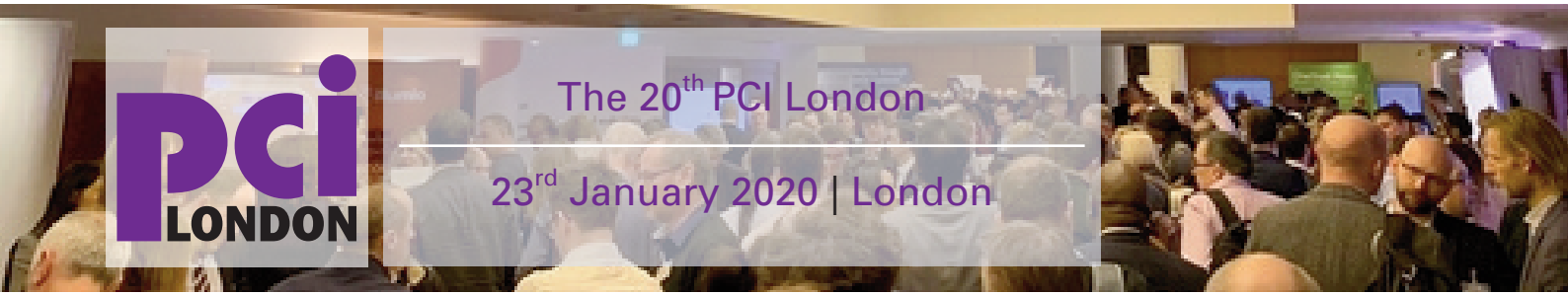
Post event report



Strategic Sponsors

NETTITUDE A LLOYD'S REGISTER COMPANY

OneTrust Privacy PRIVACY MANAGEMENT SOFTWARE

TANIUM

Education Seminar Sponsors

Card Easy™ Keypad payment by phone From Syntec

DataSecurity People

Eckoh

illumio

PCIpal®

PKWARE®

SecureTrust™ a Trustwave® division

semafone® securing data · protecting reputations

silver lining COMMUNICATION INNOVATION

Speik

SureCloud.

Networking Sponsors

One Payment

datadivider

ecsc more secure

GO ANYWHERE® A HelpSystems Solution

PRISM INFOSEC

SVL BUSINESS SOLUTIONS

tripwire®

Verifone®

Branding Sponsors

GeoLang Data Technologies A Shearwater Group plc Company

sysnet global solutions.

> “ PCI London is not only the perfect event for catching up on the new developments around the PCI standards, threats and countermeasures, but embraces the wider picture to cover GDPR, data security, cybersecurity threats and risk management also. ”
>
> **Information Security Manager, Diligenta**

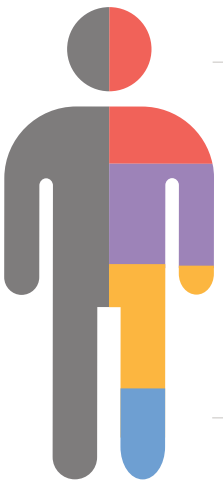
> “ The PCI event was excellent as ever. The presentation from Jeremy King, was very reassuring about the forthcoming v4 of the standard. The opportunity to discuss problems and share approaches with fellow practitioners is both refreshing and has provided Eureka moments! ”
>
> **Head of Information Security & Audit, Paragon Customer Communications**

Inside this report:

Key themes

- PCI DSS 4.0 - how to prepare
- Cutting the cost of compliance
- Building and managing compliance programmes
- New technologies, new threats?
- Aligning PCI DSS and GDPR efforts
- Cost-effective testing

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

Vipul Asher, Privacy Consulting Manager, OneTrust

Ben Barnes, Head of Product, Semafone

Simon Beeching, Business Development Director, Syntec

Theo Botha, Head of Cyber Security and Information Security, Which? Consumer's Association

Simon Brady, Managing Editor, AKJ Associates

Matthew Bryars, Vice Chairman, Speik

Ashley Burton, Head of Product, Eckoh

Thomas Chappelow, Principal Consultant, PCI and Information Security, Data Security People

