Post event report

Securing the Law Firm

25th January 2024 | London, UK

Strategic Sponsors

Akamai

SEPP**MAIL**

THREATLOCKER

Education Seminar Sponsors

Λbnormal

CISCO

FORTEM INFORMATION TECHNOLOGY

HOXHUNT

infoblox

Red Helix

Networking Sponsors

appurity

GYTPOL

Trustack

wavenet

Branding Sponsors

egress

keepit

Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

Re-thinking email and messaging: is there a better way?

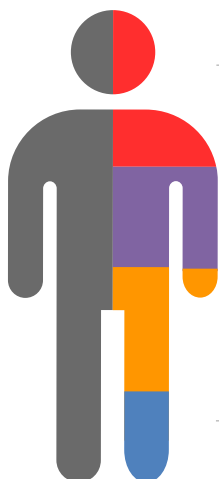Streamlining tools and information: focus on insight

Solutions for CISO burnout

Re-engineering the SOC: the problem of alert overload

Fixing Cloud configuration

From awareness to behaviour

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

Trish Almgren, Senior Product Marketing Manager & Field Evangelist, **Infoblox**

Ross Anderson, In-House Lawyer, **Clyde & Co LLP**

Jas Bassi, Head of Solutions Delivery, **Gateley Legal**

Allan Bell, Group Information Security Officer, **Ampa**

Dhruv Bisani, Head of Adversarial Attack Simulations, **Starling Bank**

Regina Bluman, Cyber Security Advisor, **Pinsent Masons**

Marco Cinnirella, Professor of Applied Social Psychology, **Royal Holloway**

Tim Collinson, Head of Information Security, **Walkers**

Simon Cuthbert, Former Advisor to the UK Government on Cybersecurity, on behalf of **Seppmail**

