Post event report

Strategic Sponsors

corelight

CROWDSTRIKE

ENTRUST
SECURING A WORLD IN MOTION

MENLO SECURITY

okta

SONICWALL

tenable

Education Seminar Sponsors

Abnormal

CISCO

egress

Networking Sponsors

Cyberint

HOXHUNT

INTEGRITY
Part of Devoteam

PentestPeople

Branding Sponsor

RED BUTTON
DDoS Experts

"It was a pleasure attending the Securing Financial Services summit. The event was well organised and provided the ideal opportunity to network with attendees and hear security specialists speak about topical issues facing the financial sector."
Group and UK Data Protection Officer – Stonehage Fleming

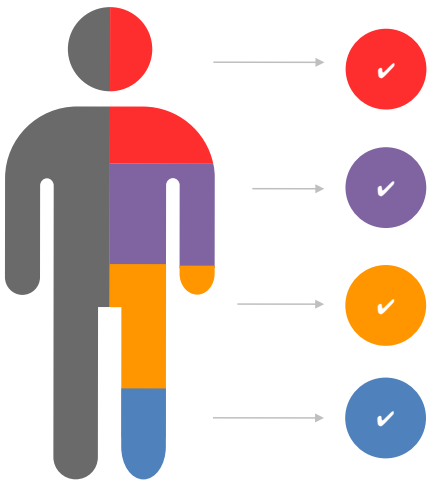
"Well done. I enjoyed the presentations and information provided all day by competent participants. Excellent organised and managed. Thank you for the very positive experience."
Director of IT Governance & Risk Manager, Commerzbank

Inside this report:

Key themes

- Cloud incident response
- The rise and rise of effective cybersecurity regulation
- Cloud native next
- Securing the technologies of the future
- Embracing risk management
- From cybercrime to cyberwar

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

Simon Brady, Managing Editor
AKJ Associates

Matthew Browning,
Former Head of Cyber Oversight
Direct Line Group

Oliver Cheal, General Manager,
Duo Security
Cisco

Moona Ederveen-Schneider,
Executive Director Europe
FS-ISAC

Guillaume Ehny,
Chief Information Security Officer
Kroo

Maya Goethals, Director – Compliance and Operational Risk
Bank of America

Robert Hann,
Global VP – Digital Security Centre of Excellence
Entrust

Kelly Hays,
Government Business Development
[redacted]

Luke Hebbes,
Director of Business Information Security
LSEG

Christian Heggen,
Strategic Threat Advisor
CrowdStrike

Philip Hoyer,
Field CTO
Okta

Ash Hunt, CISO
Apex Group

Steve Kinghan,
Head of Cyber Operations
Hiscox

David Lomax,
Security Engineering Manager EMEA
Abnormal Security

Tom McVey, Solution Architect
Menlo Security

Gavin Millard, Deputy CTO
Tenable

James Musk, Director of Public Sector and Enterprise UK
SonicWall

Ashley 'AJ' Nurcombe,
Senior Cyber Security Consultant – UK&I
Corelight

Peter Smith,
Chief Information Security Officer
Allica Bank

Sudeep Venkatesh,
Chief Customer Officer
Egress

Agenda	
08:30	Registration and networking break
09:20	Chairman's welcome
09:30	**Threat intel? Not just for your SIEM – Key opportunities for business resilience** **Moona Ederveen-Schneider,** Executive Director Europe, FS-ISAC • Enhancing business decision-making and risk management • Maximising on already existing resources • Building resilience through information sharing
09:50	**A case study in ransomware and the actor** **Kelly Hays,** Government Business Development, [redacted] • How we found them – aka 'first contact' – and how it played out • Why they're interesting • Continued tracking, evolving and growing tactics, and victim profiles • Summary: Ransomware is alive and well and still profitable for actors – it is not a saturated market. Patch your devices and call in a specialised team if you become a victim!
10:10	**People, process, technology – The road to post-quantum cryptography** **Robert Hann,** Global VP – Digital Security Centre of Excellence, Entrust • Why an accurate cryptographic asset inventory is essential in your initial preparations • How to approach your post-quantum cryptography preparedness • What steps need to be taken by organisations now, to prepare and migrate to quantum-resistant cryptography?
10:30	**How to build a quantitative technology risk programme from scratch?** **Ash Hunt,** CISO, Apex Group • Structuring loss scenarios • Collecting & calibrating the 'right' data – type and volume • Articulating risk as probable loss and opportunity • Calculating the financial and security return on investments • Delivering continuous control monitoring
10:50	Networking break
11:20	**Building a resilient and skilled SOC** **Steve Kinghan,** Head of Cyber Operations, Hiscox • Aligning skillsets to adversarial activity • The role of exercising your response • Behavioural shifts needed to empower analysts
11:40	**IAM invisible, who am I?** **Philip Hoyer,** Field CTO, Okta In this session, we'll explore how to use an identity-first approach to building future-proof systems able to withstand the cyber-threats of today and tomorrow across both workforce and customer experience use cases. • What does identity mean in the digital world? • How should organisations respond to the rising threat landscape?
12:00	**You might have 99 flaws, but they only need to find one** **Gavin Millard,** Deputy CTO, Tenable • We all know that network defenders have to be on the top of their game all the time, while an attacker only has to get lucky once. Regardless of their motivations or methods, it's that one overlooked vulnerability that will give them the opportunity to bring the business to its knees • Protecting the business is not just about being able to respond to attacks • Understanding, mapping and measuring your business's threat surface is how you can get ahead of the adversary • How to help stop your business becoming another statistic