Michelle Griffey, Chief Risk Officer, Communisis

Johan Hagdahl, GCRS Director, SecureTrust

Hugh James, CTO, PCI Pal

Mark James, Group DPO, Silver Lining Convergence

William James, Head of Payments Team, Addleshaw Goddard

Grant Jannaway, PCI Programming Manager, Vodafone

Jeremy King, International Director, PCI Security Standards Council

Richard Kirk, Vice President EMEA, Illumio

Michael Luck, IT Consultant, Xentian Limited

Nicola Lyons, Cyber Risk and Compliance Manager, The Manchester Airports Group

Craig Moores, Risk Advisory Practice Director, SureCloud

Laura Morgans, Information Security, Risk and Compliance Manager, Which? Consumer's Association

Peter O'Sullivan QSA, Principal Security Consultant, Nettitude

Joseph Okonkwo, Security Consultant, Aviva

Ian Olliffe, Global Compliance Officer, Quintessentially

Dan Oxley, Director of Technical Account Management, Tanium

Allan Packer, Managing Director, Silver Lining Convergence

Lesley Roe, Data Protection Officer, The Institute of Engineering and Technology

Blair Semple, Sr Director, Business Development, PKWARE

Dave Whitelegg, Head of Group Security, Capita

Agenda

08:00 Registration and breakfast networking

09:00 **Chairman's welcome**

Simon Brady, Managing Editor, AKJ Associates

- An overview of the current PCI DSS landscape and what to expect from the future
- Introduction to the winners of the PCI awards 2020
- Cross market case studies of PCI excellence

09:20 **Integrating PCI DSS, security and privacy**

Michelle Griffey, Chief Risk Officer, Communisis

- Linking security and privacy together and to wider risk management objectives (including ISO27001 and ISO22301)
- Balancing priorities: quasi-mandatory compliance like PCI DSS versus the law
- Working with third parties and clients to jointly solve data security and privacy concerns
- Solving complex problems with a small risk team

09:40 **Security is a continuous process**

Dan Oxley, Director of Technical Account Management, Tanium

- Security compliance should be a continuous process, why?
- Swap risky changes for incremental changes when you are resolving compliance issues
- Solve the complex task of locating where your non-compliance is and use technology rather than sweat and long hours to remediate

10:00 **Reducing PCI scope and integrating a P2PE system**

Michael Luck, IT Consultant, Xentian Limited

- Looking back at the movement towards implementing a cashless payment system
- 2011 to 2017; a period of articulation with which PCI DSS is used as the standard
- Reducing PCI scope and integrating a P2PE System

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

Eckoh	Illumio	PCI Pal	PKWARE	SureCloud
Can compliance be a catalyst for transformation? **Ashley Burton,** Head of Product, Eckoh	**Accurate scoping and effective segmentation for PCI DSS** **Richard Kirk,** Vice President EMEA, Illumio	**The evolution of digital payments in contact centres** **Hugh James,** CTO, PCI Pal	**Planning for changes in regulatory requirements** **Blair Semple,** Sr Director, Business Development, PKWARE	**PCI 4.0, so what? How to centre your PCI programme around your business objectives** **Craig Moores,** Risk Advisory Practice Director, SureCloud

11:00 Networking and refreshments

11:30 **PCI DSS 4.0 – what you need to know**

Jeremy King, International Director, PCI Security Standards Council

- New requirements: New and revised requirements to address evolving risks and threats to payment data and to reinforce security as a continuous process
- New focus on security objectives: Requirements and validation options are redesigned to focus on security objectives and meeting the intent of PCI DSS requirements
- Addressing evolving risks and threats to payment data and reinforcing security as a continuous process
- New validation option that gives more flexibility to organisations using different methodologies to meet the intent of PCI DSS requirements

11:50 **Third-party risk management: Overcoming today's most common security & privacy challenges**

Vipul Asher, Privacy Consulting Manager, OneTrust

- Review the drivers and challenges organisations face when managing third-party vendor risk
- Identify priorities before, during and after vendor procurement
- Takeaway a six-step approach for automating the third-party vendor risk lifecycle
- Hear real case studies from privacy experts on how practically to tackle third-party vendor risk

Agenda

12:10 — Happy anniversary! So you're PCI DSS compliant, now what?

