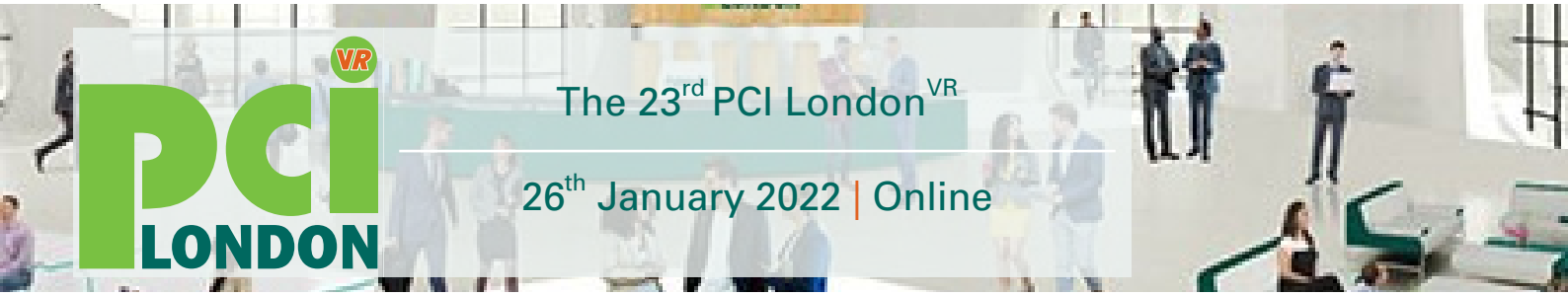
Post event report



Strategic Sponsors

Eckoh

illumio

SureCloud.

Education Seminar Sponsors

CyberCX

CYBERFORT

NETITUDE AN LRQA COMPANY

PCIpal

RAZORTHORN

silver lining COMMUNICATION INNOVATION

Networking Sponsors

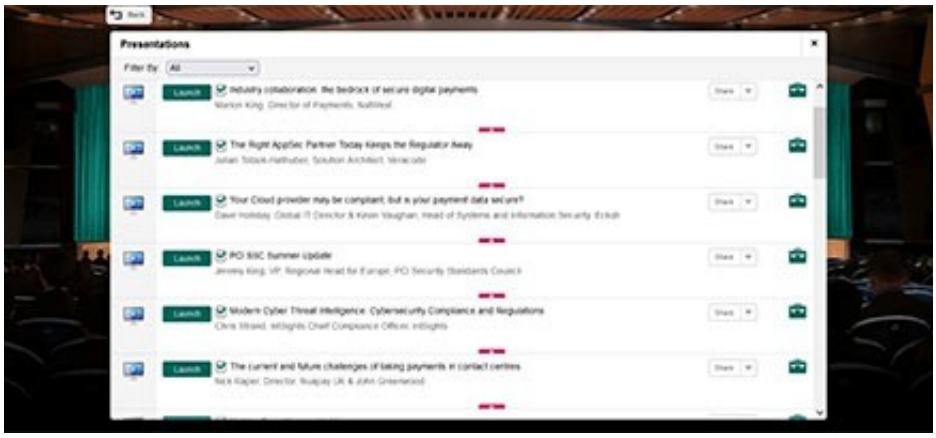
perimeter 81

"Thank you for this. I really did enjoy PCI London yesterday. Yet again, AKJ Associates produced an outstanding virtual conference. The speakers were first rate and the range of topics they covered were so varied that there was something for everyone. I was particularly glad to hear Jeremy King give his thoughts on PCI DSS 4.0 and how it's progressing. As for the platform on which the virtual conference was held, how easy can it be for us? It's so clear and intuitive to use. Whoever it was at AKJ Associates that selected the platform, well done them!"

