

Post event report



Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



“ Thanks for the invite to the PCI London Summit conducted yesterday. It was great to attend the informative sessions & network with the industry people. ”

Information Security Manager,
Currys plc

Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Key themes

Reducing the cost of PCI DSS compliance

Securing Cloud and other critical third-party dependencies

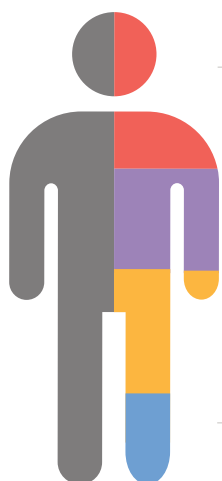
Aligning PCI DSS, GDPR and broader GRC efforts

Vulnerability Management and remediation

Getting continuous monitoring and automation right

New technologies – a challenge to compliance?

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, Event Chairman,
AKJ Associates

Kevin Burns, PCI Compliance Lead,
NMI

Stephen Cavey, Co-founder and Chief Evangelist,
Ground Labs

Katie Cowman, Senior PCI Assurance Manager,
Barclaycard

Graham Dawson, Cyber Security Architect,
Naked Wines

Dr Sam De Silva, Partner & Global Co-Head of Commercial Practice Group,
CMS

John Elliott, Security Advisor,
Jscrambler

Geoff Forsyth, CISO, **PCI Pal**

Richard Fridge, Director, Enterprise Sales EMEA,
Human Security

Sam Greaves, Senior Consultant,
CSA Cyber

Natasha Harries Roebuck, PCI Compliance Specialist,
Sky UK

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

Parminder Lall, CEO and Founder,
1 CyberValley

Peter Lane, Managing Cyber Security Consultant,
Cyro Cyber

Billy McDiarmid, Director of Solutions Engineering,
Red Sift

Laura Morgans, Security Risk and Compliance Manager,
Dr Martens, **Airwair International Ltd**

Rashmi Nadig, Data Protection and Compliance Officer,
Crisis

Peter O'Sullivan, Principal Information Security Consultant,
Blackfoot Cybersecurity

