about who was behind the Mossack Fonseca attack, "we've all just got to hope that what we've got is good enough."

In a similar vein, Jon Segger, global information security manager at Linklaters, pointed out that when news of the attack first broke, details were "sketchy", making it difficult to react from an IT security perspective. He finds the possibility that Mossack Fonseca might have been an "inside job"particular challenging because, by their very nature, the way in which most law firms operate depends on many people having access to sensitive information.

Returning to this point later in the day, Angela Robertson, director of risk and general counsel at Taylor Wessing, acknowledged that one option open to firms might be to "lock down" access to data to minimise the risk of a large-scale data theft. However, the problem with this approach, she added, is that "it goes against the whole concept of knowledge and information sharing, and collaboration."

Another security challenge identified by various conference speakers was the issue of spoofing –where a hacker pretends to be someone else. In a lively and informative presentation, Channel 4 News technology journalist Geoff White provided a detailed account of how the much-publicised, large-scale hack of TalkTalk customer data had occurred in 2015. This attack, he explained, had involved the use of spoof emails, malware and "Oscar-winning" phone calls by the hackers themselves, pretending to be calling on behalf of the company.

However, in a clear indication that the TalkTalk experience was not simply confined to consumer-facing companies, many of the ELSF attendees admitted, via a show of hands, that their own firms had been targeted in a similar manner. One speaker noted that the particular challenge of spoofing for law firms is the hierarchical nature of most legal practices, making it hard for junior employees to query instructions purportedly given by more senior personnel. The key message for this part of the debate was: please follow existing rules and procedures – the boss shouldn't mind if you do.

Of course, in many situations, technology could be deployed to stop spoofing attacks from taking place. Several exhibitors at ELSF offered solutions which do just that. However, speakers at various panel discussions also reiterated the importance of people and processes in minimising firms' risk exposure with regards to this issue.

For example, Thereza Snyman, head of IT at Kingsley Napley, recalled how one of her firm's clients had suffered from a form of a "whaling attack" – a type of spoofing attack in which a user's genuine email account is hijacked. Having received faked client instructions to transfer funds to a new account via this hacked email, the firm adopted "the human equivalent of the two-factor authentication" to verify the suspicious

14+

Netlaw Media's 14th sold out Law Event in succession

instruction. In short, the client was telephoned to enquire whether the request was genuine. Similarly, David Aird, IT director of DAC Beachcroft spoke of the significance of training personnel to be wary of "Friday afternoon 4 o'clock emails" specifically designed to put personnel under pressure. "Trust your spidey sense," he said, suggesting that law firm personnel should ask themselves if what they're being asked to do "feels right".

This prompted panel chair Graham Cluley to observe that, "It's almost as though we need to train our staff to be a little bit less helpful, a little bit less friendly. Maybe that will help save your company's bacon."

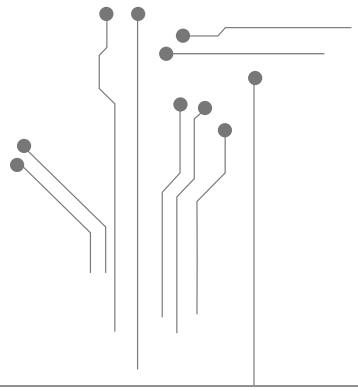
In terms of specific law firm security improvement initiatives, various case histories were offered by law firm IT security heads. David Robinson, global head of IT Security at Herbert Smith Freehills explained how his firm had recently achieved ISO/IEC 27001 information security management certification after a six-month programme of review and investment. As part of this process, he said, the firm's security team had grown from two to six – with a strong focus on hiring IT security staff who were proactive rather than reactive, and who also fitted in well with the Herbert Smith Freehills culture.

At the heart of the firm's security accreditation process was its constantly-evolving roadmap for action, Robinson said. The roadmap itself is fairly straightforward and is broken into five simple layers: endpoint, server, network, internet and outsourced services. "Each defines what's there, to be delivered, what we're doing this year and what we'd like to do."

The firm's security team is also proactive in obtaining feedback on the roadmap, he said – not just from board members, but also from business service leaders, department heads, other fee earners and vendors. And, once the roadmap was defined and its budget approved, Robinson then made use of the firm's marketing and communications team to inform the practice of what was being done.

In another presentation, Ian Lauwerys, head of security and business systems at Clyde & Co, observed that the law firm security function shouldn't act as a hindrance to implementing the practice's wider strategy – even if the strategy itself results in security challenges. Here, he identified rapid geographical growth as a major security challenge affecting his firm in particular. Helpfully, he explained, the firm now has procedures in place to make this process as smooth as possible, while also ensuring the global practice isn't exposed to unnecessary risks during the integration process. Onboarding firms are subject to an initial security audit, which provides the basis of a checklist for compliance improvement. The process of operational and cultural integration should, realistically, take 12-18 months to complete, he said.

