Post event report

Strategic Sponsors

BEYOND IDENTITY

FLOW the smart choice

MENLO SECURITY

TESSIAN

Education Seminar Sponsors

Abnormal

ankura

ARCTIC WOLF

egress

Kocho

OBSIDIAN

Networking Sponsors

CyberGuard Technologies

exabeam

themissinglink
Australia • United Kingdom

"Very useful day – great to see real life examples of what firms are doing to mitigate risk, what we can do to protect ourselves, and what's out there to keep us awake at night. Well worth the time out the office."
Director of IT, NABARRO LLP

"This was a very well attended event in a good quality venue, with a very full program and excellent networking opportunities. I was delighted to join an impressive list of speakers, with a depth of highly relevant experience, gained from an industry background."
Solicitor CIPP/US, PricewaterhouseCoopers Legal LLP

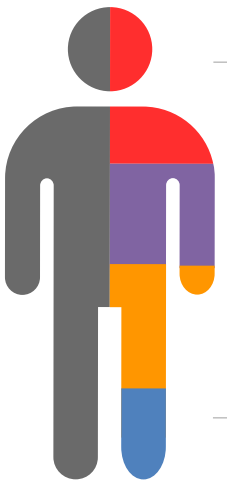
"I thought the conference was very informative, particularly the panel session from the clients at the end of the day. This really echoed the concerns and issues raised at the earlier presentations during the day, and showed us that the legal profession are rightly concerned to take information security seriously. The mix of presentations including clients, legal businesses and vendors brought depth to proceedings, it was a great opportunity to network with peers, and I had the opportunity to put faces to names of people I had only previously met via email or on the phone."
Information Security Manager, Bird & Bird LLP

Inside this report:

Key themes

- From threat/security to risk/resilience
- Can zero trust be done?
- Behavioural analytics
- Is ransomware the canary in the coal mine?
- Digging deeper into hybrid workplace security
- Building better Cloud security

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

James Alliband, Senior Product Strategy Manager, **Tessian**

Hans Allnutt, Partner & Cyber & Data Risk Practice Leader, **DAC Beachcroft**

Noha Amin, Head of Information and Cybersecurity, **TLT LLP**

Amir Ben-Efraim, CEO, **Menlo Security**

Annette Brown, Head of IT, **Milbank**

Jack Chapman, Vice President of Threat Intelligence, **Egress**

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

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

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

Chris Fuller, Principal Product and Solutions Architect, **Obsidian Security**

Etienne Greeff, CEO, **Flow**

Tanya Gross, Senior Managing Director, Cybersecurity, Data Analytics & eDiscovery, **Ankura**

David Guest, Solution Architect and Technology Evangelist, **Kocho**

Karen Jacks, CTO, **Bird & Bird**

Valerie Jenkins, CISO, **Clyde & Co**

Mark Jones, CISO, **Allen & Overy**

Karl Knowles, Head of Cyber, **HFW**

David Lomax, Systems Engineer, **Abnormal Security**

Chris Meidinger, Technical Director, **Beyond Identity**

Ahsan Qureshi, Senior Director, Cyber Security Risk Advisory, **Ankura**

Ryan Rubin, Senior Managing Director, Cybersecurity, Digital Forensics and Incident Response, **Ankura**

Steve Sandford, Senior Director, Cybersecurity, Digital Forensics and Incident Response, **Ankura**

Will Slater, Technology and Cyber Practice Director, **Gallagher**

Agenda

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **What has risk got to do with technology?**

Karen Jacks, CTO, Bird & Bird

- Buying technology platforms
- Managing the people
- The boring process bit

09:20 **Why attack surfaces heat up with remote work**

Amir Ben-Efraim, CEO, Menlo Security

- Why has the pivot to new working models increased cyber-risk?
- How are attackers leverage Highly Evasive Adaptive Threats (HEAT) to launch ransomware attacks?
- What can organisations do to avoid the next class of browser-based attacks?

09:40 **Staying ahead of cybersecurity threats in today's undeniably digital world**

Etienne Greeff, CEO, Flow

- Current geopolitical events together with the exponential increase of Ransomware means the risk for businesses has never been higher
- Identify and understand the current state of the cybersecurity threat landscape
- How businesses can securely harness the best of technology
- How we operate in a world with carrier grade adversaries

10:00 **Why do they do that? Harnessing psychology to inform information security in organisations**

Marco Cinnirella, Professor of Applied Social Psychology, Royal Holloway

- How to best leverage insights offered by psychology when investigating risky information security behaviours
- Understanding how risk perception is impacted by cognitive biases, culture, and the 'psychological work contract'
- Why a mixed methods approach to collecting data is vital
- How psychology can inform communication and education
- Why you can never completely 'design out' behavioural issues