Kris Olejniczak, CEO, **Patronusec**

Mark Osborne, BISO & Regional CISO UK, EU & ANZ,
Corpays

Martin Petrov, CTO, **Integrity360**

Mark Phillips, VP, Sales and Solutions Engineering EMEA,
Human Security

Ketan Pyne, Pre Sales team for UK&I,
Thales Group

Matthew Santos,
Thales Group

Nadav Shatz, Customer Solutions and Advisory Director,
Orange Cyberdefense

Mike Somers,
PCI DSS Consultant & Specialist

Agenda			
08:00	Breakfast networking break		
08:50	Chair's welcome		
09:00	Update from the PCI Security Standards Council: Preparing for 31st March 2025		
	<p>Jeremy King, VP, Regional Head for Europe, PCI Security Standards Council</p> <ul style="list-style-type: none"> • What does this mean? • What are the new requirements? • How will this affect your organisation? • What other standards are changing in 2025? And how can you be involved? 		
09:20	Overcoming operational challenges implementing PCI DSS requirements 6.4.3 and 11.6.1		
	<p>John Elliott, Security Advisor, Jscrambler</p> <ul style="list-style-type: none"> • Taking a risk-based approach to maximise operation efficiency and stay secure • Understanding what the requirements say and importantly, do not say • Identifying the key stakeholders, how does JavaScript get added to your website? • How to avoid drowning in authorisations and make sure you manage the risk associated with script changes • Some common myths and misinterpretations shattered 		
09:40	PCI Compliance-as-a-Service: Simplifying the path to compliance		
	<p>Martin Petrov, CTO, Integrity360</p> <p>Navigating PCI compliance can be overwhelming with its numerous moving parts and complexities. Our session will demystify the concept of PCI Compliance-as-a-Service (PCLaaS) and demonstrate how organisations can simplify compliance efforts while improving security outcomes.</p> <ul style="list-style-type: none"> • What is PCLaaS? A managed approach to simplifying and outsourcing non-core compliance activities • Focus on growth: Free your internal teams by offloading compliance burdens to trusted experts • Simplify vendor management: Reduce vendor sprawl, consolidate contracts, and simplify oversight • Enhanced security posture: Improve audit outcomes and mitigate compliance gaps through expert-led strategies 		
10:00	PCI DSS & Internal Security Standards – Managing the alignments & conflict		
	<p>Katie Cowman, Senior PCI Assurance Manager, Barclaycard</p> <ul style="list-style-type: none"> • Tailoring organisational policies to meet unique security needs • Bridging PCI DSS compliance with internal security objectives • Mitigating overlaps and contradictions between external mandates and internal protocols 		
10:20	Education Seminars Session 1		
	<p>CSA Cyber</p> <p>How to align PCI compliance with other frameworks and tackle PCI in serverless and cloud-native environments</p> <p>Sam Greaves, Senior Consultant, CSA Cyber</p>	<p>PCI Pal</p> <p>Contact centre 101: Back to basics</p> <p>Geoff Forsyth, CISO, PCI Pal</p>	<p>Thales</p> <p>PCI DSS 4.0 compliance made easy with Thales</p> <p>Ketan Pyne, Pre Sales team for UK&I, Thales Group &</p> <p>Matthew Santos, Thales Group</p>
11:00	Networking break		
11:30	Mastering PCI evidence collection: Simplify, automate, succeed		
	<p>Natasha Harries Roebuck, PCI Compliance Specialist, Sky UK</p> <ul style="list-style-type: none"> • Practical strategies to make PCI evidence gathering less burdensome and more efficient • Automation for year-round readiness • Tips to transform the annual assessment from a scramble to a seamless process 		
11:50	Countdown to compliance: Misconceptions and action plans for 6.4.3 and 11.6.1		
	<p>Mark Phillips, VP, Sales and Solutions Engineering EMEA, Human Security;</p> <p>Richard Fridge, Director, Enterprise Sales EMEA, Human Security</p> <ul style="list-style-type: none"> • With the 31st March PCI DSS v4.0 deadline approaching, organisations face increasing pressure to meet requirements 6.4.3 and 11.6.1. This session addresses common misconceptions, clarifies what's required, and outlines practical steps to prepare effectively with just weeks remaining. 		
12:10	FIRESIDE CHAT: Demystifying PCI audits: Insights for seamless compliance		
	<p>Kevin Burns, PCI Compliance Lead, NMI</p> <ul style="list-style-type: none"> • What are the key steps organisations should take to ensure they're audit-ready throughout the year, not just at audit time? • How can companies turn PCI compliance from a checkbox exercise into an integral part of their security strategy? • What are some effective ways to handle unexpected challenges or findings during a PCI audit? • How can organisations future-proof their compliance programmes to adapt to changes in PCI DSS and the broader threat landscape? 		

Agenda		
12:30	Education Seminars Session 2	
	Cyro Cyber Scope smarter, not harder, by debunking common PCI myths that derail merchants Peter Lane , Managing Cyber Security Consultant, Cyro Cyber	Orange Cyberdefense Don't let your security fall apart: PCI DSS, third-party software, and the Tetris effect! Nadav Shatz , Customer Solutions and Advisory Director, Orange Cyberdefense
		Red Sift Navigating SSL and email PCI DSS compliance with Red Sift Billy McDiarmid , Director of Solutions Engineering, Red Sift
13:10	Lunch & networking break	
14:10	The legal and contractual side of PCI DSS: What every business needs to know	
	Dr Sam De Silva , Partner & Global Co-Head of Commercial Practice Group, CMS <ul style="list-style-type: none"> • Overview of the legal framework 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 	
14:30	Mastering PCI DSS compliance in a world of unstructured data	
	Stephen Cavey , Co-founder and Chief Evangelist, Ground Labs <ul style="list-style-type: none"> • In today's data-driven world, businesses are generating and ingesting more data than ever before, with up to 90% being unstructured. Ensuring PCI DSS compliance within these vast stores of unstructured data is a critical challenge, as organisations often lack the capability to identify and manage cardholder data (CHD) outside their defined cardholder data environment (CDE) • Learn what unstructured data is and the risks it presents for security and compliance • Understand the complexities of ensuring PCI DSS compliance when dealing with unstructured data • Discover how data discovery tools and techniques can help identify and manage unknown, unexpected and unstructured data • Explore how evidence-based data discovery can help effectively manage unstructured data and its importance as we look to the future of AI/ML and ever-increasing data growth 	
14:50	From stress to success: How continuous compliance simplifies PCI DSS	
	Peter O'Sullivan , Principal Information Security Consultant, Blackfoot Cybersecurity <ul style="list-style-type: none"> • Understand the challenges of maintaining PCI DSS compliance between assessments • Discover how shifting to a continuous compliance approach reduces stress and workload spikes • Explore practical strategies for integrating compliance into daily operations • Learn how to avoid non-compliance by anticipating lapses and overcoming them proactively 	
15:10	Education Seminars Session 3	
	1 CyberValley MythBusters Parminder Lall , CEO and Founder, 1 CyberValley	Patronusec Future of PCI Compliance Kris Olejniczak , CEO, Patronusec
15:50	Networking break	
16:10	Securing payment pages: Navigating PCI DSS v4 requirements for browser-loaded scripts	
	Graham Dawson , Cyber Security Architect, Naked Wines <ul style="list-style-type: none"> • Understanding the invisible risk: How scripts and tags on your payment pages impact security and compliance • Building robust controls: Implementing practical controls to mitigate risks and meet PCI DSS v4 standards effectively • Managing scripts with Reflectiz: Exploring a cutting-edge tool to monitor, control, and secure browser-loaded scripts in real time • The road ahead: What does the future holds for compliance and innovation 	
16:30	PCI compliance: Breaking barriers and shaping the future	
	Simon Brady , Event Chairman, AKJ Associates (Moderator); Kevin Burns , PCI Compliance Lead, NMI; Laura Morgans , Security Risk and Compliance Manager, Dr Martens, Airwair International Ltd; Rashmi Nadig , Data Protection and Compliance Officer, Crisis; Mike Somers , PCI DSS Consultant & Specialist; Mark Osborne , BISO & Regional CISO UK, EU & ANZ, Corpay <ul style="list-style-type: none"> • How can organisations balance evolving PCI standards with effective vendor management? • Is AI an enabler or a risk for PCI compliance, and how can it be used responsibly? • What are the biggest challenges in standardising PCI contractual obligations? • Is scope reduction still effective, or are there better strategies for managing PCI compliance? • How can we better communicate the business value of PCI compliance? 	
17:00	Drinks reception & networking	18:00 Conference close

