Post event report

SECURING THE LAW FIRM

8th Securing the Law Firm

21st September 2017 | London, UK

Strategic Sponsors

cipher

commissum INFORMATION ASSURANCE

DARKTRACE

FORTINET

PHISHME

ONDMARC

SECUREDATA TRUSTED CYBERSECURITY EXPERTS

wandera

ZoneFox

Education Seminar Sponsors

BITSIGHT The Standard in SECURITY RATINGS

esentire

foreseeti

KASPERSKY lab SAVING THE WORLD FOR 20 YEARS

LGC

paloalto NETWORKS

SecureLink

Networking Sponsors

ACUITY RISK MANAGEMENT

IRM INFORMATION RISK MANAGEMENT

SureCloud Always Be Certain

> “I felt it was a good day overall; informative and a great opportunity to meet and hear the opinions of fellow information security conscious professionals within the legal profession. The regimented 20 minutes slots for the main presentations were timely but, informative and apart from it being a tad warm in the main meeting room – it was a good day overall. The food and refreshments were also of a good standard. I would definitely go again!”
>
> **IT Security Architect, Farrer & Co**

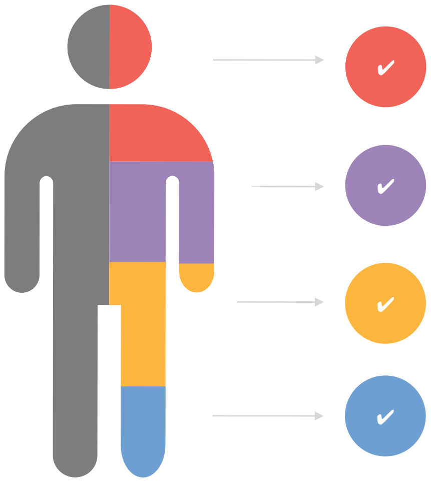
> “This event was of great interest, specifically as it enabled security professionals to consider the current challenges in the cyber space from the perspective of a specific industry sector, and vice versa. As opposed to the more insular view of a purely infosec event. A very worthwhile day. Particularly enjoyed the real-life ‘demos’ and scenarios that were presented.”
>
> **Senior Information Security Manager, Asda**

Inside this report:

Key themes

- Securing your digital transformation
- Lessons from the latest attacks
- Countering the latest threats
- Risk assessment and risk management
- Engaging employees
- Dealing with the problems

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

Sam Alderman-Miller,
Senior Account Manager
Darktrace

Tim Collinson,
Information Security Manager
Bird & Bird

Stuart Dixon, Casework Lead for the
Digital Investigation Unit,
Computer Investigation
LGC

