

# Post event report



1<sup>st</sup> Annual Securing the Employee  
23<sup>rd</sup> November 2016 | London, UK

Conference Partner



Strategic Sponsors



Branding Sponsor



“ Can I thank you and the team at AKJ for yet another well-constructed, informative day. The content of the presentations was good with the presenters both engaging, humorous and well versed in their topics. Although some of the opinions did differ, this sparked healthy debate between the delegates. The venue itself was good and the food as always was delicious. I can only applaud you all for delivering what I am sure will be another must attend event for the future. ”

Group Information Security Manager, JD Sports Fashion

“ May I thank you and your colleagues for an excellent conference, I have advised all my colleagues to look out for events run by AKJ Associates. Venue: Excellent venue, accessible easily by tube, good layout in rooms, food excellent, heating, lighting, audio visual all very good. Speakers: Without exception all very good. Format: Really loved the 20 minute format, made the presentations focussed and relevant. ”

Manager, Technology Risk, Lloyds Banking Group

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda



**Speakers**

Sam Alderman-Miller,  
Cyber Security Account Executive  
**Darktrace**

Jamie Graves,  
CEO  
**ZoneFox**

Len Hynds,  
CSO  
**Modern Times Group**

David Janson,  
VP Sales, UK & Europe  
**PhishMe**

Simon Kerr-Davis,  
Senior Employment Law Specialist  
**Linklaters**

Simon Kouttis,  
Global Lead – Cyber Security  
**Stott and May**

Thom Langford,  
CISO  
**Publicis**

Tony Leighton,  
Head of Technology Risk Oversight  
**RBS**

Andrew Little,  
Partnership and Public Policy  
Director  
**Get Safe Online**

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

Martin Smith MBE,  
Chairman and Founder  
**The Security Company** and  
**The Security Awareness Special  
Interest Group (SASIG)**

Matthew Tyler,  
CEO  
**Blackfoot UK**

Amir Yampel,  
Insider Threats Business  
Development  
**ObserveIT**

**Key themes**

Securing email and social media

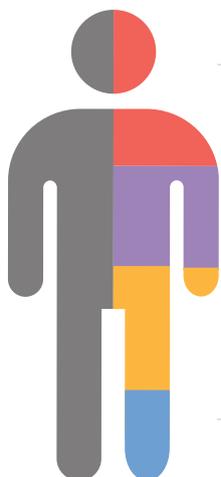
Employee engagement

Bring your own disaster?

The legal angle

Giving employees the right technology

**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

Agenda	
08:00	Registration
09:00	Conference welcome
09:10	<p><b>A glorious cyberexistence</b></p> <p><b>Andrew Little</b>, Partnership and Public Policy Director, Get Safe Online</p> <p>Get Safe Online is a not for profit public/private partnership working to deliver awareness, education and behaviour change in UK consumers and small businesses</p> <ul style="list-style-type: none"> <li>• How targeted, considered and constant messaging combining public and private sector resources to ensure positive experiences online</li> <li>• The business consequences of cyber security risk, and thoughts on an approach to mitigate</li> </ul>
09:30	<p><b>Defending against phishing: Preparing and using human sensors</b></p> <p><b>David Janson</b>, VP Sales, UK &amp; Europe, PhishMe</p> <ul style="list-style-type: none"> <li>• As the security industry has continued to underinvest in the human element of security, phishing has become the top attack vector for cybercriminals</li> <li>• Breaches continue to occur in record numbers, identification takes an exorbitantly long time, and the most preferred target is an organisation's human assets</li> <li>• Empowering humans to provide vetted intelligence into your incident response teams is often overlooked. Every organisation has these human sensors, and there's a natural desire for these employees to want to help</li> <li>• In this presentation, David Janson will discuss how to reduce susceptibility to human-targeted attacks and how to empower users to be human sensors</li> </ul>
09:50	<p><b>Awareness to action, compliance to maturity</b></p> <p><b>John Scott</b>, Head of Information Security Education, Bank of England</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Compliance vs. Maturity. What is the difference? Three 'stages' of employees</li> <li>• Case study: The Cyber 7</li> <li>• The metrics of culture change: How do you measure that you've had an impact</li> </ul>
10:10	Refreshments and networking break
10:40	<p><b>Stepping away from posters and email. The practical solutions to security awareness and engagement</b></p> <p><b>Thom Langford</b>, CISO, Publicis</p> <ul style="list-style-type: none"> <li>• Case studies in implementing cyber security culture</li> <li>• How to measure cyber security education and awareness</li> <li>• How CISOs can/need to interact with HR and other functions to integrate cyber security into the business value chain</li> <li>• Getting other senior employees on board as stakeholders in the cyber security strategy</li> <li>• The role of a CISO: not just to keep the organisation secure, but predominantly to help the business</li> <li>• How CISOs can break the stigma of being a 'technology employee'</li> </ul>
11:00	<p><b>The Enterprise Immune System: Using machine learning for next-generation cyber defence</b></p> <p><b>Sam Alderman-Miller</b>, Cyber Security Account Executive, Darktrace</p> <ul style="list-style-type: none"> <li>• How new machine learning and mathematics are automating advanced cyber defence</li> <li>• Why 100% network visibility allows you to detect threats as they happen, or before they happen</li> <li>• How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk</li> <li>• Real-world examples of unknown threats detected by 'immune system' technology</li> </ul>
11:20	<p><b>The psychology of the insider threat</b></p> <p><b>Jamie Graves</b>, CEO, ZoneFox</p> <ul style="list-style-type: none"> <li>• Why it's important to look within the perimeter to strengthen your security posture</li> <li>• The psychological and behavioural indicators of malicious insiders</li> <li>• How to mitigate all kinds of insider risks</li> </ul>
11:40	Refreshments and networking break