10:20 **Education Seminars | Session 1**

Abnormal Security	Egress
Key considerations for choosing the right email security platform	**The changing email threat landscape**
David Lomax, Systems Engineer, Abnormal Security	**Jack Chapman,** Vice President of Threat Intelligence, Egress

11:00 Networking break

11:30 **EXECUTIVE PANEL DISCUSSION** **The big risks**

Mark Jones, CISO, Allen & Overy (Moderator); **Valerie Jenkins,** CISO, Clyde & Co; **Steve Davies,** Head of Cyber Security, DLA Piper

- Combating ransomware in the legal sector
- Addressing supply chain risk in an effective way
- Cutting your cloth

12:00 **Why legacy MFA is not good enough for modern authentication requirements**

Chris Meidinger, Technical Director, Beyond Identity

- A brief history of MFA
- We look into why traditional MFA was appropriate at the time but has kept up with the progress of attackers
- We detail the dangers posed by passwords and traditional MFA that requires a second device and/or push notifications
- Finally we cover off the alternative which is unphisable passwordless MFA

Agenda

12:20 — Navigating the dark corners of social engineering attacks

James Alliband, Senior Product Strategy Manager, Tessian

- Attackers have successfully infiltrated organisations through advanced social engineering techniques that exploit people's behaviour and vulnerabilities
- The success rate of these attacks has led to some of the worst data breaches in history. Still today, the number one method for delivering socially engineered attacks is via email
- In this session, we will walk you through socially engineered attacks found by the Tessian Threat Intelligence Team and what you can do to prevent these attacks

12:40 — Education Seminars | Session 2

Ankura	Arctic Wolf
Cyber-risk management in focus	**Security by chance or security by choice? The conundrum of security operations faced by law firms**
Ryan Rubin, Senior Managing Director, Cybersecurity, Digital Forensics and Incident Response; **Tanya Gross,** Senior Managing Director, Cybersecurity, Data Analytics & eDiscovery; **Steve Sandford,** Senior Director, Cybersecurity, Digital Forensics and Incident Response; and **Ahsan Qureshi,** Senior Director, Cyber Security Risk Advisory, Ankura	**Nick Dyer,** Senior Systems Engineer, Arctic Wolf

13:20 — Lunch break

14:30 — SENIOR LEADERSHIP PRIORITIES PANEL

Steve Davies, Head of Cyber DLA Piper (Moderator); **Karen Jacks,** CTO, Bird & Bird; **Karl Knowles,** Head of Cyber, HFW; **Jonathan Freedman,** Head of Technology & Security, Howard Kennedy; **Annette Brown,** Head of IT, Milbank

- Data privacy or security? How will companies view 'security' in the post-pandemic world?
- Hybrid working: problem solved or problem postponed?
- The issue of 'basic' cyber-hygiene (or 'why can't we stop ransomware?')
- Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated?
- The future of the security stack: insource/outsource/reduce number of solutions/rely on large application and infrastructure providers more
- Reining in the costs of cybersecurity

15:00 — What should you have in your post-breach legal toolbox?

Hans Allnutt, Partner & Cyber & Data Risk Practice Leader, DAC Beachcroft

This session will look at the current legal landscape for affirmative action following cyber-incidents and data breaches including:

- Actions against 'persons unknown': what benefits can suing an unknown hacker bring?
- Ransom payments: in what circumstances are they unlawful or illegal?
- Who is to blame when email breaches give rise to payment frauds?

15:20 — Education Seminars | Session 3

Kocho	Obsidian Security
The verdict is out! How to empower digital transformation without sacrificing security	**Obsidian Security: Extending Zero Trust to SaaS**
David Guest, Solution Architect and Technology Evangelist, Kocho	**Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security

16:00 — Networking break

16:30 — Vulnerability management in the real world

Steve Davies, Head of Cyber, DLA Piper

- Vulnerability management, then and now
- Prioritisation and compliance (risks vs. patch all the things)
- The move to DevSecOps, quick wins = big wins

16:50 — Creative operational security dashboard

Noha Amin, Head of Information and Cybersecurity, TLT LLP

- Key aspects of dashboards
- Types of dashboards
- How to improve security dashboard quality

17:10 — The cyber-insurance market – managing risk

Will Slater, Technology and Cyber Practice Director, Gallagher

- State of the cyber-market
- The challenges (red flags)
- State of coverage
- The journey (risk management)

17:30 — Drinks reception & conference close

Education Seminars

Abnormal Security

Key considerations for choosing the right email security platform

David Lomax, Systems Engineer, Abnormal Security

Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars.
Unfortunately, email threats are only growing in number. Business email compromise accounts for 44% of all losses to cybercrime, and the 2021 Verizon DBIR holds that phishing remains the top entry point for breaches – a position it has held for years.