Malcolm Dowden, Legal Director
Bond Dickinson

Philip East, UK Sales Director
BitSight Technologies

Chris Few, UK Business Manager
foreseeti

Etienne Greeff, CTO and Founder
SecureData

Frank Oliver Green, Head of Marketing
Commissum

Mary Kusalic-Murphy,
Global Data Privacy Officer
Latham & Watkins

Matt Little, CTO
ZoneFox

David Mount, Cyber Security Expert
PhishMe

Joe Nelson,
Principal Solutions Architect,
eSentire

Justine Sacarello,
Head of Legal Change & Delivery
Lloyds Banking Group

John Scott,
Head of Information Security Education
Bank of England

Senior Representative from the NCSC

Ade Taylor, CTO
SecureLink UK

Rois Ni Thuama, Head of Cyber
Governance & Legal Partnerships
OnDMARC

Povel Torudd,
Head of Corporate Communications,
CSO Department
Kaspersky Lab

Rick Wilkinson, Managing Director
CIPHER Security Ltd

Joel Windels, VP of Marketing
Wandera

David Wood,
IT Security and Governance Manager
Dentons

Agenda

08:00	Registration
08:50	Conference welcome
09:00	**Insights from the NCSC** Senior Representative from the NCSC AKJ Associates are delighted to welcome a senior representative from the NCSC to share relevant perspectives
09:20	**Mo' mobiles, mo' problems?** **Joel Windels,** VP of Marketing, Wandera • The more mobiles we come across, the more problems we see • Mobile is increasingly important to the law firm – but how can devices be managed and controlled? • Explore the best approaches to identifying and blocking cyber threats on mobile • Get to grips with data-level attacks and how to keep your fleet secure • Understand how to set – and enforce – acceptable usage policies that ensure compliance, manage data consumption and reduce risk
09:40	**The 2017 phishing threat landscape** **David Mount,** Cyber Security Expert, PhishMe • High-profile leaks and mature malware tools in phishing emails and how this has led to the resurgence and emergence of ransomware and botnet malware • What is meant by the 'phishing threat landscape', how attackers have evolved this and the risks that poses to the enterprise • What your enterprise can do in the face of all this, and goals for a holistic, comprehensive and agile defence
10:00	**Clients, robots and legal practitioners: Who's the biggest security threat and what to do about it?** **Malcolm Dowden,** Legal Director, Bond Dickinson • How do CISOs and Legal Directors see the threat posed by data insecurity? • How do emerging automation technologies (AI, robotic process automation and so on) interact with cybersecurity? • How the culture and structure of law firms impact on the ways in which data security is compromised and implemented • Collaborative working: The risks and the competitive advantages. Securing third-party suppliers
10:20	**Education Seminar | Session 1** eSentire **Build, buy or both: Which approach is right for you?** **Joe Nelson,** Principal Solutions Architect, eSentire foreseeti **Driving continuous security improvement with computer aided threat analysis** **Chris Few,** UK Business Manager, foreseeti
11:00	Networking break and refreshments
11:30	**Mind the gap: A tale of transition from client attorney to privacy professional** **Mary Kusalic-Murphy,** Global Data Privacy Officer at Latham & Watkins • Case study covering transition from a client facing lawyer to Latham & Watkins' first Global Data Privacy Officer • Aligning issues of data protection, cybersecurity and information security with the business efficiency priorities of the firm and its partners • Bridging the communication disconnect between legal practitioner and information security professional
11:50	**Would you bet your reputation on a single email? Solving the problem of email impersonation** **Rois Ni Thuama,** Head of Cyber Governance & Legal Partnerships, OnDMARC • Current ways of reporting cybercrime hide the true scale of threats law firms face • The consequences of the attacks firms may not even realise are happening • Take your first steps towards stopping email impersonation today • What to look for when architecting your email security solution
12:10	**Real eyes realise real lies. Why SIEMs need SOCs** **Frank Oliver Green,** Head of Marketing, Commissum • Reframe the problem with SIEMs that lie and change the current model • SOC- and SIEM-as-a-service – a match made in heaven • Detection and response that work together to arm you with real insights to protect your firm and client data

Agenda

12:30 **The Enterprise Immune System: Using machine learning for next-generation cyber defence**

Sam Alderman-Miller, Senior Account Manager, Darktrace

- How new machine learning and mathematics are automating advanced cyber defence
- Why 100% network visibility allows you to detect threats as they happen, or before they happen
- How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by 'immune system' technology

12:50 **Education Seminar | Session 2**

Kaspersky Lab

Advanced/unknown cyber attacks – a new crisis communications challenge

Povel Torudd, Head of Corporate Communications, CSO Department, Kaspersky Lab

LGC

What should you do if you suspect you have been the victim of a cyber incident – cyber incident response

Stuart Dixon, Casework Lead for the Digital Investigation Unit, Computer Investigation, LGC

13:30 Lunch and networking

14:30 **EXECUTIVE PANEL DISCUSSION** **Cross examining cyber: A dialogue on effective cyber strategy**

David Wood, IT Security and Governance Manager, Dentons

Tim Collinson, Information Security Manager, Bird & Bird

14:50 **What AI found at the lawyers – you won't believe number 11!**

Matt Little, CTO, ZoneFox

- Learn about the cybersecurity oddities that we have helped legal firms uncover within their environment
- Our machine learning engine helps uncover unusual user behaviours – and some of the things that we found certainly fall under the category of 'very unusual'
- The human element remains indispensable in the threat hunting process – join us and discover why

15:10 **Staying ahead of the bad guys: Working cybersecurity into your business infrastructure**

Rick Wilkinson, Managing Director, CIPHER Security Ltd

- Recruit and retain: How to stay ahead of the 'bad guys' in an environment where only the few have the option to recruit and retain the required level of cyber expertise
- How to implement effective security infrastructure with the business resources available
- How technology can be used along human expertise to automate the process of early breach detection and response

15:30 **Education Seminar | Session 3**

BitSight Technologies

How to manage cyber risk on a daily basis for your company and the affiliates, your suppliers and peers

Philip East, UK Sales Director, BitSight Technologies

SecureLink UK

A rational look at threat management – L33tsp34k as a second language

Ade Taylor, CTO, SecureLink UK

16:10 Networking break and refreshments

16:30 **Legal and regulatory change and what you need to know**

Justine Sacarello, Head of Legal Change & Delivery, Lloyds Banking Group

- Key takeaways from FS and why the legal industry needs to catch up
- Actionable solutions to legal and regulatory change (GDPR, client data, etc.)
- What your clients don't tell you: Why the security of a law firm can win or lose you clients

