

Post event report



The 24th PCI London
25th January 2023 | London

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsor



“This was one of the best PCI London events I’ve been to. Many of the presentations were absolutely top class and lots of the speakers were animated, informed and provided valuable insight to all. It was great to be back in person too!”

Data Protection Officer

“Great to be back in person at another well organised event providing short, punchy and educational presentations from some quality speakers.”

Chief Compliance and Business Ethics Officer

Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Key themes

Reducing the cost of PCI DSS compliance

New technologies – a challenge to compliance?

Sustaining selective, risk-based compliance

Easing the transition to PCI DSS 4.0

Proving controls deliver secure outcomes

Aligning PCI DSS, GDPR and other efforts

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

Chris Brown,
VP, International Growth
Human Security

Matthew Browning,
Former Head of Cyber Oversight
Direct Line Group

Peter Craig,
Director of Cybersecurity
Product Marketing
Human Security

Matthew Davies,
VP of Product
SureCloud

Ian Davis,
Head of Information Security
Gemserv

James Devoy,
Managing Director EMEA
Online Business Systems

John Elliott,
Security Advisor
Jscrambler

Gil Fenney,
IT Risk Assurance Manager
Bupa

Geoff Forsyth,
CISO
PCI Pal

John Greenwood,
Director Thought Leadership
Compliance3

Michelle Griffey,
Chief Risk Officer
Communis

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

Alexander Norell,
Global Security Architect
VikingCloud

Scott Storey,
Digital Information &
Cybersecurity Manager
Parkdean Resorts

Simon Turner,
Senior Manager ISSCA
Consultancy Services,
BT Group

Jason Wallis,
Principal Consultant and lead PCI QSA
One Compliance

Agenda			
08:30	Registration and networking break		
09:30	Chairman's welcome		
09:40	PCI SSC: A new year, a new opportunity Jeremy King , VP, Regional Head for Europe, PCI Security Standards Council <ul style="list-style-type: none"> • Moving forward with PCI DSS v4 • PCI SSC launch mobile payments on COTS • Software Security Framework: Are you getting yours? • Launch of the new PO programme 		
10:00	Navigating the PCI DSS v4 supply chain and transitioning to the cloud Alexander Norell , Global Security Architect, VikingCloud <ul style="list-style-type: none"> • Navigating 3rd party software supply chain: How to maintain compliance • How to stay compliant with PCI DSS v4 and v3.2.1 service providers • Understanding the link between cloud services and PCI DSS compliance • Transitioning to serverless: What you need to consider in relation to PCI DSS 		
10:20	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Online Business Systems Digitally transforming PCI Scope – How COVID has driven change that can reduce your scope James Devoy, Managing Director EMEA, Online Business Systems </td> <td style="width: 50%; padding: 5px;"> PCI Pal Why the cloud is the best place to achieve PCI DSS 4.0 Geoff Forsyth, CISO, PCI Pal </td> </tr> </table>	Online Business Systems Digitally transforming PCI Scope – How COVID has driven change that can reduce your scope James Devoy , Managing Director EMEA, Online Business Systems	PCI Pal Why the cloud is the best place to achieve PCI DSS 4.0 Geoff Forsyth , CISO, PCI Pal
Online Business Systems Digitally transforming PCI Scope – How COVID has driven change that can reduce your scope James Devoy , Managing Director EMEA, Online Business Systems	PCI Pal Why the cloud is the best place to achieve PCI DSS 4.0 Geoff Forsyth , CISO, PCI Pal		
11:00	Networking break		
11:30	FIRESIDE CHAT Aligning PCI DSS, GDPR and other efforts Scott Storey , Digital Information & Cybersecurity Manager, Parkdean Resorts <ul style="list-style-type: none"> • Companies have spent significantly on PCI DSS, then poured more resources into GDPR and other compliance initiatives • What commonalities tie their different compliance goals together and which technologies can save them money while keeping them secure? • How can companies streamline their compliance efforts to optimise their use of resources? 		
12:00	Preventing skimming attacks, protecting customers, and enabling PCI DSS (and GDPR) compliance John Elliott , Security Advisor, Jscrambler <ul style="list-style-type: none"> • How do e-commerce skimming attacks (aka Magecart) work? • Where is the attack surface we can't control? • Understand the two requirements in version 4.0 designed to prevent and detect skimming attacks from one of the authors of PCI DSS • What should organisations do now to plan to meet the requirements? • As cardholder data is personal data, is there a GDPR compliance issue? 		
12:20	Education Seminars Session 2 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Gemserv Customised approach – benefits and drawbacks Ian Davis, Head of Information Security, Gemserv </td> <td style="width: 50%; padding: 5px;"> SureCloud Embedding PCI DSS into your organisation's security compliance programme Matthew Davies, VP of Product, SureCloud </td> </tr> </table>	Gemserv Customised approach – benefits and drawbacks Ian Davis , Head of Information Security, Gemserv	SureCloud Embedding PCI DSS into your organisation's security compliance programme Matthew Davies , VP of Product, SureCloud
Gemserv Customised approach – benefits and drawbacks Ian Davis , Head of Information Security, Gemserv	SureCloud Embedding PCI DSS into your organisation's security compliance programme Matthew Davies , VP of Product, SureCloud		
13:00	Lunch break		

