Post event report

SECURING THE LAW FIRM

12th Securing the Law Firm

18th September 2019
London, UK

Strategic Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD.

commissum INFORMATION ASSURANCE

BlackBerry | CYLANCE

exabeam

GLASSWALL

SECURE DATA PART OF ORANGE CYBERDEFENSE

silver peak

TENEO OPENING MINDS

CS CYBER SCORE

Education Seminar Sponsors

Bitdefender

CYJAX

egress

Menlo Security

OneTrust Privacy PRIVACY MANAGEMENT SOFTWARE

prēempt

SECRUTINY

Networking Sponsor

netwrix

Branding Sponsors

dohertyassociates

FORTINET

paloalto NETWORKS

> “The conference provided an opportunity to explore cyber and information security concerns with peers, sharing our own perspectives and context to learn from each other. The presentations were of good quality and struck a good balance between technology providers and information security professionals working within the legal sector. I came away with loads of questions and more importantly, contacts who might help me find the answers.”

Info Security & Data Governance Manager Mills & Reeve LLP

Inside this report:

Key themes

Bridging the skills gap

Defining your architecture

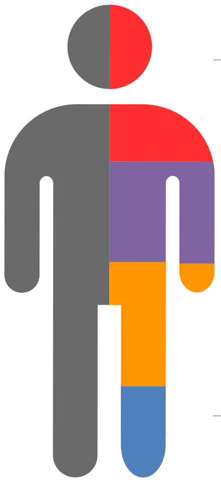
Keep the customer satisfied

Securing diffuse networks

Compliance with new regulations

Training and retaining key cyber staff

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

Nicholas Bloom, Vice President of Partnerships and Alliances, **Glasswall Solutions**

Dave Bloomer, Solutions Architect, **Menlo Security**

David Carroll, CEO, **CyberScore**

Richard Cassidy, Senior Director, Security Strategy, **Exabeam**

Simon Crumplin, CEO, **Secrutiny Ltd**

Bobbie Darrock, Legal Account Manager, **Egress**

Bruno Edenogie, Compliance Manager & Data Protection Officer, **Orrick, Herrington & Sutcliffe**

Dan Fox, Information Security Specialist, **Osborne Clarke**

Dr Anton Grashion, Senior Director of Product and Marketing, **Cylance**

Etienne Greeff, CTO, **SecureData**

Luke Hahn, Sales Manager, **OneTrust**

Rob Horne, Managing Consultant, **Commissum**

Emmet Horrigan, IT Director, **Arthur Cox**

Mark Lendon, Corporate Sales Director, **Egress**

Kadir Levent, Head of Incident Response, **CYJAX**

Simon Pamplin, EMEA Technical Sales Director, **Silver Peak**

Rob Pomeroy, Security Architect, **Hill Dickinson**

Andrew Powell, CIO, **Macfarlanes**

David Robinson, Head of IT Security, **Herbert Smith Freehills**

Ran Schwartz, Product Manager, Threat Prevention, **Check Point Software Technologies**

Mike Seeney, Head of Supply Chain Risk, **Pinsent Masons**

Steve Sumner, IT Director, **Taylor Vinters**

Mark Walmsley, CISO, **Freshfields**

Dan Wolff, Director, Endpoint Product Marketing, **Bitdefender**

Agenda

08:00	Registration and breakfast networking	
08:50	Chairman's welcome	
09:00	**Chain reactions: understanding your supply chain risk and its impact on security** A high-level interactive dialogue with **Mark Walmsley,** CISO, Freshfields, and **Mike Seeney,** Head of Supply Chain Risk, Pinsent Masons Grill two of the legal industry's most prominent security and risk leaders on what they have to share on mitigating your business risk. Topics covered include: • Understanding how your supply chain works and how you mitigate its security risk • Client questionnaires and meeting clients' security demands • Working with external auditors • Accountability and who owns supply chain risk?	
09:20	**Why understanding your attack surface matters** **Etienne Greeff,** CTO, SecureData • What does it mean to obtain and use 'cyber-intelligence' in a manner that effectively prioritises scarce resource across the full spectrum of 'Assess, Protect, Detect & Respond' cybersecurity disciplines? • Threats in cyber-space arise for two main reasons: weakness in IT infrastructure and an interest taken by an attacker. Most businesses know they must mitigate cyber-threats for their own good but also because regulators require them to • But the threat landscape is ever changing as technology evolves and attackers innovate. Ensuring an organisation has the skills, agility and underlying platforms and processes to understand, detect and manage cyber-threats is one of the most compelling challenges faced by any 21st century business. Regulatory changes have pushed to issue up to board level • What should the priority be for an organisation that wants to improve its cybersecurity posture, finding and removing vulnerabilities in its infrastructure or assessing the external threats it faces?	
09:40	**Law & disorder – raising the cybersecurity bar** **David Carroll,** CEO, CyberScore • Why organisations struggle to address the basic technical security controls • How the cybersecurity industry can help • Future trends	
10:00	**Cloud one on one** **Andrew Powell,** CIO, Macfarlanes Ask this industry leader what you really want to know about: • Where does the accountability lie for security of data in the Cloud? • Is it really all perfect on-premise? • Budget considerations when moving to the Cloud • Can you achieve the required service level agreement? • What are the contrasts/parallels between larger and smaller law firms in UK and US when it comes to Cloud adoption? • How do you deal with client reticence to Cloud adoption? • Does the structure of law firms create a unique set of risks and challenges?	
10:20	**Education Seminars | Session 1**	
	Bitdefender **Compliance does not equal security: how to identify gaps in your protection strategy** **Dan Wolff,** Director, Endpoint Product Marketing, Bitdefender	OneTrust **Perfect harmony: aligning privacy and security to supercharge your incident response plan** **Luke Hahn,** Sales Manager, OneTrust
11:00	Refreshments and networking	
11:30	**Finding the right snake oil: navigating the muddy waters of the cybersecurity solutions market** **Emmet Horrigan,** IT Director, Arthur Cox • The lack of a clearly defined cybersecurity strategy and structure in law firms. It's impacts on budget and purchasing decisions. • Put your money where your mouth is: almost every partner will now concede that cybersecurity is a key priority. But where does it really sit in terms of business priorities and client engagement? • The method behind the madness: why do we invest in cybersecurity? • Developing a reliable strategy to evaluate systems in a consistent way is a key challenge faced by every law firm. What are the metrics and techniques that information security leaders can use to find and invest in the right solutions?	
11:50	**Challenges estimating malware-associated risks and how AI can help overcome them** **Dr Anton Grashion,** Senior Director of Product and Marketing, Cylance • How unknowns make malware risks hard to estimate • How AI and machine learning can help us mitigate these unknowns	