The particular challenge of spoofing for law firms is their hierarchical nature, making it hard for junior employees to query purported instructions



Lauwerys also emphasised that Clyde & Co's security-focused clients are useful allies in building a wider cultural of security within the firm. "Clients drive our security strategy, where we invest, and what our policies should be," he said. The reason why this approach works well is simply because partners care about what clients want.

That said, Lauwerys also acknowledged that some clients came to the firm with unrealistic expectations regarding what data-protection processes the firm should put in place. Asking employees to check their phone in at the door might work for call centre personnel, by way of example, but law firm partners would never agree to such a restriction.

Overcoming unrealistic client expectations, Lauwerys said, requires a long-term process of relationship-building and reassurance, in order to convince clients that the firm's security policies are credible and capable of delivering what they expect.

Spread the word

In light of the wide-ranging and widespread security challenges facing the legal sector, several speakers called for improved knowledge-sharing and professional development. This, it was said, would help guard against common threats, while developing commonly-agreed best practices.

For example, Crest president Ian Glover called for lawyers to establish an information exchange, in order establish what an instant response should be, in a profession-specific context. Later, when discussing how firms should learn lessons from a security attack, he encouraged practices to share their own experiences as broadly as possible to help others. This makes sense as cyber criminals tend to knock on "every door in the industry" to maximize the effectiveness of a cyber-attack, he said.

Continuing this information sharing and relationship-building theme – albeit in a more lighthearted manner – Graham Cluley suggested that it's important for conference delegates to get to know each other, because "you're in the same boat, you're fighting on the same side." He then suggested an excellent way for this relationship building process to begin: over drinks at the end of the European Legal Security Forum itself.

Keynote reports

A summary of the expert keynote speeches given by conference chair Graham Cluley and cybercrime analyst Edward Lucas

Graham Cluley, Conference Chair

Cluley sheds light on Mossack Fonseca security failures

Kicking off the first of the European Legal Security Forum's (ELSF) two keynote presentations, conference chair Graham Cluley offered a detailed critique of the recent IT vulnerabilities of Mossack Fonseca, the Panamanian law firm at the centre of one of the world's largest data security breaches earlier this year.

In essence, he said, the firm's website had acted as an advertisement to the entire world, with the unfortunate message: "Hack me."

Out of date slider

The first data security vulnerability identified by Cluley was also the most obvious element of the Mossack Fonseca's website – its "revolution slider" plugin. This popular plugin allowed the firm to display its practice areas on rotation, without the need to clutter up the website with too much text.

Unfortunately, the version of the slider used by the firm at the time of its data breach was "ancient". The website's – now blocked – change log revealed that the firm was using slider version 2.1.7. However, as far back as November 2014, it had been revealed that all versions of the slider prior to version 3.9 suffered from a vulnerability, which allowed hackers to gain remote access to users' websites.

Explaining how it might have come about that the slider hadn't been updated, Cluley pointed out that it could have been acquired in only one of two ways. The first option, he said, was to buy the slider directly from the developers. The other option involved buying it as part of a WordPress website template theme.

"The problem is that, if you don't buy it [the slider] directly from the developers – if you buy it bundled with a WordPress theme instead – then you might not receive an update to the code," he said, adding that it was possible to create a direct relationship with the slider developer for around US$7, which would afford the user regular software updates and security alerts.

"And boy-oh-boy, Mossack Fonseca really needed an update," he said.

Edward Lucas, Keynote Speaker

Server fails

Further to this, Mossack Fonseca had compounded this software updating failure by using the same server to host both the firm's website and emails. It was therefore fairly easy, he explained, for a hacker to "hop across and compromise the email system as well."

Even more problematically, the firm's email server was also several years out of date. "If you went to the Mossack Fonseca website, and looked at the remote email login page, you'd have discovered that they were running a version of Microsoft Exchange from 2009 – which, again, hadn't been updated."

As a result of these security shortcomings, around 4.8 million Mossack Fonseca emails were stolen, including those sent by – and received from – its clients. Hacking the firm's email server accounted for a significant percentage of its overall data breach, Cluley recalled. But, worse was to still come.

Warnings ignored

As he put it, "Anyone with the smallest technical bent" could go onto Mossack Fonseca's website and find that the content management system which underlay its client portal was based on an old version of Drupal – version 7.2.3.

"This particular version of Drupal had at least 25 vulnerabilities, which hackers could exploit to gain access to servers and steal information. And remember, this isn't about email – we've already done that. This is now about databases instead. The information that Mossack Fonseca had been collecting since the 1970s. Really valuable data."

