Post event report

Strategic Sponsors

CYLANCE
DARKTRACE
Hewlett Packard Enterprise
NSFOCUS
nuix
PHISHME
proofpoint
UNISYS
VERISIGN

Education Seminar Sponsors

egress
esentire
eset
HANDD BUSINESS SOLUTIONS
InteliSecure Safeguarding Critical Assets Worldwide
SIRIUM SECURE · SCALE · SIMPLIFY
resilient an IBM Company
SailPoint
TANIUM
thycotic
tripwire CONFIDENCE: SECURED
ZoneFox

Networking Sponsors

EMERSON Network Power
WEBROOT
WhiteHat SECURITY

Branding Sponsor

Gemserv

> “The Mid-Year e-Crime & Information Security event was very insightful and with a good range of topics. It was nice to see more focus moving towards the people element of information security, including engagement and tone from the top. The education seminars provided a good opportunity to learn more about topics that were high on my agenda and were informal enough to allow for some Q&A during the seminar. This event is not only useful to information security professionals but to anyone who is having to grapple with the complexity of information security within their organisation. I’m looking forward to the main event in March next year.”
>
> **Senior Information Security Officer, Admin RE**

> “The presentation and the topics covered at the e-Crime & Cyber Security Congress and Mid-Year meetings are of such a high quality that I do not bother going to other events. In addition I find that hospitality offered to all delegates is also excellent. I wish to express my thanks to you and AKJ for organising and hosting such great event.”
>
> **IT Security & Risk Officer, UBS**

> “Yesterday was my first time at the e-crime event and it was refreshingly non sales based, a chance for me to catch up with old colleagues, existing and potential vendors and to listen to peers talk openly about real world strategies versus the all too common generic abc of security.”
>
> **Head of IT Security, Office Depot**

Inside this report:

Key themes

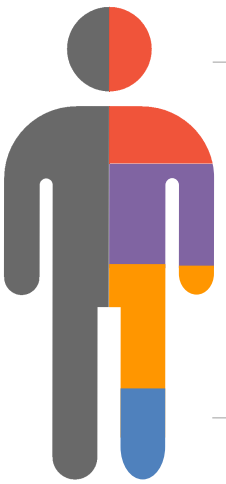
Is financial sector cyber security up to scratch?

Will your security precautions pass the scrutiny test?

What to do about us?

Consequences of the cloud

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

Darren Argyle, CISO, IHS Markit

Lee Barney, Head of Information Security, Marks & Spencer

Rohyt Belani, CEO & Founder, PhishMe

Simon Brady, Content Director, AKJ Associates

Joseph Carson, EMEA Product Marketing and Global Strategic Alliances, Thycotic

Jamie Cowper, Director of EMEA Marketing, Resilient, an IBM company

Paul Edon, Director of International Customer Services, Tripwire

Anton Grashion, Senior Director of Product Marketing, EMEA, Cylance

Jamie Graves, CEO, ZoneFox

Tim Grieveson, Chief Cyber & Security Strategist EMEA, Enterprise Security Products, Hewlett Packard Enterprise

Andy Harris, Engineering Director, Osirium

Robert Holmes, VP Products Email Security, Proofpoint

Len Hynds, Chief Security Officer, Modern Times Group

Mark James, IT Security Specialist, ESET UK

Karla Jobling, COO and Founder, BeecherMadden

Rohit Kinra, Director of Product Technology, Verisign

Simon Kouttis, Head of Cyber Security Practice, Stott and May

Matt Little, CTO, ZoneFox

Danny Maher, Chief Technology Officer, HANDD Business Solutions

Richard Meeus, VP Technology EMEA, NSFOCUS

Gary Miles, Detective Inspector, Metropolitan Police

Joe Nelson, Senior Solutions Engineer – EMEA, eSentire

Tyler Oliver, Director of Technical Account Management EMEA, Tanium

Alastair Parr, Strategic Planning and Operations Director, InteliSecure

Tony Pepper, Chief Executive Officer, Egress Software Technologies

Fraser Ross, Lead Security Architect EMEA, Unisys

Hayley Turner, Cyber Security Account Executive, Darktrace

Martin Whitby, Technical Consultant, SailPoint Technologies

Ulrich Wuermeling, Counsel and Co-editor of the Global Privacy & Security Compliance Law Blog, Latham & Watkins

Agenda

08:00 Registration

08:50 Chairman's welcome.