Agenda

12:10	**Destruction by document: the greatest threat to law firms requires the most innovative solution** **Nicholas Bloom,** Vice President of Partnerships and Alliances, Glasswall Solutions • Malicious files and documents are the most common delivery vehicle for malware • Traditional detection-based methods of defence are increasingly failing • New approaches to document security offer increased levels of security without hampering productivity
12:30	**Leveraging SD-WAN to evolve and improve security for law firms** **Simon Pamplin,** EMEA Technical Sales Director, Silver Peak • Why SD-WAN is not to be feared • How SD-WAN complements, enables and improves security • How exactly Silver Peak can help improve your security posture
12:50	**Education Seminars | Session 2** CYJAX **How do you use next generation technology to build your threat intelligence & incident response capabilities?** **Kadir Levent,** Head of Incident Response, CYJAX Egress **Can't stop, won't stop: how to actually prevent email data breaches** **Bobbie Darrock,** Legal Account Manager, Egress, and **Mark Lendon,** Corporate Sales Director, Egress
13:30	Lunch and networking
14:30	**Crossing over from the dark side: one former lawyer's journey to information security professional and his cross-function business insights** **Rob Pomeroy,** Security Architect, Hill Dickinson • The journey from solicitor to information security professional. Insights from both sides of the security communication disconnect • Cybersecurity risk management: why the industry needs to gear up, assassinate the lowly risk matrix and bury it six feet under
14:50	**Insider threats: risks continue to grow** **Richard Cassidy,** Senior Director, Security Strategy, Exabeam • Familiarise yourself with breaches caused by insiders (41% of orgs had a threat last year) • Understand key challenges for detecting an insider threat • Learn how to protect against compromised and malicious employees
15:10	**Data on the move: protecting privacy and sensitive data in a mobile world** **Ran Schwartz,** Product Manager, Threat Prevention, Check Point Software Technologies • In 2019, mobile is a major player in every organisation's business. How do you maintain requirements to safeguard sensitive data of your customers? • You can trust your employees but can you trust their apps? • Key takeaways: you can trust your employees with sensitive business assets, but can you trust their apps?
15:30	**Education Seminars | Session 3** Menlo Security **Can you immunise yourself from web and email diseases?** **Dave Bloomer,** Solutions Architect, Menlo Security Secrutiny **SOC-as-a-Service: one size can fit ALL** **Simon Crumplin,** CEO, Secrutiny Ltd
16:10	Refreshments and networking
16:30	**EXECUTIVE PANEL DISCUSSION** **The inside(r's) story. How law firms are managing security and compliance alongside innovation and technological evolution** **Bruno Edenogie,** Compliance Manager & Data Protection Officer, Orrick, Herrington & Sutcliffe **Dan Fox,** Information Security Specialist, Osborne Clarke **David Robinson,** Head of IT Security, Herbert Smith Freehills
16:50	**Enlisting the elite castle guards – how an old defence method is still relevant today** **Rob Horne,** Managing Consultant, Commissum • Are you taking the necessary steps to ensure your company's cyber-defence is working? • Is protecting your company against new threats something you can do alone? Or would it be more cost effective to use an extra helping hand? • How does this defence work, what exactly does it do and what benefits will it provide? • Why an age-old method of defence is just as relevant in today's technologically advanced world and the best way to implement it
17:10	**Keeping it confidential. Client relationships. Confidentiality and openness** **Steve Sumner,** IT Director, Taylor Vinters • Security and the client relationship – confidentiality and openness • Binding commitments on security – can you deliver? • Managing client and partner expectations – business case may mean no • Asking the client – how dare you?
17:30	Conference close

