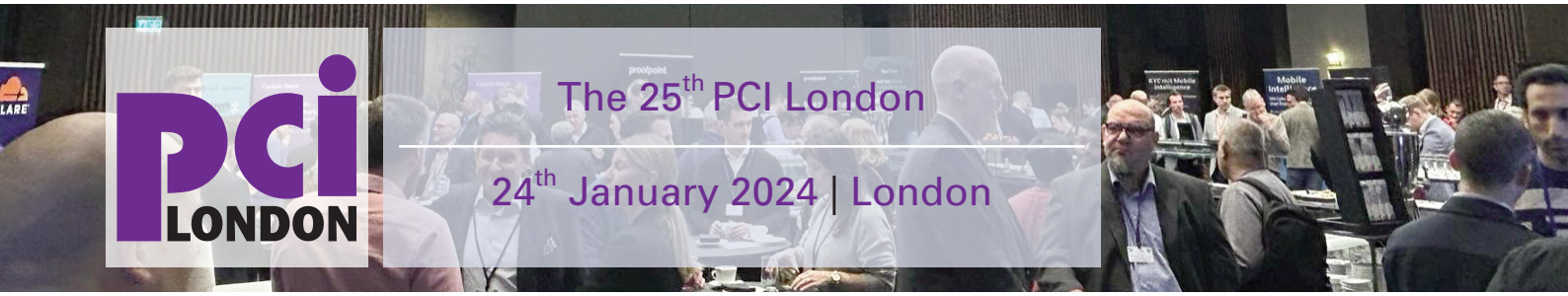
Post event report



Strategic Sponsors

blackfoot cybersecurity

GROUND LABS

HUMAN

Integrity360
your security in mind

jscrambler

Education Seminar Sponsors

cyber valley.

PCIpal

SureCloud.

Sycurio.

Networking Sponsors

orange Cyberdefense

reflectiz

silver lining
COMMUNICATION INNOVATION

VIKINGCLOUD™

Branding Sponsor

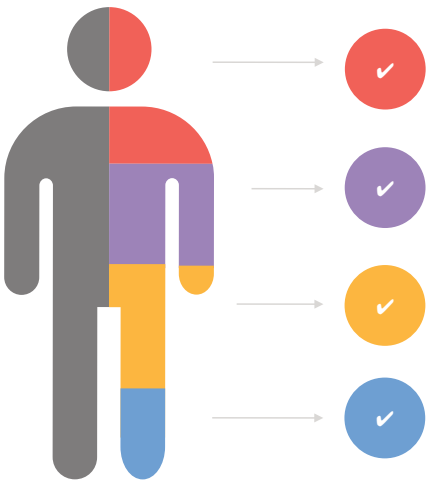
RED BUTTON
DDoS Experts

Inside this report:

Key themes

- Reducing the cost of PCI DSS compliance
- Sustaining selective, risk-based compliance
- Aligning PCI DSS, GDPR and other efforts
- Proving controls deliver secure outcomes
- New technologies – a challenge to compliance?
- Easing the transition to 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

Dhruv Bisani, Head of Adversarial Attack Simulations, Starling Bank

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

James Cullen, Principal Security Consultant, Lead QSA, SureCloud

John Elliott, Security Advisor, Jscrambler

Geoff Forsyth, CISO, PCI Pal

Richard Fridge, Enterprise Sales, HUMAN

Alex Gardner, Senior Product Marketing Manager, HUMAN

Michelle Griffey, GRC Director, Paragon

Keith Harper, Pre-Sales Engineer, Sycurio

Nicholas Howard, Director of Information Security, Reward Gateway

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

Anil Kumar, Head of IT Security, Risk and Compliance, Homebase

Parminder Lall, CEO and Founder, 1 Cyber Valley

Eleanor Ludlam, Partner – Cyber, Privacy and Technology Litigation, Pinsent Masons