Information Security Manager, Shaw Trust

Inside this report:

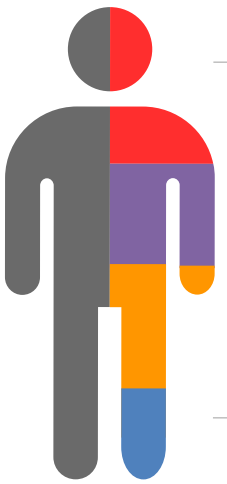
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars



Key themes

- Reducing the cost of PCI DSS compliance
- Building continuous, costeffective testing
- Sustaining selective, riskbased compliance
- Ensuring new technologies are compliant and secure
- Aligning PCI DSS, GDPR and other efforts
- What's happening with PCI DSS 4.0

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

Adam Brady, Director Systems Engineering EMEA
Illumio

Ashley Burton, Head of Product
Eckoh

Thomas Chappelow, Principal Security Consultant
Surecloud

Zac Crofts, Director of Sales & Marketing
Silver Lining Convergence

David L. Dann, ISA, PCI Project Lead
Under Armour

Dr Sam De Silva, Partner (solicitor)
CMS Cameron McKenna Nabarro Olswang LLP

John Elliott, Former Director, Industry Standards
Mastercard

Debbie Evans, Group Data Protection Officer
Rentokil Initial

Gill Fenney, IT Risk Assurance Manager
Bupa

Geoff Forsyth, CISO
PCI Pal

John Greenwood, Head of Technology & PCI Compliance
Compliance3

Matt Kay, Deputy Data Protection Officer
Metro Bank

Jeremy King, Regional Head for Europe
PCI Security Standards Council

Raghu Nandakumara, Field CTO EMEA
Illumio

Peter O'Sullivan, Principal Security Consultant
Nettitude

Sujit Parambath, Head of PCI Consulting Services
IT Governance

Candice Pressinger, Director of Customer Data Security
Elavon Europe

James Rees CISM, QSA, Managing Director
Razorthorn Security

Christina Stevenson, Director of GRC
CyberCX

Scott Storey, Security Architect
DLA Piper

David Toozs-Hobson, Business Development Director
Cyberfort

Agenda

08:00 Login & networking

08:50 Chairman's welcome

09:00 **PCI SSC 2022 update**

Jeremy King, Regional Head for Europe at PCI Security Standards Council

- Current status of the PCI DSS V4.0 and the release timescale
- Updates on other PCI Standards:
  - Software security framework
  - Point to point encryption
  - Mobile payments
- Remote assessments

09:20 **Dynamic cybersecurity: Adapting to a fast-evolving IT landscape**

Raghu Nandakumara, Field CTO EMEA, Illumio

- Overview of the benefits and risks of emerging technologies
- Adopting new IT systems with a robust risk and cybersecurity management embedded to it
- How can you build a cybersecurity, regulatory compliance and data privacy framework?

09:40 **Expanding the 'C' in PCI. Should we talk more broadly than 'card' payment security?**

Ashley Burton, Head of Product, Eckoh

- There's an increasing trend to use eWallets and alternative payment methods
- Personally identifiable data is being used more than card details to authenticate payments
- How could PCI DSS evolve to regulate these payment methods?
- What else should we consider in an increasingly diverse payments landscape?

10:00 **PCI compliance: The Challenges with a service provided card data environment (CDE)**

David L. Dann, ISA, PCI Project Lead, Under Armour

- Spreading the word within the enterprise – no single PCI compliant server provider bestows 100% compliance on a CDE
- What to look for in service provider attestations of compliance (AoC) and responsibility matrices
- The continued challenges in applying the Requirements (like 2.1.a and 2.1.b) to cloud-provided services

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

Illumio	Nettitude	Silver Lining Convergence
Why PCI matters for PCI DSS	**Planning, preparation & actions for PCI DSS 4.0**	**Remote working, omnichannel solutions & crypto – the future of payments**
Adam Brady, Director Systems Engineering EMEA, Illumio	**Peter O'Sullivan,** Principal Security Consultant, Nettitude	**Zac Crofts,** Director of Sales & Marketing, Silver Lining Convergence

10:50 Networking break

11:10 **EXECUTIVE PANEL DISCUSSION** **So you've lost cardholder data, what now?**

Matt Kay, Deputy Data Protection Officer, Metro Bank
Candice Pressinger, Director of Customer Data Security, Elavon Europe
Scott Storey, Security Architect, DLA Piper

- What are the key PCI DSS requirements around incident response and breach notification?
- How does the PCI DSS forensic investigation process work (and mesh with mandatory mechanisms)?
- For most privacy and security professionals, do modern cybersecurity and GDPR processes achieve enough PCI DSS compliance that specific provisions are no longer needed?