Your customers are worried. They're starting to conduct their own assessments, because they want to feel confident that you're not going to be the next Mossack Fonseca

Mossack Fonseca's failure to update its version of Drupal was all the more remarkable, Cluley told the assembled audience, because Drupal had issued a "highly critical public service announcement" – dubbed Drupalgeddon – several months before the data breach took place. This announcement had explicitly stated that, "Attackers may have copied all data on your site and could use it maliciously".

Cluley commented, "The announcement was along the lines of, 'Oh my god, we're on fire. We have a huge problem' – and yet Mossack Fonseca did nothing."

Whether that amounted to a failure by the firm itself, or by an outsourcing partner, Cluley said he didn't know – not that it mattered either way. What was important, he said, was that the damage had been done, and that it was now possible to go online and download every electronic file, image and email produced by Mossack Fonseca prior to the data breach. "Imagine if that happened to your company," he said.

Protect the customer

Fundamentally, Mossack Fonseca's failure to update its software was not usual. But, Cluley suggested, if the firm had done so, it was quite possible that it would never have been hacked. He therefore recommended to the audience members that they check whether the software used to manage their own websites – and also any third party code their website relies on – is up to date.

There is, Cluley concluded, one final reason why law firms should carry out such an assessment. "Your customers are worried – and you don't want worried customers. They're starting to conduct their own assessments, because they want to feel confident that you're not going to be the next Mossack Fonseca," he said, bringing his speech to an end.

No magic bullet to improve cyber security, says Lucas

The internet will only become more secure if there's a holistic approach to improving it, in a manner reminiscent of attempts to improve road safety in the past, Edward Lucas told the ELSF audience in the final keynote presentation of the day. Lucas is the author of a new book on internet security, *Cyberphobia*, and also a senior fellow at the Center for European Policy Analysis in Washington DC.

Previously, he explained, the motor car killed around 6,500 people each year in the UK, because it hadn't been designed with road safety in mind. But, by undertaking a host of activities, including cracking down on drink driving, addressing car safety and accident blackspots, penalising bad drivers through their car insurance premiums, as well as huge public information programmes, the UK death toll caused by road accidents had now fallen dramatically, to under 2,000 per year.

Improving internet security requires a similar approach, Lucas said. "We also need to end criminals' culture of impunity. We need to ensure they make less and less money and are exposed to more and more risk."

Reverse priorities

Lucas highlighted various problems with the existing internet infrastructure, starting with the very basic proposition that the internet was "never designed to be the central nervous system of modern life." Over the years, convenience, adaptability and low cost have been prioritised over security, which has resulted in a scenario where "the hardware is rubbish, the software is rubbish and the network design is rubbish."

At the same time, the criminal fraternity has invested heavily in R&D, to make their offering ever more sophisticated and effective. "We're driving in first gear in a Lada while they're roaring ahead in a turbo-charged Bentley – paid for with our money," he added. "I don't see any sign of that gap changing any time soon," he said.

The ID challenge

According to Lucas, whole network infrastructure is one problem area which will have to be addressed before internet security can be improved; another issue is our collective willingness not to question the identities of possible fraudsters who contact us online. Here, he cited the example of a spoof email he sent to six senior individuals as part of his research for his book, purporting to be from the Russian Embassy in London. It was quite obvious that the email was fake because it came from a Gmail account. However, each of the recipients, including the ambassador of a NATO country, fell for the scam.

"I was expecting them to say, 'Ha ha, very funny' but they didn't. That's bad. I was quite upset by that," he said.

Lucas went on to explain how easy it would be to trick ELSF audience members into opening an email attachment infected with malware, and then escape undetected. All he had to do was create a false email account in the name of fellow conference speaker Graham Cluley, saying, "Nice to see you at the conference. Here are the slides for my presentation."

> **We need to end criminals' culture of impunity, to ensure they make less and less money and are exposed to more and more risk**

A new outlook

He said that overcoming the ID challenge will require a change in mindset, for people to assume that they're constantly under threat. Lucas spoke favourably of the regime in Estonia, which has, for several years, provided citizens with a government-backed, public key cryptography-based ID card. Using this card and an encryption-based system, he said, means that Estonian citizens can only send an email that comes from themselves, or send a document that only they can sign, and which only certain recipients can read. "That's a really powerful platform of trust for the [digital] interactions which are the basis of our civilisation" he said.

Although the speaker expressed a hope that improvements in information security and identity verification will improve over time, he also shared his fear that "It's going to get a lot worse before it gets better."

