

Post event report



Strategic Sponsors



Education Seminar Sponsors

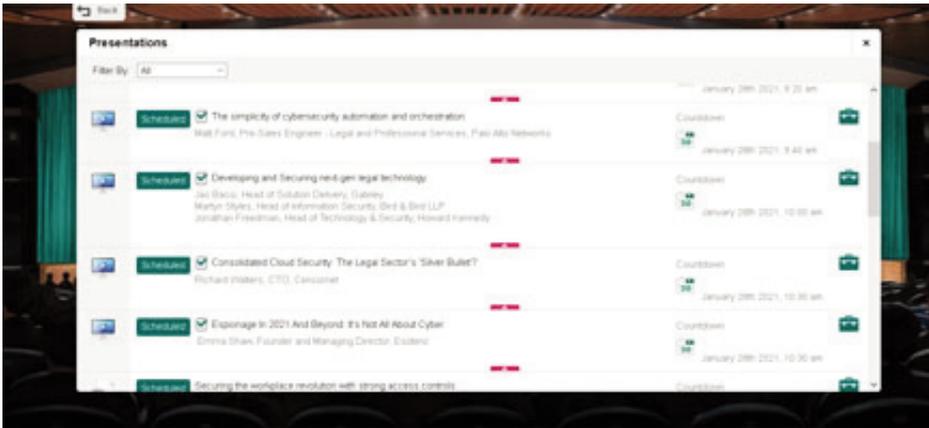


“Thanks for another excellent StLF session; I am glad it was able to go ahead online. Fingers crossed we can all get together properly for a September session.”

Cyber Security Specialist, Addleshar Goddard LLP

Inside this report:

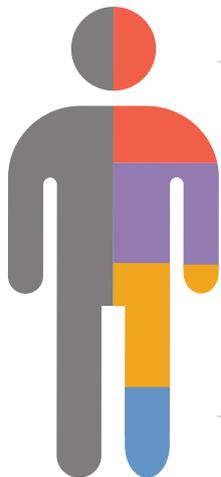
- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



Key themes

- Securing the workplace revolution
- Strengthening identity and access management
- What to do about ransomware?
- Sorting out GDPR compliance
- Improving visibility
- Cybersecurity for business resilience
- Application security
- Building in security: easier said than done?

Who attended?



- Cyber-security**
 We have a 15-year track record of producing the events cyber-security professionals take seriously
- Risk Management**
 We attract senior risk officers with responsibility for information risk assessment and mitigation
- Fraud, Audit, Compliance**
 We provide the go-to events for fraud prevention and compliance owners at the world's key corporates
- Data Protection & privacy**
 We are a key venue for decision-makers with budget and purchasing authority

Speakers

- Burak Agca, Mobile Security Advisor UK/I
Lookout UK
- Jas Bassi, Head of Solution Delivery
Gateley
- David Bish, Head of Research and Analysis
Solicitors Regulation Authority
- Simon Brady, Managing Editor
AKJ Associates
- Steve Byrne, Information Security Officer
DWF
- Razvan Cretu, Director of IT
CMS
- Bobbie Darrock, Information Security Specialist
Egress Software Technologies
- Nour Fateen, Pre-sales Consultant
Recorded Future
- Max Faun, EMEA Head of Business Consulting
Okta
- Matt Ford, Pre-Sales Engineer – Legal and Professional Services
Palo Alto Networks
- Jonathan Freedman, Head of Technology & Security
Howard Kennedy
- Karl Knowles, Global Head of Cyber & Service Delivery
HFW
- Mariana Pereira, Director of Email Security Products
Darktrace
- Joshua Pool, Detective Sergeant
Metropolitan Police Cyber Crime Unit
- Emma Shaw, Founder and Managing Director
Esoteric
- Martyn Styles, Head of Information Security
Bird & Bird LLP
- Zeki Turedi, CTO, Europe, Middle East and Africa
CrowdStrike
- Richard Walters, CTO
Censornet