11:40 **Data, the DSS, and evidence-based control design**

Thomas Chappelow, Principal Security Consultant, Surecloud

This session will cover:

- Cyber 9/11? Cyber arms race? Surely not? Escape the hyperbole and fear with us!
- Learn how to use operational data to inform custom validation routes in Version 4.0 of the PCI DSS
- Can we make PFI report findings work for us?
- Is 'baseline' compliance OK?

Agenda

12:00	**Education Seminars | Session 2**	
	CyberCX **Achieving and maintaining an integrated management system** **Christina Stevenson,** Director of GRC, CyberCX	**PCI Pal** **PCI DSS V4.0: The challenges for organisations and QSAs** **Geoff Forsyth,** CISO, PCI Pal; and **Sujit Parambath,** Head of PCI Consulting Services, IT Governance
12:30	Lunch break	
13:30	**How much PCI DSS should you really do?**	
	John Elliott, Former Director, Industry Standards, Mastercard • Picking the right compliance strategy for your organisation's cyber-maturity • The critical success factor most people are afraid of • How to take advantage of card scheme rules to minimise compliance requirements • What's the future of PCI DSS compliance? Should you wait until it is unnecessary?	
13:50	**PCI DSS – overview of the key legal issues**	
	Dr Sam De Silva, Partner (solicitor), CMS Cameron McKenna Nabarro Olswang LLP (CMS) • Overview of the legal framework and implications of PCI DSS • Understanding the 'PCI DSS Contract Chain' • Identifying problems with PCI DSS in the legal context • Outline of actions that merchants should explore to reduce legal risk arising out of PCI DSS • Considering issues in PCI DSS clauses in contracts	
14:10	**Education Seminars | Session 3**	
	Cyberfort **Security is business critical – How will PCI V4 help push the agenda?** **David Toozs-Hobson,** Business Development Director, Cyberfort	**Razorthorn Security** **The criticality of scoping** **James Rees** CISM, QSA, Managing Director, Razorthorn Security
14:40	Networking break	
15:10	**EXECUTIVE PANEL DISCUSSION** **Getting technical**	
	Gill Fenney, IT Risk Assurance Manager, Bupa **Debbie Evans,** Group Data Protection Officer, Rentokil Initial **John Greenwood,** Head of Technology & PCI Compliance, Compliance3 The most stubborn and difficult technical challenges of achieving and maintaining PCI DSS compliance. For example, in the real world: • How can you restrict physical access to cardholder data across a multi-channel sales operation in a complex enterprise? • What are the key problems with regularly testing security systems and processes? • How do you go about preparing for a change like PCI DSS 4.0? • Is continuous monitoring of PCI DSS compliance unrealistic and if so, what is the frequency of your reviews?	
15:50	Chairman's closing remarks	
16:30	Conference close	

Education Seminars

CyberCX

Achieving and maintaining an integrated management system

Christina Stevenson, Director of GRC, CyberCX

Certifications and assessments are widely adopted by organisations as a means to evidence how compliant and effective an organisations' security practices are. Often it can seem a rather daunting task undertaking a certification assessment to ensure your organisation is aligned and that policies and procedures are implemented, with many organisations not knowing where to start. Throughout this session, we will provide practical suggestions on how your organisation can get started with the adoption of security best practices and key hints and tips on what to spend time on and what common mistakes to avoid. CyberCX will then cover how an integrated management system can be a cost effective way to achieve certification and compliance.

During the session, we will cover:

- What integrated management systems are and why are they beneficial
- Which certification is most important to your organisation
- How to get started on your compliance journey
- How to do the right thing at the right time whilst not overloading your teams and systems

Cyberfort

Security is business critical – how will PCI V4 help push the agenda?

David Toozs-Hobson, Business Development Director, Cyberfort

When it comes to regulations do, they go far enough? Are they clear or are they interpreted differently by businesses and QSAs? How do we change something so important to our business from a tick box exercise to a serious topic at the board meeting and ensure it is adhered to by all employees? Join us as we go beyond the importance of regulations and how these should be implemented as an enabler for your business not a hindrance.