Agenda	
<b>12:00</b>	<p><b>The cure for 'Insiderphobia'</b></p> <p><b>Amir Yampel</b>, Insider Threats Business Development, ObservelT</p> <ul style="list-style-type: none"> <li>• Insider threat: Market background and overview                             <ul style="list-style-type: none"> <li>– Who is an insider?</li> <li>– Malicious vs. Unintentional</li> </ul> </li> <li>• Protecting employees to help protect your company                             <ul style="list-style-type: none"> <li>– Adding a proactive dimension to a traditionally reactive approach</li> <li>– Working together with employees to protect your organisation</li> <li>– Real-time security awareness</li> <li>– Deter malicious actors</li> </ul> </li> <li>• Ensuring security while maintaining employee privacy</li> </ul>
<b>12:20</b>	<p><b>The changing world of the CISO</b></p> <p><b>Len Hynds</b>, CSO, Modern Times Group</p> <ul style="list-style-type: none"> <li>• The constantly changing cyber threat landscape and the theatre of operations for a modern Chief Information Security Officer</li> <li>• The dynamics, the skills and the strategies of the business-centric CISO 3/. Finding, recruiting and keeping the talent necessary to deliver modern information security</li> <li>• Putting information security on the Board's agenda – and the synergies with corporate and social responsibility</li> </ul>
<b>12:40</b>	<p><b>The insider threat and the employment lifecycle</b></p> <p><b>Martin Smith MBE</b>, Chairman and Founder, The Security Company and The Security Awareness Special Interest Group (SASIG)</p> <ul style="list-style-type: none"> <li>• Where are we today and what might good look like?</li> <li>• The minimum requirements and the barriers to success</li> <li>• Security should influence every stage of the employment lifecycle</li> <li>• An opportunity for change</li> <li>• Trust versus security</li> </ul>
<b>13:00</b>	Lunch
<b>14:00</b>	<p><b>How the right training can help improve security culture</b></p> <p><b>Matthew Tyler</b>, CEO, Blackfoot UK</p> <ul style="list-style-type: none"> <li>• More about the legal and regulatory requirements for staff training contained in PCI, FCA, CNI, Public Sector – IG Toolkit, SRA best practice, Data Protection Act, EUGDPR, etc.</li> <li>• Who should be trained, about what, how and when</li> <li>• How to make best use of scarce training budget</li> <li>• Top tips for embedding information security awareness and best practice into a business-as-usual culture</li> </ul>
<b>14:20</b>	<p><b>EXECUTIVE PANEL DISCUSSION</b> <b>The cyber recruitment bottleneck – challenges and opportunities</b></p> <p><b>Simon Kouttis</b>, Global Lead – Cyber Security at Stott and May  <b>Thom Langford</b>, CISO, Publicis  <b>Len Hynds</b>, CSO, Modern Times Group  <b>Martin Smith MBE</b>, Chairman and Founder, The Security Company and The Security Awareness Special Interest Group (SASIG)</p>
<b>14:40</b>	<p><b>The legal risks and implications of employees as part of the security system</b></p> <p><b>Simon Kerr-Davis</b>, Senior Employment Law Specialist, Linklaters</p> <ul style="list-style-type: none"> <li>• The legal risks and implications of employees as part of the security system</li> <li>• How much of a duty/obligation does the organisation have to make sure the employee is not 'negligent'?</li> <li>• Solutions: What you need to know</li> </ul>
<b>15:00</b>	Refreshments and networking break
<b>15:20</b>	<p><b>Employees are your first line of defence...</b></p> <p><b>Tony Leighton</b>, Head of Technology Risk Oversight, RBS</p> <ul style="list-style-type: none"> <li>• How can you manage the risk?</li> <li>• 3 layered structure of defence, how it works at a large financial institution</li> <li>• Control environment? Is preventative better than detective?</li> <li>• How people based solutions (education) can work with technology to create a secure culture</li> </ul>
<b>15:40</b>	<p><b>People as perimeter, people as problem: The right approach</b></p> <p><b>Simon Brady</b>, Managing Editor, AKJ Associates</p>
<b>16:00</b>	Conference close