Agenda			
08:00	Login and networking		
08:55	Chairman's welcome		
09:00	Legal cyber-risks: Regulatory observations and guidance David Bish , Head of Research and Analysis, Solicitors Regulation Authority <ul style="list-style-type: none"> • Overview of the current cybercrime landscape: what changed in 2020? • Current trends – what are we seeing as the regulator, and what are the impacts on firms? • Ongoing COVID-19 and remote working security considerations: practical advice for 2021 • Regulatory obligations and resources: SRA guidance and enforcement strategy 		
09:20	Security is important, and it can be done without compromising usability Max Faun , EMEA Head of Business Consulting, Okta <ul style="list-style-type: none"> • Mobile and cloud proliferation along with the shift to working from home has exposed law organisations to much higher risks for potential hacks and attacks • The traditional perimeter is crumbling under the weight of these threats, making it imperative to re-examine traditional security approaches • Identity & access management must now take centre stage to defend against identity-based security breaches, using modern approaches to do this whilst dramatically improving user experience. 		
09:40	The simplicity of cybersecurity automation and orchestration Matt Ford , Pre-Sales Engineer – Legal and Professional Services, Palo Alto Networks Join Matt Ford, who'll share insights from his experience providing cybersecurity advice to the legal industry and also as an Ethical Hacker, to help you: <ul style="list-style-type: none"> • Understand how to simply and quickly automate and orchestrate • Learn from the use cases he shows • Understand the unique benefits to the legal industry 		
10:00	EXECUTIVE PANEL DISCUSSION Developing and securing next-gen legal technology Law firms are adopting technologies such as automated contract review, AI and chatbots which are significantly altering the services provided by firms, helping to automate routine tasks and provide next-gen client services. But cybersecurity and data protection need to be carefully considered when developing online legal services. So how are law firms transforming their services, securely? Jas Bassi , Head of Solution Delivery, Gateley Martyn Styles , Head of Information Security, Bird & Bird LLP Jonathan Freedman , Head of Technology & Security, Howard Kennedy		
10:30	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Censornet Consolidated cloud security: The legal sector's 'silver bullet'? Richard Walters, CTO, Censornet </td> <td style="width: 50%; padding: 5px;"> Esoteric Espionage in 2021 and beyond: It's not all about cyber Emma Shaw, Founder and Managing Director, Esoteric </td> </tr> </table>	Censornet Consolidated cloud security: The legal sector's 'silver bullet'? Richard Walters , CTO, Censornet	Esoteric Espionage in 2021 and beyond: It's not all about cyber Emma Shaw , Founder and Managing Director, Esoteric
Censornet Consolidated cloud security: The legal sector's 'silver bullet'? Richard Walters , CTO, Censornet	Esoteric Espionage in 2021 and beyond: It's not all about cyber Emma Shaw , Founder and Managing Director, Esoteric		
11:00	Networking break		
11:30	Is perimeter defence sufficient to protect the 'crown jewels'?! Implementing strong access controls to secure the workplace revolution Razvan Cretu , Director of IT, CMS <ul style="list-style-type: none"> • Today's distributed business models necessitate the refocus of security towards the user's identity, what does this mean for your current security controls? • What do law firms need to consider when implementing access controls on their services? • Should we embrace the 'assume breach' strategy? Prevention is still important, but in this environment should the emphasis shift to reactive security? 		
11:50	Adversary infrastructure in 2020: A defender's view Nour Fateen , Pre-sales Consultant, Recorded Future <ul style="list-style-type: none"> • Adversary infrastructure has evolved throughout 2020, including the creation and modification of new malicious infrastructure for a multitude of post-exploitation toolkits, custom malware frameworks, and open-source remote access trojans • 2021 outlook, examining the tools that espionage-oriented actors are using to achieve their goals and the further adoption of open-source tools • How to implement security controls and mitigations against these malware families, and how to adopt defence-in-depth approaches to detect intrusion activity on the victim host, at the perimeter, and on the wire 		
12:10	Oh no, not another ransomware presentation Zeki Turedi , CTO, Europe, Middle East and Africa, CrowdStrike <ul style="list-style-type: none"> • A discovery of the key trends observed within the attacks of today and dissection of key examples • Why ransomware that leverages the fear of uncertainty around the pandemic is on the rise and what can be done to combat it • Recommendations on how legal firms can best protect their organisations data and network across both corporate supplied and employee-owned devices, regardless of where they are located 		

