Post event report

Strategic Sponsors

MENLO SECURITY

mimecast®

SentinelOne®

> “ Many thanks for the Public Sector Summit; it was very informative and helped me keep up to date with new and emerging risks and threats. ”
>
> **Technical Security Specialist, Department for Work and Pensions**

Inside this report:

Key themes

- Cybersecurity as a service: the pros and cons
- The rise and rise of effective cybersecurity regulation
- Developing the next generation of security leaders
- Reining in BigTech
- From smart machines to smart cities – securing the IoT
- Keeping citizens safe
- Insuring the uninsurable?
- Getting real about cyber-risk management
- Making the most of next gen tech: automation, AI and the rest
- Securing digital currencies and DLT
- Cybersecurity for SaaS/IaaS/PaaS
- Upskilling security teams

Who attended?

Cyber-security
We have a 20-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

Simon Brady,
Event Chairman
AKJ Associates

Andrew Dillon,
Sales Engineer
Mimecast

Glen Hymers,
Deputy Director Cyber and Information Security (CISO)
Cabinet Office

Anthony Garrett,
Risk Management Specialist
Essex County Council

Neil Kemp,
Senior Officer,
National Cyber Crime Unit
National Crime Agency

Chris Maddocks,
Head of Economic & Cyber Crime
North West Regional Organised Crime Unit

Ross Martin,
Sales Engineer UKI
SentinelOne

Bec McKeown,
CPsychol
Mind Science

Tom McVey,
Senior Solutions Architect, EMEA,
Menlo Security

Martin Peters,
Detective Superintendent, Deputy Lead
NPCC National Cybercrime Programme

Jonathan Pownall,
Senior Digital Specialist
National Audit Office

Dr. Adrian R. Warman,
Deputy Head of Security Operations
Ministry of Justice

Agenda	
09:40	Chairman's opening remarks
09:45	**Compliance as a mindset: Embracing regulation for better cybersecurity** **Glen Hymers,** Deputy Director Cyber and Information Security (CISO), Cabinet Office • Integrating cybersecurity into organisational values from decision-making processes to daily operations • Establishing clear policies and procedures that align regulatory requirements, industry best practices and business objectives: data protection, access control, incident response, and employee training • Implementing robust security controls • Establishing mechanisms for monitoring and measuring compliance with cybersecurity regulations and internal policies • Fostering a culture of accountability and collaboration and leading by example
10:05	**Modernising SecOps: How to optimise your estate, embrace legacy and improve operational efficiency** **Ross Martin,** Sales Engineer UKI, SentinelOne • Whilst a distributed digital landscape and broad, and varied surfaces, breed new opportunities for today's businesses, it also gives rise to new cybersecurity challenges. And those challenges can often be magnified if you happen to still have legacy OS in your estate. So what strategy and approaches should you be considering? • Ways to modernise your security operations and put your security analysts in the driving seat • How to ensure operational efficiency isn't aspirational, but achievable • Why legacy OS shouldn't be a hindrance to security, and can be accommodated to keep your organisation protected • How SecOps should accommodate a heterogeneous environment, driving efficient processes and reducing mean time to diagnose and fix issues
10:25	**Best practice in building human resilience in cybersecurity environments** **Bec McKeown,** CPsychol, Mind Science • The psychology behind resilience • The research into 'Best Thinking' • Cross-functional communication • Building high-performing teams
10:45	Comfort break
10:50	**PANEL DISCUSSION** **Law enforcement in the fight against cybercrime** **Simon Brady,** Event Chairman, AKJ Associates **Martin Peters,** Detective Superintendent, Deputy Lead, NPCC National Cybercrime Programme **Neil Kemp,** Senior Officer, National Cyber Crime Unit, National Crime Agency **Chris Maddocks,** Head of Economic & Cyber Crime, North West Regional Organised Crime Unit • Why is it so key from an investigative perspective that organisations report into law enforcement when they suffer a ransomware incident? • We have seen lots of activity against marketplaces and ransomware groups. For the future of law enforcement are there any other areas in the ecosystem you see as key targets to focus on in the fight against ransomware? I.E. initial access brokers, crypto seizures, infostealers etc • We have recently seen actions taken against two of the biggest ransomware groups (Alphv and Lockbit). Do you think the tide is turning in the fight against ransomware? • Following on, the measure of success of the Lockbit actions are still to be seen. If a multilayered disruption campaign including infrastructure takedowns, public attribution and sanctions can't kill a group, is making payments illegal the next logical step to take?

Agenda

11:10	**Human risk: It's not one size fits all**
	Andrew Dillon, Sales Engineer, Mimecast • Traditional security awareness programmes often fail to answer critical questions: 'Does training work? Does it reduce risk? What's the ROI?' The reality is, they can't and don't. To truly mitigate risk, we need to rethink our approach to security awareness. Security awareness needs to do more, and to do more, it needs to be re-envisioned • Learn how to transform your organisation's strategy for managing human risk • Identifying your riskiest employees with precision • Gain unprecedented visibility to mitigate real risks • Revolutionise security awareness with a human-centric approach
11:30	**The challenges of managing risks and security in the public sector**
	Anthony Garrett, Risk Management Specialist, Essex County Council • Balancing the imperative of accessibility in public services with the necessity of stringent cybersecurity measures • Establishing incident response plans and resilience strategies to ensure continuity of government operations amidst cyber-attacks • What collaborative frameworks can effectively bridge the gap between government agencies and private sector entities in mitigating cyber-risks? • Overcoming the key barriers to proposed changes and implementation
11:50	Comfort break
11:55	**Beyond tech: Building a human-centric approach to public sector security**
	Dr. Adrian R. Warman, Deputy Head of Security Operations, Ministry of Justice • The mindset shift: From compliance to proactive security culture • Vendor risk: Overreliance and its consequences • Empowering people, not gadgets: A balanced approach • Fail secure: Planning for when things do go wrong • Leadership's role in championing security
12:15	**Browser security: The proven prevention layer for enterprise cybersecurity**
	Tom McVey, Senior Solutions Architect, EMEA, Menlo Security According to Google, 98% of attacks originate from internet usage and 80% of those target end user browsers – sadly all too successfully. Combine this stark reality, with users' relentless demand for new SaaS and private applications, often collaborating with external stakeholders, and security pros are always running to stand still. Attendees will learn: • Security – The proven value of robust browser security across managed and unmanaged devices – automating browser configuration and establishing enhanced browser forensics • Connectivity – Your users and third parties need access to SaaS applications, private web apps and data, including the use of GenAI. We share how organisations are enhancing user protection and productivity while reducing the cost and complexity of solutions such as VDI • Compliance – How browser security supports organisations striving to comply with key NIS 2 requirements for incident management and prevention • We will provide real world examples and case studies of how to increase cyber-prevention through improved browser security
12:35	**Cybersecurity perspectives from the NAO**
	Jonathan Pownall, Senior Digital Specialist, National Audit Office • Cybersecurity strategies 2011-present: Why we are where we are • The new approach – a higher bar • Why legacy is such a big problem in government and is cloud the future?
12:55	Chairman's closing remarks
13:00	End of conference