Steve Davies, Head of Cyber Security, **DLA Piper**

Ethan Duffell, Head of Information Security, **Clifford Chance LL**

Lee Dzendrowski, Solutions Director, **Fortem IT**

Matt Finn, Information Security Director, **DLA Piper**

Jonathan Freedman, Head of Technology & Security, **Howard Kennedy**

Valerie Jenkins, Chief Information Security Officer, **Clyde & Co LLP**

Petri Kuivala, Strategic Advisor, **Hoxhunt**

Seamus Lennon, Solutions Engineer, **ThreatLocker**

Richard Meeus, Director of Security Technology and Strategy, **Akamai**

Jorge Montiel, Sales Engineers EMEA, **Red Sift**

Edward Patmore, IT Manager, **SE Solicitors**

Jason Price, Solutions Engineer, **Red Helix**

Jonathan Root, Head of Information Security, **Mishcon de Reya**

Manit Sahib, Ethical Hacker, **The Global Fund**

Francisco Sanches, Director of Cyber Consulting, **Mishcon de Reya**

Mel Smith, Information Security Officer, **Buckles Solicitors LLP**

Tim Wadhwa-Brown, Senior Consulting Engineering Technical Leader, **Cisco**

Steve Wills, Senior Systems Engineer, **Abnormal Security**

Agenda	
08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**Information security and in-house legal: Thesis, antithesis, synthesis**
	Valerie Jenkins, Chief Information Security Officer, Clyde & Co LLP & **Ross Anderson,** In-House Lawyer, Clyde & Co LLP In-house legal teams and the CISO teams can report to the same person, and while their focus often aligns, there are times when a healthy tension ensures a balanced and fitting outcome for the Firm. In this session, we will explore how we work together in those times of clear alignment and when there may be differing perspectives, how we balance them to achieve success. • Looking through a matching lens • Different views, same outcome • Telescope or microscope
09:20	**Why email is still the number 1 threat to businesses (And how can we mitigate the threat?)**
	Simon Cuthbert, Former Advisor to the UK Government on Cybersecurity, on behalf of Seppmail • A brief history of email and why tales of the past are still relevant today • What lessons can we learn from the past? • How cybercriminals today use email to enter and manipulate your network • What does the future of hacking look like? • What can we do to beat the bad guys at their own game?
09:40	**Exposure management in the real world**
	Steve Davies, Head of Cyber Security, DLA Piper As law firms adopt new technology and develop new services, their attack surface will grow and become increasingly complex. Exposure management is the essential proactive practice of identifying, assessing and remediating potential vulnerabilities before they can be exploited by threat actors. This talk will introduce exposure management, provide an overview of the vulnerability landscape and outline how exposure management can be used to manage cyber-risks and make better business decisions. • What is exposure management? • Exploration of the latest developments in coverage and detection • What to expect in 2024 and beyond
10:00	**The good, the bad and ugly of AI**
	Jas Bassi, Head of Solutions Delivery, Gateley Legal (Moderator); **Ethan Duffell,** Head of Information Security, Clifford Chance LLP; **Steve Davies,** Head of Cyber Security, DLA Piper; **Jonathan Freedman,** Head of Technology & Security, Howard Kennedy • Panel looking at the opportunities, threats of AI in relation to protecting your firm
10:30	**Education Seminars | Session 1**
	Cisco **NIS2, DORA et al: What do they mean for the way we conduct business?** **Tim Wadhwa-Brown,** Senior Consulting Engineering Technical Leader, Cisco	**Infoblox** **The untapped power of DNS** **Trish Almgren,** Senior Product Marketing Manager & Field Evangelist, Infoblox
11:10	Networking break
11:40	**Information security culture in the law firm**
	Mark Jones, CISO, Allen & Overy (Moderator); **Deane Woods,** Global Security Operations Senior Manager, Allen & Overy; **Allan Bell,** Group Information Security Officer, Ampa; **Mel Smith,** Information Security Officer, Buckles Solicitors LLP; **Valerie Jenkins,** Chief Information Security Officer, Clyde & Co LLP; **Tim Collinson,** Head of Information Security, Walkers • Panel looking at the importance of creating a healthy cybersecurity culture within the firm: influencing, educating and intervening
12:10	**The purpose & future of endpoint security: How successful malware is created & how zero trust protects**
	Seamus Lennon, Solutions Engineer, ThreatLocker • The plethora of security vendors operating in today's marketplace can be overwhelming • With so many options, it's easy to be distracted with the latest, greatest, shiny tool • Join Seamus Lennon for a deep dive into the purpose of cybersecurity and how you can use that to your operational advantage today

Agenda

12:30	**Education Seminars | Session 2**	
	Fortem IT	**Hoxhunt**
	Securing legacy legal applications for compliance and navigating the complexities of email domain security	**Nation state data breach investigations and disclosure**
	Lee Dzendrowski, Solutions Director, Fortem IT &	**Petri Kuivala,** Strategic Advisor, Hoxhunt
	Edward Patmore, IT Manager, SE Solicitors	

13:10	Lunch and networking break

14:00	**The growing risk of your third parties' data breaches**
	Francisco Sanches, Director of Cyber Consulting, Mishcon de Reya (Moderator); **Jonathan Root,** Head of Information Security, Mishcon de Reya; **Ethan Duffell,** Head of Information Security, Clifford Chance LL; **Matt Finn,** Information Security Director, DLA Piper; **Regina Bluman,** Cyber Security Advisor, Pinsent Masons • The intricacies of this growing risk • Real-world examples of third-party data breaches • What steps organisations must take to mitigate this risk

14:30	**Keep your data safe without hindering your staff**
	Richard Meeus, Director of Security Technology and Strategy, Akamai Legal professionals handle sensitive data every day; this is like gold dust for hackers who are increasingly targeting law firms with different types of malware and more specifically ransomware. • Review how a ransomware attack unfolds, phase by phase • Learn how to prepare your firm for a ransomware attack by protecting critical applications and data • Understand how to ensure that only the correct piece of data ends up in the correct hands

14:50	**Education Seminars | Session 3**	
	Abnormal Security	**Red Helix**
	Cybersecurity in today's UK law firm: The importance of modern technology	**Safeguarding law firm communications under Google and Yahoo's mandates**
	Steve Wills, Senior Systems Engineer, Abnormal Security	**Jorge Montiel,** Sales Engineers EMEA, Red Sift & **Jason Price,** Solutions Engineer, Red Helix

15:30	Networking break

15:50	**Just when you thought it couldn't get any worse: How organisational responses to cyber-risk can (and often do) make things worse**
	Marco Cinnirella, Professor of Applied Social Psychology, Royal Holloway • Organisational responses to cyber-risk often ignore human psychology • How can red teaming and phishing sims jeopardise cybersecurity? • How can harmful group dynamics play a part in cyber-risk? • What does a psychology-aware response to cyber-risk look like?