Agenda

12:30	Securing the new normal: Cyber AI for the inbox Mariana Pereira , Director of Email Security Products, Darktrace <ul style="list-style-type: none"> • Today, 94% of cyber-threats still originate in the inbox • ‘Impersonation attacks’ are on the rise, as artificial intelligence is increasingly being used to automatically generate spear-phishing emails, or ‘digital fakes’, that expertly mimic the writing style of trusted contacts and colleagues • Humans can no longer distinguish real from fake on their own – businesses are increasingly turning to AI to distinguish friend from foe and fight back with autonomous response • In an era when thousands of documents can be encrypted in minutes, ‘immune system’ technology takes action in seconds – stopping cyber-threats before damage is done.
12:50	Lunch and networking break
13:50	Current cyber-threats to the UK legal sector and how to keep yourself safe Joshua Pool , Detective Sergeant, Metropolitan Police Cyber Crime Unit <ul style="list-style-type: none"> • In the first half of 2020, law firms reported losses of nearly £2.5 million of client funds – find out the common attack vectors and areas of most risk from cybercriminals • How should law firms respond and what steps can be taken to mitigate these risks? Are offline backups and access management enough? • Law enforcement and industry collaboration following a breach is encouraged but unfortunately, not always the chosen path. What are the other ways in which we can work together to reduce organisational risk and potential for reputational damage?
14:10	Responding to client pressure for improved email security, without impacting productivity Bobbie Darrock , Information Security Specialist, Egress Software Technologies <ul style="list-style-type: none"> • Understand why legacy DLP technologies have failed to mitigate risk and keep data secure • See how law firms can dynamically quantify and mitigate breaches through intelligent technology • Understand the value this brings to client relationships and firm-wide working practices
14:30	How mobile devices are leaving the door open to legal cyber-risks Burak Agca , Mobile Security Advisor UK/I, Lookout UK Mobile devices are at the intersection of work and personal life. Now more than ever employees are using these devices to access business apps and corporate data. <ul style="list-style-type: none"> • Where the mobile risk resides – overview of the latest cyber-threats • How cyber-threats are affecting the legal sector • How can cybercriminals compromise corporate cloud data • How to secure any mobile device with access to corporate cloud data and protect all employees, no matter where they work from.
14:50	Communicating cyber: Senior management engagement in the new reality When law firms make the cybersecurity headlines it’s generally a high-profile third-party issue. When such incidents make headlines, panicked board members have one question for information security leaders; “How can we be sure this will not happen to us?” So, how can information security leaders effectively communicate cybersecurity strategies across their firm and get the board on side to foster a cyber-secure culture from the top-down? Fireside chat with: Karl Knowles , Global Head of Cyber & Service Delivery, HFW
15:10	Networking break
15:40	Third-party management: The risk-based approach Third-party breaches underscore the potential risks involved in firms outsourcing services and how such firms can be exposed not only by their own internal systems but by the vulnerabilities of their third-party service providers. Despite this, many firms struggle to assess their level of exposure to third-party risks and the impact a third-party issue could have on brand, reputation, and operations. When their security is just as integral as your own, what are the risk-based approaches to managing your third parties? Fireside chat with: Steve Byrne , Information Security Officer, DWF
16:00	Another year of living dangerously? Simon Brady , Managing Editor, AKJ Associates <ul style="list-style-type: none"> • How secure are your security providers and how would you know? • As key third-party suppliers, how can you convince your clients you are secure? • Remote working is insecure – but just how insecure? • Three key tasks for 2021
16:30	Networking
17:00	Conference close

Education Seminars	
<p>Censornet</p> <p>Consolidated cloud security: The legal sector’s ‘silver bullet’?</p> <p>Richard Walters, CTO, Censornet</p>	<p>As we enter a new age of the workplace where ‘anywhere work’ is a necessity, the major shift in work location and jump to adopt new tools has highlighted the risks associated with the cloud and meant that many law firms have, or need to, radically re-evaluate their cybersecurity posture.</p> <p>In this session we will explore:</p> <ul style="list-style-type: none"> • The drivers of change and implications for cybersecurity in a remote landscape • Securing data as your Lawtech moves to the cloud – must watch for iManage users • Why now is the time to take a holistic view of cybersecurity – including findings from Censornet’s mid-lockdown survey of 300 cybersecurity professionals • Real examples of legal sector security challenges solved • How to quickly and easily achieve robust seamless protection and efficiencies across core security products
<p>Esoteric</p> <p>Espionage in 2021 and beyond: It’s not all about cyber</p> <p>Emma Shaw, Founder and Managing Director, Esoteric</p>	<p>Espionage in the legal sector is a threat which can have devastating effects on not only an organisation’s performance, reputation and finances, but also on the privacy of its own clients. While cybersecurity is front of mind for most, adversaries are using traditional techniques to facilitate both cyber and other technical eavesdropping attacks. Shifts in ways of working post-Covid-19 are only exacerbating this risk.</p> <ul style="list-style-type: none"> • Espionage in the legal sector: Is it really still a threat? • Trends in espionage driving the need for a strategic shift • Layers and crossover: Considerations for effective cyber/physical/technical/insider threat mitigation • Ways that technology can help in 2021 and beyond