09:00 **Gamification of cyber security: An M&S case study**

Lee Barney, Head of Information Security, Marks & Spencer

- Why gamification is necessary for M&S
- M&S case study: Motivating colleagues to go past KPIs
- How gamification fits into the M&S corporate culture
- The limitations of gamification

09:20 **Ransomware, BEC, nation-state led attacks: Can we stem the epidemic?**

Rohyt Belani, CEO & Founder, PhishMe

- Gone are the days when cyber attacks were a simple nuisance, and digital perpetrators were teenage pranksters hacking out of intellectual curiosity
- Today, cyber attacks are conducted by organised criminal rings and nation-state actors, and failure in early detection often results in massive data breaches or critical systems being held to ransom
- Rohyt Belani, a cyber security industry veteran of 15 years, will walk through the gory details of such attacks and innovative defensive approaches that leverage human intelligence

09:40 **The internet of theft – industry trends, disrupting the adversary and swimming in the tsunami of data**

Tim Grieveson, Chief Cyber & Security Strategist EMEA, Enterprise Security Products, Hewlett Packard Enterprise

Tim focuses on the business of hacking and how the adversary is becoming more specialised and focused to steal enterprises critical assets, as well as touching on how the new EU GDPR impacts organisations in Europe and what CIOs and CISOs need to do to prepare for the new regulations.

- In the face of increasingly sophisticated cyber attacks, the cost and complexity of regulatory pressures, and the rapid transformation of enterprise IT, how do security professionals manage risk?
- Apps as the new battlefield – discover key insights into how security professionals can adjust their approach to defend not just the edge, but the interactions between users, applications and data regardless of location or device
- Patch or perish – why security teams must be more vigilant about applying patches at both the enterprise and individual user level
- Monetisation of malware – ransomware attacks targeting the enterprise and individuals are on the rise, how do security professionals avoid the loss of sensitive data?

10:00 **Managing data breach notification obligations**

Ulrich Wuermeling, Counsel and Co-editor of the Global Privacy & Security Compliance Law Blog, Latham & Watkins

- Regulatory requirements to notify data breaches to authorities and individuals
- Practical challenges and risks of data breach notifications
- Implementing notification requirements in incidence response procedures

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

Egress Software Technologies	eSentire	SailPoint Technologies	Tanium	ZoneFox
The enemy within: Why a company's greatest vulnerability is its people **Tony Pepper,** Chief Executive Officer, Egress Software Technologies	**Managing cyber security in a volatile world** **Joe Nelson,** Senior Solutions Engineer – EMEA, eSentire	**The anatomy of a data breach** **Martin Whitby,** Technical Consultant, SailPoint Technologies	**The uncomfortable reality – security hygiene is broken. Learn how to be the hunter, and never the hunted** **Tyler Oliver,** Director of Technical Account Management EMEA, Tanium	**GDPR – practical steps to keep you on track** **Jamie Graves,** CEO, ZoneFox

11:00 Networking and refreshments break

11:30 **Cyber security ambassadors: Effective and business efficient cyber security culture across a global enterprise**

Darren Argyle, CISO, IHS Markit

- Case study of IHS Markit security ambassador scheme
- What are the implications and advantages of making employees part of your security strategy? Are there risks?
- How this engages/gains the cooperation and attention of the wider company
- Dealing with security culture after a merger

11:50 **The enterprise immune system: Using machine learning for next-generation cyber defence**

Hayley Turner, Cyber Security Account Executive, Darktrace

- How new machine learning and mathematics are automating advanced cyber defence
- Why 100% network visibility allows you to detect threats as they happen, or before they happen
- How smart prioritisation and visualisation of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by 'immune system' technology