Peter O'Sullivan QSA, Principal Security Consultant, Nettitude

- Achieving compliance for the first time is a big achievement, but it's just the beginning, and maintaining BAU compliance can be just as challenging
- Many merchants and service providers struggle to maintain compliance from year-to-year, and find themselves locked into arbitrary routines for tasks such as vulnerability scans and penetration tests based on their initial assessment date
- In this session, we'll discuss how you can spread the workload more evenly, maintain BAU compliance, and take some of the stress out of your next assessment

12:30 — Education Seminars | Session 2

SecureTrust	Speik	Semafone	Syntec	Tanium
Encryption solutions – are they secure or a hidden risk? **Johan Hagdahl,** GCRS Director, SecureTrust	**Your large or complex DTMF deployment may be at risk: lessons learned and first-hand advice** **Matthew Bryars,** Vice Chairman, Speik, and **Grant Jannaway,** PCI Programming Manager, Vodafone	**The challenge of compliance in an omnichannel business** **Ben Barnes,** Head of Product, Semafone	**Securing payments and card data in the evolving contact centre** **Simon Beeching,** Business Development Director, Syntec	**Putting into practice: security is a continuous process** **Dan Oxley,** Director of Technical Account Management, Tanium

13:10 — Lunch and networking

14:10 — How new digital business initiatives can disrupt your PCI DSS regime

Fireside chat with: **William James,** Head of Payments Team, Addleshaw Goddard

- The monetisation of payment data outside the transaction: novel PCI DSS issues for data controllers
- When is payment data (not) payment data? How aggregation of partial data affects PCI DSS
- Accidental scope: how to avoid novel data usage bringing your environment back into scope for PCI DSS
- Changing PCI DSS processes to cover new compliance and legal challenges

14:40 — EXECUTIVE PANEL DISCUSSION — How to adapt your PCI DSS structure to the changing data governance landscape

Lesley Roe, Data Protection Officer, The Institute of Engineering and Technology
Nicola Lyons, Cyber Risk and Compliance Manager, The Manchester Airports Group
Ian Olliffe, Global Compliance Officer, Quintessentially
Joseph Okonkwo, Security Consultant, Aviva

15:10 — Education Seminars | Session 3

Data Security People	Illumio	Silver Lining Convergence
Exploring the use of data and evidence – rather than hyperbole and fear – to drive security decisions **Thomas Chappelow,** Principal Consultant, PCI and Information Security, Data Security People	**Accurate scoping and effective segmentation for PCI DSS** **Richard Kirk,** Vice President EMEA, Illumio	**Helping organisations achieve GDPR & PCI DSS compliance without losing the will to live including good DPIAs!** **Mark James,** Group DPO, Silver Lining Convergence, and **Allan Packer,** Managing Director, Silver Lining Convergence

15:50 — Networking and refreshments

16:10 — Developing a PCI DSS and security strategy for a maturing PCI estate

Laura Morgans, Information Security, Risk and Compliance Manager, Which? Consumer's Association, and
Theo Botha, Head Of Cyber Security and Information Security, Which? Consumer's Association

- Engineering a security programme and strategy; building services, creating teams and delivering a business case to secure budget
- Successfully improving maturity against ISF Standard of Best Practice
- Implementing a constructive PCI DSS culture; dejargonise, clarify and embed

16:35 — Compliance, not complacency: using PCI DSS as a standard of excellence

Dave Whitelegg, Head of Group Security, Capita

- Internal restructuring and external assessments; how one of the UK's largest payments gateways became PCI DSS compliant
- Compliance with standards generates consistent standards of excellence
- Resolutions and take-aways; is PCI DSS compliance just one piece of the security puzzle?