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

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

Martin Petrov, CTO – PCI, Integrity360

Ahmed Rahman, CISO-Compliance Manager, Direct Line Group

Gaynor Rich, Former Deputy CISO, BT Group

Manit Sahib, Ethical Hacker, The Global Fund

Scott Storey, Cybersecurity Architect, University of Manchester

Simon Turner, Head of Security Governance and Compliance, BT Group

Jo Vane, InfoSec Compliance Director, Checkout.com

Soraya Viloria Montes de Oca, Group Information Security Officer, Harvey Nichols

Agenda	
08:00	Registration and networking break
09:00	Chairman's welcome
09:10	**PCI Security Standards: The latest developments in the payment space** **Jeremy King,** VP, Regional Head for Europe, PCI Security Standards Council • Version 4.0 transition timeline • Moving successfully to PCI DSS 4.0 • Steps to take in the next 6–9 months
09:30	**The challenges of managing e-commerce JavaScript** **John Elliott,** Security Advisor, Jscrambler • Managing JavaScript to meet the new requirements in DSS 4 is a challenge • The amount of JavaScript on websites is increasing, not decreasing • Optimising the business processes used to manage JavaScript is the only way to meet the new requirements • There isn't a one-size-fits-all solution for every organisation or for every script • It's important to understand what the standard asks for, not some people's interpretation of it
09:50	**Transitioning from PCI DSS v3.2.1 to v4.0: Navigating the changes and future-proofing compliance** **Martin Petrov,** CTO – PCI, Integrity360 This session provides an in-depth analysis of the transition from PCI DSS v3.2.1 to v4.0, focusing on key changes, effective strategies for outsourcing non-core security activities, and future-proofing against emerging security threats. Highlights include: • Overview of new and evolving requirements and their relationship to core business processes • The benefits of outsourcing in meeting the demands of an increasingly complex and rigorous standard • Strategies for outsourcing non-core security activities to improve security posture, reduce compliance costs, and increase efficiency • Best practices for ensuring continuous compliance in the dynamic payment security landscape Join us to gain insights and practical guidance on adapting to the evolving standards of PCI DSS and maintaining robust payment security.
10:10	**CASE STUDY** **From zero to hero, implementing a compliance framework for ISO27001, PCI DSS, SOC 2 Type 2 and Cyber Essentials Plus at a tech unicorn** **Nicholas Howard,** Director of Information Security, Reward Gateway • Journey from ISO to PCI to SOC 2 to CE+ • Using automation to streamline the ongoing monitoring, assessment and audit processes • Lessons learnt along the way
10:30	**Education Seminars | Session 1** **1 Cyber Valley** **Back to the future** **Parminder Lall,** CEO and Founder, 1 Cyber Valley **SureCloud** **PCI goals, timelines, myths: a QSA perspective** **James Cullen,** Principal Security Consultant, Lead QSA, SureCloud
11:10	Networking break
11:40	**PANEL DISCUSSION** **So you've lost cardholder data, what now?** **Eleanor Ludlam,** Partner – Cyber, Privacy and Technology Litigation, Pinsent Masons (Moderator); **Jo Vane,** InfoSec Compliance Director, Checkout.com **Soraya Viloria Montes de Oca,** Group Information Security Officer, Harvey Nichols **Michelle Griffey,** GRC Director, Paragon • It is impossible to guarantee 100% cardholder data security. So, if you do lose data, what are the key incident response and remediation priorities? • Identify how attackers are accessing your environment? • Determine how to mitigate attacker's existing access? • PR/legal responses?

Agenda

12:10 — How you can harness data discovery for sustainable compliance

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

Data discovery forms the foundation of scoping for PCI DSS compliance, but there are several pitfalls to the process that can leave organisations exposed, non-compliant and at risk of data breach. In this session, you'll learn:

- The ugly, the bad and the good of scoping for PCI DSS
- The dirty secrets of data discovery and how they could cost your compliance
- The dark places your data hides and how you can implement effective discovery practices to identify them
- The wider benefits of evidence-based discovery for PCI DSS compliance and beyond

12:30 — Education Seminars | Session 2

PCI Pal	Sycurio
The Cloud: Why it's the best place to achieve PCI DSS 4.0 **Geoff Forsyth,** CISO, PCI Pal	**Securing your payment infrastructure and delivering PCI DSS compliance with the acceleration in AI driven services** **Keith Harper,** Pre-Sales Engineer, Sycurio

13:10 — Lunch and networking break

14:00 — Moving parts around PCI: Centralising across technology, security and governance

Scott Storey, Cybersecurity Architect, University of Manchester

- Responding to crisis and accelerating the opportunity for change
- Aligning competing stakeholders
- Handling heritage and emerging technologies

14:20 — 6.4.3 & 11.6.1: The script to secure your browser scripts

Alex Gardner, Senior Product Marketing Manager, HUMAN & **Richard Fridge,** Enterprise Sales, HUMAN

Learn how to achieve and maintain compliance with PCI DSS 4.0 requirements 6.4.3 (authorise, justify, and assure the integrity of each payment page script) and 11.6.1 (alert to unauthorised modification to HTTP Headers in the consumer browser) while benefitting from the value of browser scripts.