- Discover the risks that are impacting our businesses and regulations
- Understand why security testing is critical, and does it go far enough
- Why security should be designed around risk and your business, not just the regulations
- The anticipated journey PCI DSS V4 will be taking us on

Illumio

Why PCI matters for PCI DSS

Adam Brady, Director Systems Engineering EMEA, Illumio

In this session we will give insight into:

- The most common challenges around compliance and the difficulty of tackling this from a security perspective
- How to scope the requirements for PCI including some observations around common architecture
- Why segmentation is important for compliance-based security and how Illumio can help

Nettitude

Planning, preparation & actions for PCI DSS 4.0

Peter O'Sullivan, Principal Security Consultant, Nettitude

With the release of PCI DSS 4.0 the hot topic, and appearing to be so close on the horizon, are you finding yourself in limbo wondering what you can or should be doing right now? In this session, we'll look at how you need to keep the wheels in motion on your current compliance programme, and what you should consider thinking about as we move into the next era of PCI DSS compliance.

This includes:

- When is the optimum time to migrate?
- How do you start the plan?
- What are your third-party service providers likely to be doing?
- The session will use some of the previous experiences around version migrations, along with Nettitude's own expectation of PCI DSS v4.0 to try and start you on your journey

Education Seminars

PCI Pal

PCI DSS V4.0: The challenges for organisations and QSAs

Geoff Forsyth, CISO, PCI Pal; and **Sujit Parambath,** Head of PCI Consulting Services, IT Governance

There is a buzz in the compliance industry about the new version of PCI DSS, due for release later this year.

In this session, PCI Pal's CISO, Geoff Forsyth talks with Sujith Parambath, Head of PCI Consulting Services at IT Governance about the new v4.0 standard and the impact it will make to the way organisations achieve PCI compliance.

The pair look at what's new within the standard:

- How QSAs will assess companies against the new requirements
- The major shift from a prescriptive to a subjective compliance model
- The challenges this will bring for organisations and QSAs alike.

Razorthorn Security

The criticality of scoping

James Rees CISM, QSA, Managing Director, Razorthorn Security

Of all the PCI DSS project work that takes place in a PCI DSS project one of the most critical parts to undertake is a full scoping to understand the environment that will need to become PCI DSS compliant.

Far too often the simple aspect of PCI DSS scoping is misunderstood, meaning that projects are quite often mis-scoped at their initial stages, causing projects to undertake remediation activities that are either not needed or can miss remediation that is. Scoping is by far the most important part of a PCI DSS project to get right; failure to do so can cause significant delays or problems when seeking full PCI DSS compliance.

During this session we will explore the following points of discussion:

- A QSA view on the importance of scoping
- The basics – how to scope a PCI DSS project
- The three rules of PCI DSS scoping
- Third parties
- Things to be careful of

Silver Lining Convergence

Remote working, omnichannel solutions & crypto – the future of payments

Zac Crofts, Director of Sales & Marketing, Silver Lining Convergence

As we see new technologies emerging, it opens us to a whole new set of challenges.

Following the last couple of years, there has never been a greater need for a fool-proof remote working strategy with an omnichannel offering. Businesses are to looking at more people working from home and the need to provide flexibility to both employees and customers is vital.

Advances in open-source technology, decentralisation, and cloud computing have enabled flexibility and on-demand capacity provisioning, paving the way for financial technology companies.

These new flexible, modular, and automated technologies have enabled the rapid adoption of cutting-edge technologies such as blockchain and crypto, powering the next wave of card and payments technology.

To be sure, there are technological and regulatory hurdles still to be crossed before full blockchain implementation – but the potential is clear.

In this session, Zac Crofts provides an insight into the importance on having a robust remote working strategy and omnichannel solution in place. He also explores the rise of crypto and what that could mean for the future of the payment industry.

Our seminar will cover the following:

- Importance of a robust remote working & omnichannel solution
- Rise of crypto and what this means for the payment industry
- Risk! – The likelihood v impact