12:10 **Strengthen the core by stealth**

Fraser Ross, Lead Security Architect EMEA, Unisys

- What is micro-segmentation?
- Why the traditional approach to network security is flawed
- How micro-segmentation can help you regain and maintain the upper hand

12:30 **Fighting the next generation of targeted BEC attacks**

Robert Holmes, VP Products Email Security, Proofpoint

Business Email Compromise (BEC) attacks that impersonate executives and business partners to trick your employees are the biggest cyber threat to organisations today. This is not news. But what may surprise you is that the vast majority of BEC attacks are preventable. According to Gartner, Secure Email Gateways are struggling to address social engineering attacks with no payload. Well, things are changing. New technology can now surpass 'people' and 'process' initiatives to proactively protect your email channels while removing the guesswork for users. Learn about:

- The identity deception challenge – why spoofing works!
- Current BEC trends and attack methods
- Advances in technology to identify and block BEC attacks before they reach the inbox

Agenda

12:50 Education Seminars | Session 2

ESET	Intelisecure	Resilient, an IBM company and HANDD Business Solutions	Tripwire	ZoneFox
Hidden information within easy reach – threat intelligence **Mark James,** IT Security Specialist, ESET UK	**Effective data loss prevention: Bypassing the common pitfalls of DLP Management** **Alastair Parr,** Strategic Planning and Operations Director, InteliSecure	**The role of incident response in your cyber security strategy** **Jamie Cowper,** Director of EMEA Marketing, Resilient, an IBM company; and **Danny Maher,** Chief Technology Officer, HANDD Business Solutions	**Tales of a data breach survivor: Real world tips, tricks and advice** **Paul Edon,** Director of International Customer Services, Tripwire	**User behaviour modelling with ZoneFox** **Matt Little,** CTO, ZoneFox

13:30 Lunch

14:30 Business versus security: Does the drive for competitive advantage mean less due diligence?

Gary Miles, Detective Inspector, Metropolitan Police

- Functionality, ease of use and security: The tricky balance of keeping you safe
- The human element: The greatest cyber security threat?
- How can businesses and law enforcement collaborate more closely to ensure greater cyber security?

14:50 Latest DDoS trends and understanding the risks to your business

Rohit Kinra, Director of Product Technology, Verisign

- Recent DDoS attack trends indicate DDoS attacks are becoming more sophisticated and persistent – what do these DDoS trends mean for your organisation, especially during the upcoming holiday season?
- How should these behavioural shifts observed by Verisign in recent DDoS attacks concern you?
- Recommendations on how your organisation can prepare and defend against DDoS attacks

15:10 Intelligent hybrid security in action – protecting the G20 Summit 2016

Richard Meeus, VP Technology EMEA, NSFOCUS

- The current state of cyber security and global threat landscape
- Why it's important to have global threat intelligence to effectively combat advanced cyber threats
- How an intelligent hybrid security approach improves defences by combining cloud and on-premises security platforms with world-class global threat intelligence to provide real-time threat detection and mitigation
- How NSFOCUS protected the G20 Summit 2016 from targeted attacks

15:30 Education Seminars | Session 3

eSentire	Intelisecure	Osirium	Thycotic	Tripwire
Managing cyber security in a volatile world **Joe Nelson,** Senior Solutions Engineer – EMEA, eSentire	**Effective data loss prevention: Bypassing the common pitfalls of DLP Management** **Alastair Parr,** Strategic Planning and Operations Director, InteliSecure	**What to do about our most important wetware (those behind the keyboard)** **Andy Harris,** Engineering Director, Osirium	**Have you seen my cyber security perimeter?** **Joseph Carson,** EMEA Product Marketing and Global Strategic Alliances, Thycotic	**Tales of a data breach survivor: Real world tips, tricks and advice** **Paul Edon,** Director of International Customer Services, Tripwire

16:10 Networking and refreshments break

16:30 EXECUTIVE PANEL DISCUSSION **Security talent: Where to find it, how to qualify it and how to keep it**

Karla Jobling, COO and Founder, BeecherMadden

Len Hynds, Chief Security Officer, Modern Times Group

Simon Kouttis, Head of Cyber Security Practice, Stott and May

- What do you need in today's CISO?
- How valuable is experience in a landscape that is changing so fast?
- How do you measure cyber security effectiveness?
- How does the normal executive search model work in the cyber security industry?