17:00 — Drinks reception

17:30 — Conference close

Education Seminars	
Data Security People **Exploring the use of data and evidence – rather than hyperbole and fear – to drive security decisions** **Thomas Chappelow,** Principal Consultant, PCI and Information Security, Data Security People	As both a PCI QSA, and a critical infrastructure auditor, Tom frequently sees conflicting security requirements from a suite of information assurance standards competing for attention and budget. In this talk, Tom will expand on the evidence that he submitted to the Parliamentary Joint Committee on the National Security Strategy, and will explore the concept of data-driven security control design. The big question is: how well does this concept play with the requirements of the PCI DSS? Join us for this workshop to learn about: • Data types and what they bring to your organisation (what exactly are authoritative or non-authoritative data?) • Using behavioural models to target data to specific stakeholder needs • Using real-world breach data to iterate and re-focus security efforts to common points of weakness • Track evidence-driven events • How bad Tom's jokes are!
Eckoh **Can compliance be a catalyst for transformation?** **Ashley Burton,** Head of Product, Eckoh	Today's consumers want choice. They also want convenience and security. With the need to address different regulations, increasing cybersecurity and fraud risks, organisations too often look at these as incompatible goals – but that need not be the case. Instead, we need to 'think bigger' about what we offer consumers whilst also considering how the approach to compliance impacts the contact centre and innovation within our organisations. You'll learn how to 'think bigger' by: • Embracing alternative payments to meet consumer preferences • Letting your customers pay via whatever channel they find convenient • Making your contact centre compliant without affecting their existing processes • Extending PCI DSS de-scoping to reduce risk beyond payment processing • Overall, you'll learn to think about compliance, not as an inconvenience but as an enabler of great customer experience.
Illumio **Accurate scoping and effective segmentation for PCI DSS** **Richard Kirk,** Vice President EMEA, Illumio	PCI DSS compliance is hard. Qualified Security Asses-sors (QSAs) continue to issue findings about segmen-tation errors. Reports about high-profile data breaches via lateral movement attacks are still common. This session will outline: • How to lower the audit burden and prevent lateral movement attacks due to PCI scoping and segmentation errors • How to keep track of change and automatically adapt the applicable firewall rules – at scale • How to avoid the cost and management complexity associated with using networking/ SDN and data centre firewalls to segment internal traffic

Education Seminars	
PCI Pal **The evolution of digital payments in contact centres** **Hugh James,** CTO, PCI Pal	For today's 'always-on' consumer, being able to engage with an organisation via their channel of choice is rapidly becoming the norm and therefore being able to make payments, securely, via their preferred channel will surely follow. As we enter a new decade, Millennials and Gen Z are entering the economy preferring 'digital first' methods of communicating with companies. The rapid evolution of consumer demand and communication technologies are equally marked by an evolution of payment tools based on new digital communication channels. This seminar covers how the world of payments within contact centres is evolving alongside new digital communication applications to provide a true omnichannel solution for payments that is flexible, efficient and, above all, secure. In this session you'll find out: • How the contact centre payment landscape has evolved • How digital customer service channels are influencing and forcing the evolution of payments via contact centres • How to provide a true omnichannel solution for payments that is PCI compliant
PKWARE **Planning for changes in regulatory requirements** **Blair Semple,** Sr Director, Business Development, PKWARE	The proliferation of unstructured data has created many new security and compliance risks. Addressing this challenge will become increasingly important as regulations to protect customer data continue to evolve in the coming years. In this workshop, PKWARE Senior Director of Business Development Blair Semple will take you through: • A case study of how a global card issuer found and planned to deal with significant challenges in their unstructured data, and the ultimate result of their successful assessment • A discussion with your peers on how to prepare and manage changes in regulations and requirements to ensure continued compliance
SecureTrust **Encryption solutions – are they secure or a hidden risk?** **Johan Hagdahl,** GCRS Director, SecureTrust	Merchants are offered a plethora of solutions for their POS environments. Which type of solution should they choose? Can a non-listed encryption solution be as secure as a validated P2PE solution? What scope reduction can be expected when using validated solutions compared to non-validated solutions? Topics: • P2PE solutions, what are they and what should you look for when choosing one? • Non-listed encryption solutions, common pitfalls • Scope reduction capacity of implemented solutions • Examples from actual investigations
Speik **Your large or complex DTMF deployment may be at risk: lessons learned and first-hand advice** **Matthew Bryars,** Vice Chairman, Speik, and **Grant Jannaway,** PCI Programme Manager, Vodafone	What can go wrong, and how to avoid it. Speik (formerly known as Aeriandi) are experienced with very large enterprise deployments of DTMF suppression including for Vodafone UK's own contact centres. In addition to Vodafone UK, Speik's DTMF solutions for both agents and IVR payment systems have been deployed at many of the UK's largest utilities, insurance and retail organisations. In this session, we'll discuss the challenges faced by all our large corporate customers and we'll be joined by Grant Jannaway, Vodafone UK PCI Programme Manager for his merchant-eye view of the deployment challenges he has experienced and the lessons he's learned. Our years of experience have demonstrated the importance of coordination and communication and we'd like to share some of these lessons with you. Attendees will learn how to avoid saying "Oops, I...": • "Assumed my outsourced suppliers would understand what we are trying to achieve technically" • "Thought you were in charge of the project plan" • "Had conflicts between internal corporate security policies and PCI DSS" • "Left cardholder data in my legacy call recording" • "Didn't realise that some of my customers cannot use a keypad to enter card data" • "Did it again..." – well, we can't help you with that one!