Agenda

12:20 — Demystifying the e-Crime ecosystem and its diverse array of adversaries

Christian Heggen, Strategic Threat Advisor, CrowdStrike

- Hear how financially motivated e-Crime adversaries currently account for the majority of cybercriminal activity
- Discover clarity around the type of threat actors and their complex environment they use such as access brokers and affiliated models such as RaaS
- Receive tangible recommendations on how to protect your networks

12:40 — Education Seminars | Session 1

Abnormal Security	Cisco	Egress
7 key considerations for choosing the right email security platform	**User experience versus security – making security easy**	**The changing email threat landscape**
David Lomax, Security Engineering Manager EMEA, Abnormal Security	**Oliver Cheal,** General Manager, Duo Security, Cisco	**Sudeep Venkatesh,** Chief Customer Officer, Egress

13:20 — Lunch break

14:20 — How do we keep our clients' data safe?

Maya Goethals, Director – Compliance and Operational Risk, Bank of America

- How to balance data protection (security) with data protection (privacy)
- Is the juice worth the squeeze? Does requesting additional data still pay off?
- How to do privacy right in a world where privacy laws continuously change at the behest of local regulators
- Are rulings becoming too political?

14:40 — Is network evidence really needed for security operations?

Ashley 'AJ' Nurcombe, Senior Cyber Security Consultant – UK&I, Corelight

- Do you consider network evidence a crucial part of your SOC strategy?
- How do you really know which alerts are the most serious?
- What's the best way to shift from responding to alerts to hunting for threats?
- Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response

15:00 — Preventing the single biggest unknown cybersecurity threat targeting financial services organisations

Tom McVey, Solution Architect, Menlo Security

- Why current security solutions are failing to protect the remote legal workforce
- How modern work has given rise to Highly Evasive Adaptive Threats (HEAT) that target law firms
- How HEAT attacks leverage phishing and malicious document techniques to dupe lawyers
- Understanding if your firm is susceptible to HEAT attacks and how to prevent them

15:20 — Storms ahead: The dark side of the rush to the cloud

James Musk, Director of Public Sector and Enterprise UK, SonicWall

Join this session to understand more about:

- The biggest cyber-threats to your cloud infrastructure
- Why your cloud providers proprietary firewall is not enough
- The importance of layered security in securing financial services
- Recommendations to help mitigate today's most evasive attacks

15:40 — Networking break

16:00 — EXECUTIVE PANEL DISCUSSION — Matching resources to risks

Moderated by Simon Brady, Managing Editor, AKJ Associates;
Maya Goethals, Director – Compliance and Operational Risk, Bank of America;
Matthew Browning, Former Head of Cyber Oversight, Direct Line Group;
Steve Kinghan, Head of Cyber Operations, Hiscox;
Luke Hebbes, Director of Business Information Security, LSEG

- Has cyber-risk risen in the past 12 months and how do you measure that?
- What changes in the profile of your cyber-risk have been most significant?
- Is the bulk of security spend people or technology? Which is rising?
- We know about legacy tech, but what about legacy cyber-tech? Is it time to swap out first/second gen tools?
- Can banks outsource cybersecurity? If not, is the future just more and more expense?

16:30 — Drinks reception

17:30 — Conference close

Education Seminars

Abnormal Security

7 key considerations for choosing the right email security platform

David Lomax, Security Engineering Manager EMEA, Abnormal Security

Invoice fraud. Payroll diversion. Gift card requests. Fraudulent wire transfers. Malicious attachments. These types of attacks have dominated the cybersecurity space for the past few years, as security leaders worldwide attempt to find ways to stop increasingly sophisticated inbound threats.

But what about those attacks that are circumventing your inbound email, yet still infiltrating your email environment? How do you stop the attacks that come through indirect channels? Or perhaps even more concerning… how do you even discover these attacks in the first place?

Join this session to learn about:

- How the move to cloud email has opened your organisation to a variety of new attacks that no longer come through inbound email
- The real-world examples of these side-channel attacks that abuse third-party application access or result from legacy authentication exploitation
- How these attacks can result in credential theft, stolen session cookies, and compromised accounts – without you ever being aware
- How better mitigate this risk with cloud email security designed to detect and prevent these attacks

Cisco

User experience versus security – making security easy

Oliver Cheal, General Manager, Duo Security, Cisco

While security teams work to stay vigilant and put defences in place, how can we balance this with high productivity and low friction? User experience should not be the sacrificial lamb. If productivity takes a hit, then security is seen as the bad guy in the organisation, even within IT teams.

At the same time as people and organisations find innovative ways to transform digitally, we also see attackers finding new and creative ways to circumvent security controls. Protecting against attacks that bypass authentication and compromise users is now a heightened priority.

Cisco Secure looks at some typical user journeys, referencing security at the backend and how we keep this quietly effective.

- Where is the market?
- End user experience versus security
- User journeys and backend operation
- Security uplift

Egress

The changing email threat landscape

Sudeep Venkatesh, Chief Customer Officer, 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