17:00 Balancing risk – tackling security challenges with AI

Anton Grashion, Senior Director of Product Marketing, EMEA, Cylance

- The need for endpoint protection is nothing new and organisations don't spend a lot of time thinking about it, even though traditional security suites can only protect against threats that have been previously identified
- Artificial intelligence can secure a system against previously unknown threats, in addition to threats that may hide their malicious behaviour while under scrutiny
- Legacy solutions that sort through signatures stored in their database to determine whether an application meets their profile of a threat depend on the threat already existing within the database
- How to stop the millions of new threats that are released each month, many of which are able to hide their presence and mimic other types of file
- Modern enterprises inevitably increase their attack surface area as they adopt new and different work practices in order to better compete

17:20 No-where to hide: Coping with scrutiny and metrics

Simon Brady, Content Director, AKJ Associates

For some time now, cyber security has stopped being an internal function hidden from the C-suite; but more profound still, it's now a variable in the metrics of the key stakeholders who decide your companies' financial future. Be careful what you wish for.

- Financial markets want cyber security answers: Turn this to your advantage as CISOs and as companies
- Third-party companies are publishing unsolicited ratings of your cyber-competence. What to do?
- CISOs in transition: Making the jump from IT geek to strategic business partner

17:40 Drinks reception and networking

18:30 Close of conference

Education Seminars	
Egress Software Technologies **The enemy within: Why a company's greatest vulnerability is its people** Presenter: Tony Pepper, Chief Executive Officer, Egress Software Technologies	Employees pose a significant threat to the sensitive information held and processed by their organisation – and therefore to their company's compliance with industry and data protection legislation. In fact, ICO data breach trends reveal that two-thirds of breaches are caused by human error alone – that is, poor processes and systems in place, and lack of care when handling data. The insider threat, meanwhile, also remains ever-present for organisations. Organisations have for a long time recognised the importance of securing the 'sensitive' information they process and share electronically. However, despite identifying this need, they continually fail to implement solutions that can be effectively deployed to protect sensitive information. To improve compliance, it is therefore essential the challenges and limitations of using isolated DLP and encryption solutions be addressed and overcome. This presentation will examine how this can be achieved by implementing technology that mandates data protection from the point of creation to sharing internally and externally. In addition, it will address the growing role of technology to secure data throughout its 'lifecycle', providing greater information security and assurance, and reducing the opportunity for employees to cause a data breach – whether by accident or intentionally. What attendees will learn: • How to improve compliance with industry and data protection legislation • How to address the challenges and limitations of using isolated DLP and encryption solutions • Ways to implement information security solutions that address the 'lifecycle' of data protection, from creation to secure data release
eSentire **Managing cyber security in a volatile world** Presenter: Joe Nelson, Senior Solutions Engineer – EMEA, eSentire	What attendees will learn: • What is managed detection and response, and how can it defend your network from sophisticated cyber attacks? • Why technology is not the answer to cyber security: combining people, process and technology • Going beyond the traditional cyber security approach on perimeter defences: Today's attacks are cleverly disguised, proving that even with an arsenal of layered technology, attacks can still perforate the perimeter. • Discover next generation endpoint protection for today's advanced threats
ESET **Hidden information within easy reach – threat intelligence** Presenter: Mark James, IT Security Specialist, ESET UK	Are you informed about potential malware attacks that are under preparation or an ongoing attack aimed specifically against your organisation? Are you informed soon enough? Detailed knowledge of security threats provides companies with valuable insights about the present-day risks they are exposed to. By knowing more about these security risks, it makes it possible to actively prevent potential damages, comply to legal requirements, or at least to implement the necessary measures to mitigate them. Intelligence Reports help in recognising security threats and provide information about malware and its configurations, which is actually used or would be utilised in attacks against specific organisations or their customers (e.g. targeted threats). At the presentation you will hear more about the intelligence and information on targeted malware within your reach. What attendees will learn: • The kind of threat intelligence information that organisations can access • How this information can be analysed • How these insights can help to secure your organisation