Education Seminars	
<p>1 Cyber Valley</p> <p>MythBusters</p> <p>Parminder Lall, CEO and Founder, 1 Cyber Valley</p>	<p>Following on to last year’s success of ‘Back To The Future’ presentation at PCI London, this year we bring you ‘MythBusters: Who You’re Gonna Call?’. In an ever-evolving security landscape and with numerous interpretations and opinions about the PCI DSS framework, organisations can often misunderstand their responsibilities or fail to comply fully. We need to identify ‘Misconception v Reality’.</p> <p>Attendees will learn:</p> <ul style="list-style-type: none"> • Will all QSAs maintain the same perspective? • Does reliance on outsourcing to a third-party provider eliminate your compliance responsibilities? • Are you protected by treating PCI DSS as a One-Time effort? • If you don’t store cardholder data you do not need to comply
<p>CSA Cyber</p> <p>How to align PCI compliance with other frameworks and tackle PCI in serverless and cloud-native environments</p> <p>Sam Greaves, Senior Consultant, CSA Cyber</p>	<p>This session has a bit of scope creep – much like your last PCI audit! You’re getting two topics for the price of one today. Most large organisations requiring PCI compliance also adhere to other standards, such as ISO 27001 or SOC 2. Traditionally, audits for each framework are conducted separately, making them time-consuming and resource intensive. By mapping controls across standards and conducting combined audits, organisations can streamline evidence collection and reduce effort. At the same time, modern serverless and cloud-native environments introduce unique challenges, such as shared responsibility models and the inability to apply traditional security controls – all whilst offering significant benefits like scalability and efficiency.</p> <p>Join Sam as he explores the future of PCI compliance in a serverless world and how to navigate these emerging opportunities.</p> <p>Attendees will learn:</p> <ul style="list-style-type: none"> • Framework alignment: Map controls across PCI DSS, ISO 27001, and SOC 2 etc., to minimise duplication and streamline compliance • Unified audits: Consolidate audits across multiple frameworks to save time, effort, and costs • Cloud native challenges: Address complexities in serverless and containerised environments • Compensating controls: Replace traditional methods like FIM with modern approaches such as logging, runtime security, and immutable infrastructure
<p>Cyro Cyber</p> <p>Scope smarter, not harder, by debunking common PCI myths that derail merchants</p> <p>Peter Lane, Managing Cyber Security Consultant, Cyro Cyber</p>	<p>You know the drill. PCI requirements are notoriously complex, scoping gets messy, and the plethora of guidance out there often raises more questions than answers! With tight deadlines and limited resources, most merchants don’t have the bandwidth to master the intricacies that QSAs live and breathe. The result? The same scoping mistakes and misconceptions continue to derail compliance efforts and stunt business growth. But with the right strategies, you can avoid these pitfalls.</p> <p>Join Peter Lane, PCI DSS QSA and seasoned security expert, for a solution-focused session that tackles common PCI problems head-on. With 17+ years’ experience helping businesses from SMBs to enterprises, Peter will demystify the PCI essentials that impact your ability to meet the various demands. He will cover everything from why scoping matters more than you think, to the real-world implications of which technology or service providers you use and how to avoid unnecessary reporting challenges to ensure simpler compliance, and stronger security.</p> <p>By the end of the session, you’ll be able to:</p> <ul style="list-style-type: none"> • Understand the most common PCI scoping mistakes that derail compliance and growth • Identify the impact of technology and service providers on your scope and audit requirements • Develop your ability to understand the requirements intent and know where to find the best advice • Refine your PCI strategy and strengthen your security posture