16:50 **Is cybersquatting for brand reputation or profit?**

Etienne Greeff, CTO and Founder, SecureData

- Recent research findings from the latest cybercriminal activity typosquatting and soundsquatting
- The industries and businesses most at risk
- How organisations can protect themselves most effectively

17:10 **From compliance to culture: Awareness to action**

John Scott, Head of Information Security Education at Bank of England

- Case studies/actionable lessons from FS. What the legal industry can learn
- Securing employees as a business asset: If your employees are trained to be your first line of defence, how this can work as a business enabler
- The metrics of culture change: How do you measure that you've had an impact

17:30 Conference close

Education Seminars	
BitSight Technologies **How to manage cyber risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal)** **Philip East,** UK Sales Director, BitSight Technologies	Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber risk monitoring works for your company and the affiliates, your suppliers and peers. What attendees will learn: • How the cyber risk rating can be improved in the easiest way. All risk vectors and the results will be demonstrated • How cyber risk for the own company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings
eSentire **Build, buy or both: Which approach is right for you?** **Joe Nelson,** Principal Solutions Architect, eSentire	As cyber attacks become more frequent and more devastating, many organisations are quickly devising plans to protect against inevitable threats that could jeopardise their business. In this session, we break down the common dilemma of building your own Security Operations Centre (SOC) using your own staff, technology and resources versus enlisting the help of a Managed Detection and Response (MDR) partner. What attendees will learn: • What is a SOC, and how to decide if you need one • In-house vs MDR: The pros and cons • Build AND Buy: The advantages of a second SOC
foreseeti **Driving continuous security improvement with computer aided threat analysis** **Chris Few,** UK Business Manager, foreseeti	One of the most man-power intensive tasks in cybersecurity management has been analysing how vulnerable sensitive information is to cyber attack. It requires detailed understanding of both attacker capabilities and system defences. This presentation will explain and demonstrate how new software tools can import system security data at the device level and output a system level analysis of the most vulnerable attack paths. This is based on the likely time for a skilled attacker to exploit them. The approach enables repeatable, objective and quantitative analysis of the cybersecurity of IT systems. It can greatly increase the productivity of cyber threat analysts. With suitable security governance, these techniques can be used to drive continuous security improvement across the law firm based upon business needs and risks from cyber attack. What attendees will learn: • The concepts that underpin computer aided threat analysis • How computer aided threat analysis can measure the vulnerability of attack paths through complex IT systems • How to integrate computer aided threat analysis into a framework for continuous, business driven security improvement
Kaspersky Lab **Advanced/unknown cyber attacks – a new crisis communications challenge** **Povel Torudd,** Head of Corporate Communications, CSO Department, Kaspersky Lab	Based on a real case study we'll explore the challenges that come with advanced and unknown cyber attacks. What this means for both the CISO and corporate communication professionals within an organisation and how they must work together to ensure minimal reputational damage and regulatory compliance following an attack. What attendees will learn: • Why standard crisis communication templates aren't applicable for these types of incidents • Why a new incident classification is needed – and what it means for the corporate communications professional from a technical point of view • Open discussion on how new regulations, like GDPR, will affect transparency

Education Seminars	
LGC **What should you do if you suspect you have been the victim of a cyber incident – cyber incident response** **Stuart Dixon,** Casework Lead for the Digital Investigation Unit, Computer Investigation, LGC	Join Stuart to work through the correct and essential standard operating procedures to ensure preservation and examination of forensic digital evidence following a cyber incident. What attendees will learn: Essential operating and investigation procedure as a step by step guide for: • Preparing to respond • Equipment requirements • When you arrive at the clients site • While you're there on-site • When you leave – what is next
SecureLink UK **A rational look at threat management – L33tsp34k as a second language** **Ade Taylor,** CTO, SecureLink UK	Join Ade Taylor, CTO of SecureLink UK, as he explores the underbelly of the internet, shines a light into the so-called 'dark web' and explains why it's all a bit disappointing once you get there, and reveals some of the sophisticated and not quite so sophisticated approaches to gathering information about your electronic assets, the dysfunctional virtual project teams behind some of the more impressive attacks in recent years, and how being unlucky can be as bad as not having the right firewall when it comes to exposing yourself to threats. What attendees will learn: • What the 'dark web' is and how to get there, and that it's not really that dark at all • How easy it is to launch common attacks, and how people are making money from them • How to protect yourself from 'scattergun' attacks • How to rely a little less on luck • Why most 'threat intelligence' is useless