- Understand the scope of requirements 6.4.3 and 11.6.1
- See how businesses can comply with the new requirements while securely benefitting from browser scripts
- Learn more about what to look for in a solution

14:40 — PCI DSS and quality third-party supplier relationships

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

Service providers are significant within the payment ecosystem, and their relationship with merchants is essential in the protection of cardholder data. The session will examine:

- Some of the common challenges and mistakes experienced by service providers and merchants from their respective sides
- PCI DSS v4.0, and real-life problems observed in the merchant/service provider relationship; where in a worst-case scenario, the service provider causes a merchant to be non-compliant

15:00 — Networking break

15:30 — PANEL DISCUSSION — PCI DSS-as-a-consequence of 'Secure in Operation': Striking the balance – Compliance-centric vs. Security-first strategies

Simon Turner, Head of Security Governance and Compliance, BT Group (Moderator);
Gaynor Rich, Former Deputy CISO, BT Group; **Anil Kumar,** Head of IT Security, Risk and Compliance, Homebase;
Ahmed Rahman, CISO-Compliance Manager, Direct Line Group;
Laura Morgans, Security Risk and Compliance Manager, Dr Martens, Airwair International Ltd

- Do alternative strategies, particularly security-first approaches aligned with frameworks like CIS or NIST hold the key to robust protection?
- The practical implications of compliance-led security, alternative strategies, the alignment with business objectives, ROI considerations
- The pivotal role of security leaders in addressing critical concerns
- Security-first strategy and the ability to comply with the multiple compliance requirements such as PCI DSS

16:00 — Bypassing multi-factor authentication (MFA) via phishing techniques

Manit Sahib, Ethical Hacker & **Dhruv Bisani,** Head of Adversarial Attack Simulations, Starling Bank

- Live demonstration of MFA bypass attack
- Countermeasures and best practices
- Conclusion of demo and presentation

16:30 — Drinks reception & networking

17:30 — Conference close

Education Seminars	
1 Cyber Valley **Back to the future** **Parminder Lall,** CEO and Founder, 1 Cyber Valley	Examining how credit card habits have transformed over the past two decades, which have resulted in the adaption of the PCI DSS standard. • What's happened in the payments industry in the last 20 years? • PCI DSS v4.0 – The new normal! • Explaining the key changes with v4.0 • The QSA's take on the new v4.0 • Predicting the future – Where is technology taking us in the next decade and how will PCI DSS adapt?
PCI Pal **The Cloud: Why it's the best place to achieve PCI DSS 4.0** **Geoff Forsyth,** CISO, PCI Pal	The PCI DSS v4.0 updated standard has changed the compliance landscape. In this session, Geoff Forsyth, CISO at PCI Pal, analyses how PCI DSS v4.0 affects achieving and maintaining compliance in the Cloud, why the cloud is the best place to achieve PCI DSSv4.0 and how descoping your infrastructure from the requirements of PCI DSS is still one of the most effective ways to protect your customers' data and your organisation's reputation. • Learn what it takes to design and deliver a global cloud platform for achieving PCI DSS compliance • Learn how PCI DSS v4.0 affects achieving and maintaining compliance in the cloud • Hear advice and considerations for embarking on your own cloud journey in the era of 4.0 • And a little bit about AI, as it's so trendy right now!
SureCloud **PCI goals, timelines, myths: a QSA perspective** **James Cullen,** Principal Security Consultant, Lead QSA, SureCloud	A quality security assessor (QSA)'s view of where we are, what to expect and what to do over the next few months. This session will cover: • Council objectives for PCI DSS version 4 • Timelines and how to prepare • Combatting myths about PCI DSS • The key requirements you need to know • How SureCloud can help
Sycurio **Securing your payment infrastructure and delivering PCI DSS compliance with the acceleration in AI driven services** **Keith Harper,** Pre-Sales Engineer, Sycurio	AI is changing the way organisations in every industry interact with customers and their data, particularly through its use in contact centres. From providing quicker, smoother customer experiences, powering self-service, delivering secure billing and payment solutions and augmenting agents, to cutting down on fraud risks, AI is revolutionising contact centre operations. As both customer and business needs evolve, the payments landscape, channels and services are expanding, necessitating heightened security and protection. Today, hosted AI services are making their way into the payment environment, introducing both opportunities and challenges. Inevitably there are challenges arising from the intersection of AI and PCI DSS compliance. AI services accessing open data sources offer increased efficiency and convenience, but this raises the question: Should we compromise on data security and privacy for the sake of convenience? Striking the right balance is crucial… join our session and discover: • AI's impact on your business, your payment environment and how you can navigate the changing landscape • Creating a harmonious balance between efficiency, convenience, and PCI DSS compliance when embracing AI services in the evolving payment ecosystem • Weighing up the benefits of open data sources against the imperative of safeguarding sensitive information • Why AI services which are accessing, processing and storing data from diverse sources will create complexities and concerns around data security and achieving and maintaining PCI DSS compliance • How to secure multiple payment channels and ensure PCI DSS compliance with AI 'blackbox' service vendors?