Concluding his presentation – and also the proceedings of the European Legal Security Forum itself – Lucas expressed a fear that the Mossack Fonseca scandal could well end up as no more than a "footnote for what we're facing, which is a full-scale attack on the corpus of our economy and our civilisation."

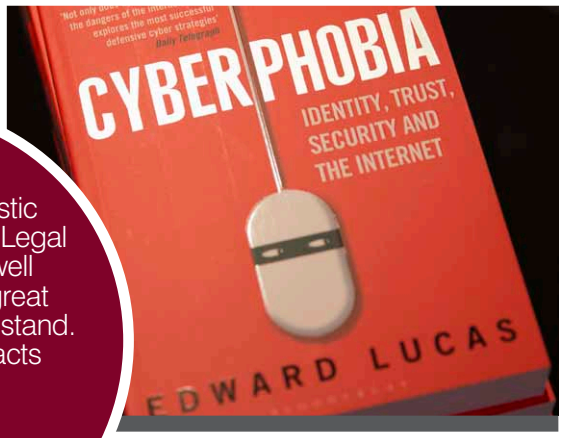
The European Security Forum is an excellent event at a top and centrally located venue.

Partner, Stone King LLP

EUROPEAN LEGALSECURITY FORUM 2016

One of the most informative seminars I have been to in a long while. As a new comer to the legal IT world I was able to learn an awful lot.

IT Manager, Wansbroughs



> Thank you for a fantastic event. The European Legal Security Forum was well run which made it a great experience to have a stand. We made good contacts and had some great conversations.
>
> Business Development Manager, Risk-X

Evaluate, avoid, detect, restore

Vendors explain how they can protect law firms

Many of the discussions at the European Legal Security Forum (ELSF) were devoted to identifying the key security risks now facing law firms. But, while several of these presentations were somewhat downbeat in terms of the breadth of the security challenges facing the legal sector, the perspective of vendors attending the event was noticeably more positive. Challenge by challenge, threat by threat, vendors and security consultants were on hand to offer software- and process-based solutions intended to help law firms mitigate their security risk exposure.

For example, in order help firms avoid a Mossack Fonseca-style attack, David Ford and Adrian Stanley from BlackBerry were promoting their recently-launched professional cybersecurity evaluation service, BlackBerry Encryption. The new offering, which forms part of BlackBerry's wider drive into enterprise security, follows the company's acquisition of UK-based encryption consultancy service earlier this year.

Another company promoting its push into security-based solutions was Mimecast, hitherto best known for its cloud-based email management service. Its suite of email-based security services were actively demonstrated at the ELSF event, including Attachment Protect, designed to combat zero-hour attachment threats; URL Protect, which guards against spear-phishing and targeted attacks; and Impersonation Protect, which aims to defend against whaling attacks.

Several of the ELSF exhibitors, including Darktrace and eSentire, demonstrated their respective threat detection response offerings, based around machine-learning. In essence, both of their solutions monitor organisations' entire networks in real time for any signs of unusual behaviour, which were not predefined. Once a threat is detected, problematic users and devices can be immediately locked down, in order to prevent possible infections from spreading.

Elsewhere in the conference hall, another vendor planning to move into the threat detection space is iManage, currently best known in the legal IT community for its popular document management system (DMS). The company's rationale for this service line extension is that as many firms have used

iManage's DMS for many years, it is now well-placed to use artificial intelligence to spot subtle deviations in normal user behaviour.

Where security breaches do occur, tracking down the location of the breach quickly is essential – which is no mean feat, especially for multi-site, multi-time-zone law firms. The presentation by LogRhythm regional sales manager Mark Baker reminded the audience of the importance of robust and standardised log management, when seeking evidence that could help identify the time and locations of such breaches.

At a more advanced level, Barker also explained how his company is now offering multi-source "instant analytics" of people and processes, which can be used to establish when suspicious activities might be occurring. Here, he gave the example of comparing door access logs with remote access account logins to help determine whether it was physically possible for a user to be in both locations within a specified time period.

Finally, for any law firm that has suffered a security breach, it's vital to restore the practice's IT systems as quickly as possible – without risking a reinfection of the entire network. In this space, James Holt, service delivery manager at Databarracks, explained the usefulness of his company's recently-launched Cyber Disaster Recovery as a Service (Cyber DRaaS) offering. This involves intensively scanning backup data for signs of infection, and then identifying the most recent backup point where no infection is present.

"If you find you need to invoke your disaster recovery plan, you need to know exactly which point you should recover back to," Holt told the ELSF audience. "Our solution takes the guesswork out of that process."

Darktrace and eSentire's threat detection response solutions monitor entire networks in real time for signs of unusual behaviour

An event by NetLawMedia