Does that mean email is doomed, and we should give up? Quite the opposite – instead, we should look to newer technologies and an integrated security strategy that provides a modernised approach to email defence. In this webinar, we do just that.

Attend the Abnormal Security session for answers to your most pressing questions, including:

- What are modern email threats, and how are they different from legacy attacks?
- Which email threats are most concerning, and how can we defend against them?
- Which technical capabilities are required from modern email security providers?
- How do modern email security companies use AI, machine learning and data science to detect the most dangerous and costly attacks?

Ankura

Cyber risk management in focus

Ryan Rubin, Senior Managing Director – Cybersecurity, Digital Forensics and Incident Response, **Tanya Gross,** Senior Managing Director – Cybersecurity, Data Analytics & eDiscovery, **Steve Sandford,** Senior Director – Cybersecurity, Digital Forensics and Incident Response, and **Ahsan Qureshi,** Senior Director – Cyber Security Risk Advisory, Ankura

Securing the law firm in 2022 remains a challenge. In 2021, we saw examples of how cyber-exposures have adversely impacted companies in the legal sector. Our threat analysis on a sample of the industry in 2022 generates further food for thought. The key question is what else can law firms be doing to reduce their cyber-risk exposure. Join Ankura experts in this presentation as we discuss several challenges facing law firms today and some practical strategies to get ahead of the risks and reduce the likelihood of common breach scenarios impacting the industry.

- Key threats facing law firms today
- Understanding law firm structural inherent risks
- Key risk reduction strategies
- Tactics, techniques and procedures to drive down impact from breaches
- Recent case studies and key lessons learnt

Arctic Wolf

Security by chance or security by choice? The conundrum of security operations faced by law firms

Nick Dyer, Senior Systems Engineer, Arctic Wolf

- How can legal firms mitigate the growing alert & process fatigue whilst managing the increasing cyber-risk across an exploding multi-cloud attack surface?
- Why cyber-insurance premiums are on the rise, and proactive measures to ensure your business is covered
- We'll share our perspective running one of the world's largest security operations services, handling over 2 trillion security events per week
- How Arctic Wolf's Security Operations Cloud, and the Concierge Security Team, detected & remediated against ransomware for a customer.

Egress

The changing email threat landscape

Jack Chapman, Vice President of Threat Intelligence, Egress

Cybercriminals continue to launch increasingly sophisticated social engineering attacks. This is driven by crime as a service ecosystem, change in human behaviour and hardening of traditional routes into organisations. Because of these factors and more, it's no surprise that 85% of today's security breaches involve a human element.

Join this presentation to learn more about:

- Today's email security landscape and how the threats are evolving
- The behaviours behind email data breaches
- Why legacy approaches are no longer fit for purpose
- How to use behavioural science and zero trust to take back control over data loss
- How real-time teachable moments are more effective at changing human behaviour than traditional security awareness training

Education Seminars	
Kocho **The verdict is out! How to empower digital transformation without sacrificing security** **David Guest,** Solution Architect and Technology Evangelist, Kocho	Over the last 2 years, the way many law firms work has radically changed, with increases in virtual working, remote access, and cloud adoption. All of this is driving an explosion in apps, devices and users across an increasingly complex infrastructure. As the barriers blur between who is in your network and out of it, organisations struggle to manage identities and secure access for not only their employees but external partners, suppliers, and even clients. Learn how Microsoft technologies can help you provide secure, seamless, and compliant access to your business apps and data whilst striking the perfect balance between productivity and security. Join this seminar as we examine: • *Exhibit A:* How to enable seamless and secure end-user authentication • *Exhibit B:* How to protect critical resources with Conditional Access • *Exhibit C:* Why you should put identities at the heart of your security framework • *Exhibit D:* How to establish passwordless authentication in Azure AD
Obsidian Security **Obsidian Security: Extending Zero Trust to SaaS** **Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	In a world where the natural evolution towards SaaS was accelerated by remote working during the pandemic, do the principles of Zero Trust still apply? SaaS currently makes up 75% of the cloud, yet SaaS security visibility is notoriously difficult for security teams to manage, given the expertise, visibility and control required to manage each disparate SaaS application. Meanwhile, integrations between SaaS applications create a highly interconnected environment. With more sensitive business data entrusted to SaaS than ever before, it's time to consider how best we secure those applications. In this session, we'll explore how the Zero Trust principles of continuous verification, breach impact limitation and facilitation of rapid incident response can be applied to SaaS applications. • Review the guiding principles of Zero Trust • Learn the inherent risks of SaaS usage and why securing SaaS applications goes beyond the identity provider • Understand how the principles of Zero Trust can be applied to SaaS