Education Seminars	
InteliSecure **Effective data loss prevention: Bypassing the common pitfalls of DLP Management** Presenter: Alastair Parr, Strategic Planning and Operations Director, InteliSecure	While many organisations claim to have an effective data loss prevention methodology deployed, the reality is often very different. Please join us to understand where most go wrong, from inception, deployment, through to business as usual. This presentation will discuss how to effectively get to the nirvana of an effective data loss prevention programme benchmarked against best practice. Drawing from our experience managing over 3 million endpoints globally, we will cover what needs to be in place to avoid becoming dreaded 'shelfware' while getting the wider business onboard in a data loss prevention strategy. What attendees will learn: • What sort of data breaches we most commonly see in industry • How to effectively deploy a best-of-breed DLP programme • What the key challenges are in any DLP programme • How a DLP programme is effectively maintained over time to avoid false positives and false negative incidents • How a DLP programme integrates with wider data driven InfoSec initiatives
Osirium **What to do about our most important wetware (those behind the keyboard)** Presenter: Andy Harris, Engineering Director, Osirium	What attendees will learn: • Wetware to system interfaces • Where the threats are, how they work and how to defend against them • How to automate out as many human decision points as possible
Resilient, an IBM company and HANDD Business Solutions **The role of incident response in your cyber security strategy** Presenters: Jamie Cowper, Director of EMEA Marketing, Resilient, an IBM company; and Danny Maher, Chief Technology Officer, HANDD Business Solutions	Companies have invested in more security tools to detect and prevent cyber attacks and they now have challenges in how best to integrate these processes and manage the number of security incidents. Smart organisations are now looking at how they can reduce their time to detect and contain security incidents. This session, delivered by Resilient, the leading global provider of incident response platforms and HANDD, independent specialists in data protection, will review the current security landscape, looking at the shifting balance between prevention, detection and response. What will attendees learn: • Latest research into the state of cyber resilience in the UK market • What technology innovation exists to help security teams reduce their operational burden. • How companies are refocusing their efforts on cyber security incident response
SailPoint Technologies **The anatomy of a data breach** Presenter: Martin Whitby, Technical Consultant, SailPoint Technologies	When it comes to compromising user accounts, not much seems to have changed in the last 30 years. Breaches from decades ago could have just as easily happened today despite the high level of maturity many enterprises believe themselves to maintain. The reality is that many enterprises miss chances to catch identity-based attacks all of the time. What attendees will learn: • How a data breach occurs • How identity management could have prevented the breach • Why it is critical to put identity at the centre of cyber defence

Education Seminars

Tanium

The uncomfortable reality – security hygiene is broken. Learn how to be the hunter, and never the hunted

Presenter: Tyler Oliver, Director of Technical Account Management EMEA, Tanium

There is no silver bullet for endpoint security risk, and even the most advanced point solution will be ineffective without the fundamentals of security hygiene, but that's just the beginning. Basic security measures will stop the majority of the unsophisticated attacks, but what about attackers using more advanced methods to ruin your day? What if your estate is highly distributed, overly-complex, and constantly under attack? How do you hunt without visibility of your entire estate and the ability to evaluate what is normal/abnormal behaviour?

With just one server, Tanium allows you to ask a question of millions of endpoints, get a response in 15 seconds, make a decision quickly, and take action on an objective. This speed and scale gives you the advantage over the most advanced attacker, and in today's dynamic computing environments, the ability to see, observe, and interpret what is around you is crucial in order to successfully operate and defend your estate.

You want always to be the hunter, and never the hunted.

What attendees will learn:

- The foundations of good security hygiene
- How to discover unknown attacks with Tanium
- Why customers trust Tanium

Thycotic

Have you seen my cyber security perimeter?