16:10	**Building cyber-resilience with adversary simulation (threat driven defence)**
	Manit Sahib, Ethical Hacker, The Global Fund & **Dhruv Bisani,** Head of Adversarial Attack Simulations, Starling Bank • An overview of Red/Purple Teaming & its effectiveness in building rapid cyber-resilience • Industry frameworks for regulating attack simulation: CBEST; TIBER-EU & DORA • Leveraging threat intelligence for a threat driven defence • Measuring success: Discussing effective KPIs & metrics for tactical and strategic decisions (CISO/Board) • Assessing your current cyber-maturity posture: Identifying potential improvements & gaining additional funding • How to get started: Hiring an external team vs building your own internal Red Team • Common hurdles faced when establishing and operating a Red Team, drawing from real-world scenarios and providing actionable solutions • Best practices: Sharing proven best practices and lessons learned from our past experiences

16:40	Drinks reception
17:30	Conference close

Education Seminars

Abnormal Security

Cybersecurity in today's UK law firm: The importance of modern technology

Steve Wills, Senior Systems Engineer, Abnormal Security

From workflows, to data vulnerabilities, there is an expanse of unique challenges to be faced by the legal sector.

During this session, you will learn:

- Why the current email threat landscape requires a different approach
- How bad actors exploit the data vulnerabilities that exist within everyday workflows
- Why legal organisations face a higher volume of attacks
- What a modern behavioural AI solution can do to help secure law firms and their third-party clients from data or fiscal exploitation

Cisco

NIS2, DORA et al: What do they mean for the way we conduct business?

Tim Wadhwa-Brown, Senior Consulting Engineering Technical Leader, Cisco

In this presentation, Tim will talk about big changes to EU law – and how they'll affect legal services. He'll explore the overall changes stemming from NIS2 and DORA, and how Cisco is addressing them as an affected organisation, a vendor, and a professional services provider. This includes:

- New regulatory changes and challenges
- Third-party risks to legal services organisations
- Helpful guidance from the NCSC and other UK organisations
- Readiness tips and next steps

The purpose of Tim's blog is to drive awareness on NI52 and DORA, and to help organisations gauge their readiness.

Fortem IT

Securing legacy legal applications for compliance and navigating the complexities of email domain security

Lee Dzendrowski, Solutions Director, Fortem IT & **Edward Patmore,** IT Manager, SE Solicitors

This seminar is in two parts. In the first, hear Lee talk about how to deal with the problems you face in securing your legacy technology and how to think about upgrade paths from a security perspective. In the second, Edward will describe their organisation's approach to a major security and compliance upgrade for email – still your number one attack vector.

- Unsupported operating system challenges for the legal sector
- How to mitigate legacy unsupported applications
- Future-proof legacy legal applications
- Preparing for Windows 11
- Preparing your organisation for major upcoming email security compliance
- Achieve DMARC with ease
- What is BIMI and why implement it?

Hoxhunt

Nation-state data breach investigations and disclosure

Petri Kuivala, Strategic Advisor, Hoxhunt

As a CISO, Petri Kuivala has established board reporting, run OT-Security programmes, run insider protection programmes and evicted nation-state attackers from the network, which is his story...

This session will look at the following;

- Detailed anatomy of a major breach
- How can complex organisations protect themselves as attackers continue to grow more sophisticated?
- How to turn people into one of your greatest resources to detect true attacks
- Crossing the chasm in communicating with the board about cyber-risk

Education Seminars	
Infoblox **The untapped power of DNS** **Trish Almgren,** Senior Product Marketing Manager & Field Evangelist, Infoblox	Email/phishing, supply chain, and ransomware attacks are some of the top attack vectors facing UK-based firms, and they all have one thing in common – DNS. In this session, learn: • How to protect against advanced threats, including lookalike domains, with DNS-based intelligence • How DNS can be used to detect threat infrastructure several months (at least 60–80 days) before a planned attack • How taking a DNS detection and response approach can improve mean time to respond
Red Helix **Safeguarding law firm communications under Google and Yahoo's mandates** **Jorge Montiel,** Sales Engineers EMEA, Red Sift & **Jason Price,** Solutions Engineer, Red Helix	As we navigate the evolving landscape of email security, this presentation will address the concerns of law firms in light of Google and Yahoo's upcoming mandates for bulk email senders highlighting how to: • Future-proof your email security and block unauthorised mail from bad actors • Start dynamically managing your SPF, DKIM, DMARC, and MTA-STS records without needing to access your DNS • Save time, avoid manual configuration errors, and quickly add, authenticate or remove email sending services