Education Seminars	
Bitdefender **Compliance does not equal security: how to identify gaps in your protection strategy** **Dan Wolff,** Director, Endpoint Product Marketing, Bitdefender	Many firms who passed rigorous compliance certifications have been the victims of serious breaches. Due to the security skills shortage, high cost and fragmented state of today's security tools, no one can be confident they are safe. Detecting sophisticated hacker groups might prove too much of a challenge for most firms as full-time monitoring of events is not an activity all organisations can afford. Cost effective methods, tools and services exist which can maximise protection with the lowest cost to the firm. By investing in low overheard protection, firms can avoid the financial, reputational and regulatory implications of an inevitable security breach. **In this seminar, you will learn:** • Specific techniques and tools to assess where your gaps are • How simple configuration risk assessments can continuously harden your systems against attack • A three-pronged approach to realise the best protection
CYJAX **How do you use next generation technology to build your threat intelligence & incident response capabilities?** **Kadir Levent,** Head of Incident Response, CYJAX	In this compelling presentation, delegates will learn how next generation technology is being deployed in order to increase the power and enhance the reach of their intelligence and incident response teams. Delegates will hear how AI is adding a new dimension to their capabilities and helping shape the resource planning in ever more complex cyber-events and response panel activities. • How do you balance technology and your human resource in incident response? • Can you rely solely on technology to give you the answers you need? • Do you see potential in AI to drive efficiencies and time to recovery? • How can you use your incident response planning for more than data breaches?
Egress **Can't stop, won't stop: how to actually prevent email data breaches** **Bobbie Darrock,** Legal Account Manager, Egress, and **Mark Lendon,** Corporate Sales Director, Egress	People cause data breaches every day. That simple statement hides layers of complexity, compliance issues, and stress for CISOs and their security teams. While we may be able to 'logically' explain malicious breaches by linking them to motivations such as financial gain, it's often more difficult to understand and anticipate incidents caused by well-intentioned employees. The staff member who, for example, has too many things to do and sends an email to the wrong person. Or the person who feels they need to share information just to get their job done, choosing not to apply security or using unapproved channels. This presentation will look at some of the most common 'well-intentioned' email data breaches and what technology can do to prevent incidents caused by employees when sharing sensitive data via email. In particular, the session will examine developments in machine learning and advanced DLP technologies that can determine the risk of a data breach in real time to prevent unauthorised disclosure and enforce security for assured compliance. **Attend this presentation and learn about:** • The most common email data breach incidents • How machine learning and advanced DLP technology can detect and prevent email data breaches • How to practically improve protection for sensitive data shared via email, including ensuring adoption by end users • What all of this means for security ROI
Menlo Security **Can you immunise yourself from web and email diseases?** **Dave Bloomer,** Solutions Architect, Menlo Security	With 90% of cybercrime using web browsing and email as the entry into your organisation, is it possible to immunise your teams from these malicious attacks? Separation of users and their data from the outside world has been a method used by military and financial institutions for decades but at a high usability cost. What if you could use these same techniques and achieve a solid defence but without a user impact? • What is web, email and document isolation? • Why are the military and global top banks turning to isolation to protect themselves? • Is it actually possible to be 100% safe even browsing a known bad website?

Education Seminars	
OneTrust **Perfect harmony: aligning privacy and security to supercharge your incident response plan** **Luke Hahn,** Sales Manager, OneTrust	In the event of a breach, privacy and security professionals often approach incident response from two different outlooks. Whereas security teams are focused on threat vectors, privacy teams are concerned with personal data leaks and adhering to various global privacy laws. While the two come from different perspectives, it is possible to build an incident and breach response plan that addresses the needs of both teams. In this session, we'll discuss how to build a harmonised response plan that addresses both the security team's technical needs and privacy team's regulatory requirements across the patchwork of US privacy laws, the GDPR and other global privacy regulations. We'll also provide tips to help you map out a 72-hour personal data breach action plan and share practical advice to improve your privacy programme. • Learn how to build an incident and breach response plan that fits the needs of security teams and privacy teams • Breakdown what stakeholders, teams, tools and processes should come together in the event of an incident or breach • Understand how to maintain a consistent approach to incident response while complying with privacy regulations across the globe
Secrutiny **SOC-as-a-Service: one size can fit ALL** **Simon Crumplin,** CEO, Secrutiny Ltd	Law firms are engaged in a constant battle to ensure a reasonable security posture while balancing costs, usability, technology, user behaviour, transformation and agility. The SOC-as-a-Service (SOCaaS) concept resonates for many as it provides firms with the knowledge and skills necessary to combat cybersecurity threats. **In this session, we explore:** • Myths and realities of SOCaaS (What is it? How does it work in 'real-life'?) • Is building and maintaining a SOC price/function scalable? • Not all SOCaaS offerings are the same (How to evaluate SOCaaS providers) • Noisy SIEMs to meaningful SOC alerts (Getting SOC ready)