Education Seminars

Semafone

The challenge of compliance in an omnichannel business

Ben Barnes, Head of Product, Semafone

Consumers these days are savvy. They're also often impatient. Constantly connected and with the world in the palm of their hands through their smartphones and tablets, they've become accustomed to an instantaneous response to any issue that arises, especially with the businesses they transact with. Using a variety of channels to communicate, whether it's email, SMS, webchat, social media, or IM, they seamlessly switch from one to the next, and they expect any brand they engage with to do to the same.

However, not all customers fit into the same demographic – your channel usage will vary depending on customer type. The challenge is to ensure that every user's experience is as frictionless as possible, whilst also meeting rigorous security, data protection and regulatory compliance legislation.

In this session you will learn:

- Why PCI DSS compliance should be at the core of your omnichannel engagement strategy
- How to optimise your PCI DSS compliance by channel
- Balancing omnichannel compliance and a frictionless user experience

Silver Lining Convergence

Helping organisations achieve GDPR & PCI DSS compliance without losing the will to live including good DPIAs!

Mark James, Group DPO, Silver Lining Convergence, and **Allan Packer**, Managing Director, Silver Lining Convergence

Silver Lining Convergence is involved in a variety of projects that pose significant commercial and 'Data Subject' risk. Most clients have identified commercial objectives. Most have some detail around workflows and infrastructure. Most can identify risks. Most have a good appreciation for the security requirements. So far so good…

Where many experience struggles is how to put all that together in a way that allows them to deploy a cohesive strategy that can be conveyed with some simplicity and does not cause them to pull any remaining hair out!

Our educational seminar will cover:

- Top 10 Gotcha's when 'doing it'
- How to conduct a DPIA (Data Protection Impact Assessment) – legal under GDPR
- Risk! – Likelihood v impact
- It's all about the people, people.

SureCloud

PCI 4.0, so what? How to centre your PCI programme around your business objectives

Craig Moores, Risk Advisory Practice Director, SureCloud

SureCloud will explore the challenges that organisations face when achieving and maintaining compliance with PCI DSS, with a particular focus on how organisations can design and deploy a programme that aligns with wider business objectives and embeds compliance activities into business operations.

With headlines focusing on the evolution of PCI DSS 4.0, our session will target all levels of stakeholder involvement in the management of PCI compliance. Using our experience of delivering compliance applications, as an Approved Scanning Vendor, as a penetration testing provider and critically from the experience of our ex-QSAs, we will share some of the shortfalls that organisations have experienced, particularly focusing on the people, process and technologies critical in protecting an organisation's payment channels.

We'll also look at how organisations can embrace the next release of the DSS and use this as a mechanism to prepare for the proposed changes coming in DSS 4.0 – the main consideration being baselining the compliance programme. Finally, we'll present our thoughts on how organisations can gain greater visibility of their compliance position by ensuring that timelines are defined and met and key metrics are defined, managed and reported on.

The session will be structured around our case study organisation, Bananas, to help bring this use case to life.

Key session takeaways:

- Understand some of the business challenges that organisations face when implementing and maintaining a PCI compliance programme
- Gain real-world insight into the compliance management shortfalls and lessons learned by other organisations
- Reflect on how the next release of the PCI DSS 4.0 provides an opportunity for organisations
- Learn how to gain visibility of compliance using metrics and automation

Education Seminars	
Syntec **Securing payments and card data in the evolving contact centre** **Simon Beeching,** Business Development Director, Syntec	Ensuring compliance across the whole contact centre environment is a multi-dimensional challenge, with technology and consumer expectations evolving to embrace multi-channel in addition to voice. What attendees will learn: • Point-to-point encryption (P2PE) versus DTMF masking – the pros and cons • De-scoping from PCI DSS controls by eliminating the sensitive card data in contact centres, following the PCI SSC's most recent guidelines for protecting telephone-based payment card data • Meeting the new multi-channel compliance challenge • Protecting the customer experience and improving customer trust • Case study feedback
Tanium **Putting into practice: security is a continuous process** **Dan Oxley,** Director of Technical Account Management, Tanium	In this session: • See how Tanium provides you with continuous monitoring for compliance • Solve the complex task of remediating non-compliance in your environment • Enable real-time reporting of your compliance position using the Tanium platform