Education Seminars	
<p>Orange Cyberdefense</p> <p>Don't let your security fall apart: PCI DSS, third-party software, and the Tetris effect!</p> <p>Nadav Shatz, Customer Solutions and Advisory Director, Orange Cyberdefense</p>	<p>Third-party security risks are one of the top threats to organisations. Within this, the risk posed by third-party software is constantly on the rise as a major emerging threat especially for organisations that develop and offer payment solutions.</p> <p>Now more than ever, the PCI DSS places an unprecedented focus on securing both custom and third-party software, including new, future-dated requirements set to come into effect early next year as part of PCI DSS v4.0.1.</p> <p>We will show:</p> <ul style="list-style-type: none"> • A real-life demonstration of a customer case, exploiting a third-party software vulnerability to not only gain control of account data but also to turn a POS terminal into a music player! • Explore and suggest solutions for properly addressing this threat, to secure payment environments and ensure compliance with the relevant requirements of PCI DSS v4.0.1.
<p>Patronusec</p> <p>Future of PCI Compliance</p> <p>Kris Olejniczak, CEO, Patronusec</p>	<p>Artificial intelligence is transforming the landscape of payments security. This includes the growing use of AI-driven tools that simplify compliance management, reduce operational complexity, and lower costs. However, the same advancements empower fraudsters and hackers, reshaping attack vectors and the overall threat landscape in payments security. AI is also redefining the role of QSA companies, enabling them to deliver assessments with greater focus on broader and more complex elements of compliance. Furthermore, as organisations increasingly explore processing cardholder data within AI and LLM-powered systems, the boundaries of PCI DSS scope are evolving, presenting new challenges and considerations.</p> <p>Attendees will learn:</p> <ul style="list-style-type: none"> • The shifting threat landscape as fraudsters leverage AI tools to enhance their capabilities • How organisations are utilising AI to streamline and enhance internal compliance processes • The evolving role of QSA companies in delivering more impactful and focused assessments • Key considerations for building AI-powered systems and specialised LLM models that process cardholder data while remaining PCI DSS compliant • Discussing the above through real-world experience and case studies

Education Seminars	
<p>PCI Pal</p> <p>Contact centre 101: Back to basics</p> <p>Geoff Forsyth, CISO, PCI Pal</p>	<p>A look at how PCI impacts MOTO payments as we dive deeper into issues with SAD storage, and explore scope reduction techniques such as IVR, DTMF masking, speech recognition, digital payments.</p>
<p>Red Sift</p> <p>Navigating SSL and email PCI DSS compliance with Red Sift</p> <p>Billy McDiarmid, Director of Solutions Engineering, Red Sift</p>	<ul style="list-style-type: none"> • Understanding PCI DSS compliance: Explore the latest updates to PCI DSS requirements and their implications for organisations • Certificates: Learn how compliance standards have evolved and the role of certificates in meeting these mandates • Email security as a key compliance driver: Learn how securing your email domain with solutions like DMARC, SPF, and DKIM contributes to PCI DSS compliance by protecting cardholder data from phishing and spoofing attacks • Data protection: Discover how Red Sift solution monitors and secures sensitive information across your digital footprint, supporting critical compliance mandates • Streamlining compliance efforts: See how automation and actionable insights from Red Sift simplify achieving and maintaining PCI DSS compliance
<p>Thales</p> <p>PCI DSS 4.0 compliance made easy with Thales</p> <p>Ketan Pyne, Pre Sales team for UK&I, Thales Group & Matthew Santos, Thales Group</p>	<ul style="list-style-type: none"> • Drawing on decades of experience helping banks and financial institutions comply with industry mandates, Thales offers integrated products and services that enable your organisation to protect stored cardholder data, encrypt it for transfer, restrict access on a need-to-know basis and protect applications managing payment transactions • Working with Thales can reduce the scope of your PCI DSS compliance burden.