Presenter: Joseph Carson, EMEA Product Marketing and Global Strategic Alliances, Thycotic

Blurred boundaries mean traditional security practices are failing. Understand why and learn about the next generation cyber security perimeter.

The traditional security perimeter is proving to no longer be an effective cyber security control and fast growing technologies like cloud, mobile and virtualisation make the boundaries of an organisation blurry. For many years organisations have protected their valuable and sensitive information by building a fence around assets, and all the data that flowed in and out was either via a single internet access point or on physical devices. This meant that a traditional perimeter was an effective measure as the boundaries were known. As long as the internet access was controlled by the data that flowed through it, it was possible to protect, monitor and control that data. Organisations protected the internet access with firewalls, VPNs, access controls, IDS, IPS, SIEMs, email gateways, and so forth, building multiple levels of security on the so-called perimeter. On physical devices, systems management and antivirus protected those systems and kept them updated with the latest security patches. This is a traditional security approach, used for almost 30 years, but in today's world it is no longer effective alone.

So why do we continue to see so many cyber breaches? If we look at why many of the cyber breaches in the past year have occurred, it comes down to three major factors that can be categorised into human factor, identities and credentials, and vulnerabilities. With the digital social society, we are sharing more information, ultimately causing ourselves to be much more exposed to social engineering and targeted spear phishing attacks with the ultimate goal to compromise our systems for financial fraud or steal our identities in order to access the company we are entrusted with protecting.

The perimeter has moved and we need to move with it. Learn about how identity and access management is evolving fast and becoming the new security perimeter.

What attendees will learn:

- Why the traditional perimeter is no longer effective
- What hacker techniques are being used to compromise organisations
- What some governments are doing to protect their citizens
- Technologies that will help create the new cyber security perimeter

Education Seminars	
Tripwire **Tales of a data breach survivor:** **Real world tips, tricks and advice** Presenter: Paul Edon, Director of International Customer Services, Tripwire	Join this engaging presentation as we share real-world examples of how organisations can effectively recover from a security incident. Learn how to quickly respond after detecting malicious indicators of compromise and minimise the potential damage to an organisation. This session will share practical activities that security professionals can implement regardless of their industry. What attendees will learn: • Quickly determine the extent of a compromise once a breach is detected • Understand the steps necessary to contain the affected systems and reduce security risk • Understand how to apply a 'standard of due care' in order to prove compliance to regulatory agencies • Use a systematic approach to restore trust in affected systems • Understand key information that needs to be communicated to various stakeholders in the event of a breach
ZoneFox **GDPR – practical steps to keep you on track** Presenter: Jamie Graves, CEO, ZoneFox	It's been a wild ride over the past few weeks with a great deal of changes now on the horizon, and not to mention a fair deal of uncertainty. In spite of this, and regardless of our new relationship with the EU, the General Data Protection Regulation (GDPR) will still impact on UK companies if we wish to provide services to EU citizens. Not following this regulation may end in very large fines (up to €20 million). As a result, there are a number of practical considerations organisations need to get to grip with now if they're to be ready for the 2018 start-date. What attendees will learn: • Understand what EU GDPR is really about and why compliance is crucial • Discover which aspects of GDPR are of high importance to your business • Gain insights into key activities that you'll need to focus on to be EUGDPR ready – and when you need to implement them
ZoneFox **User behaviour modelling with ZoneFox** Presenter: Matt Little, CTO, ZoneFox	Insiders – they're the one thing that we all have in our businesses. Whether we are talking about employees, contractors or partners, you need to know that your confidential data, intellectual property and your customer's personal data is secure. Signatures are old hat and just don't work. Rules describe your company but you can't define rules to cover every possible threat scenario. Learn about the new approach of behaviour modelling and how it can be used to spot unusual and potentially dangerous user behaviour – even those behaviours which you hadn't considered as risky. What attendees will learn: • Harness the power of machine learning to automatically spot unusual behaviours • Use peer group behaviour to highlight users of real concern • Discover how quickly you can investigate the detail of concerning behaviour once it has been highlighted • Spot potential leavers – before they hand in their notice