Agenda	
14:00	<p>Effective security risk analysis – Why it is important to have a multi-faceted view?</p> <p>Michelle Griffey, Chief Risk Officer, Communisis</p> <ul style="list-style-type: none"> • Why understanding risk is everybody's role • Recognising how overlaps between different risk SME groups can give a better insight • Ensuring risk controls and mitigations don't become an obstacle
14:20	<p>PCI DSS 4.0 compliance is the starting point for website script security</p> <p>Chris Brown, VP, International Growth, and Peter Craig, Director of Cybersecurity Product Marketing, HUMAN Security</p> <ul style="list-style-type: none"> • 92% of companies lack visibility into 3rd party scripts • Understand how website payment scripts are vulnerable and how you can enable effective real-time monitoring for PCI compliance • Learn how to comply with PCI DSS 4.0 script visibility requirements and provide quality script management on all site scripts • Adopt a modern defence strategy to stay ahead of sophisticated and rapidly evolving digital attacks designed to evade detection • Discover solutions that extend beyond simply blocking scripts to stay protected and meet your business needs
14:40	<p>PCI DSS Compliance for Level 1 Merchants/Service Providers made simple</p> <p>Jason Wallis, Principal Consultant and lead PCI QSA, One Compliance</p> <ul style="list-style-type: none"> • First time PCI QSA engagement with Level 1 Merchants and Service Providers including the use of scoping workshops to identify key payment channels and scope reduction possibilities • PCI DSS SAQ equivalent assessments and how they can be used by Level 1 merchants and service providers to achieve PCI compliance • Creation of a 'PCI roadmap to compliance' and acquirer engagement to allow a merchant or service provider time to obtain full compliance across all payment channels • Ongoing PCI engagement requirements specific to the growth of a level 1 merchant or service provider
15:00	<p>Last stop approaching – all change here!</p> <p>Simon Turner, Senior Manager ISSCA Consultancy Services, BT Group</p> <ul style="list-style-type: none"> • We could think of our compliance endeavours with PCI DSS as a train journey, some of you may have been on this for a while whereas others may have only recently just embarked • Plan to transfer early at one of the minor stops, as this will give you some flexibility with time to deal with the unexpected • Can you shed some load as part of the transfer? • Make sure all of your party are equally prepared and stay together • Possibly look to improve your onward journey
15:20	Networking break
15:50	<p>EXECUTIVE PANEL DISCUSSION PCI DSS v4: Evolution, revolution or extinction?</p> <p>Moderated by Simon Brady, Managing Editor, AKJ Associates;</p> <p>Simon Turner, Senior Manager ISSCA Consultancy Services, BT Group;</p> <p>Gil Fenney, IT Risk Assurance Manager, Bupa;</p> <p>Michelle Griffey, Chief Risk Officer, Communisis;</p> <p>John Greenwood, Director Thought Leadership, Compliance3;</p> <p>Matthew Browning, Former Head of Cyber Oversight, Direct Line Group</p> <ul style="list-style-type: none"> • What are the pros and cons of moving to PCI DSS 4.0? • Does a risk-based approach to PCI DSS compliance imply non-compliance? • What's in a PAN? From payment instrument to personal data – PCI DSS. DPP7 and the rest • How do changes in technology affect the remit and application of PCI DSS 4.0?
16:30	Drinks reception
17:30	Conference close

Education Seminars	
<p>Gemserv</p> <p>Customised approach – benefits and drawbacks</p> <p>Ian Davis, Head of Information Security, Gemserv</p>	<p>The customised approach was introduced in PCI DSS v4.0 with the aim of providing organisations that already possess a mature risk-based environment the flexibility to use controls they may have in place to achieve PCI requirement objectives. During this session we review the customised approach, examine why an organisation may opt to use the customised approach over the more familiar defined approach, and discuss the challenges facing the QSA when either advising on or assessing compliance with PCI requirements. Delegates will learn from an experienced QSA Company what they will need to consider when deciding whether the customised approach is right for them or their customer.</p> <ul style="list-style-type: none"> • Overview on customised approach • Benefits and drawbacks of the customised approach • Examples of why the approach may work for some organisations • The Targeted Risk Analysis • Challenges faced by both QSAs and their customers
<p>Online Business Systems</p> <p>Digitally transforming PCI Scope – How COVID has driven change that can reduce your scope</p> <p>James Devoy, Managing Director EMEA, Online Business Systems</p>	<p>James will discuss a case study where a major car dealership had no choice but to embrace digital transformation and new customer engagement experiences to survive COVID. Coming out the other side, the organisation has also addressed issues it faced before COVID from the proliferation of Internet low margin vehicle sellers.</p> <p>James will discuss how a successful strategy cannot only offer a great customer experience, but also add new value to the sales channel, reduce personal data, and dramatically reduce the PCI DSS scope.</p> <ul style="list-style-type: none"> • Moving the payment experience away from Cardholder Present • Using custom mobile apps and payment links to reduce scope • Moving KYC and AML to third party to dramatically decrease stored personal data • Moving to subscription models to reduce card payments • Building natural language AI customer experience • Integrating with new partners, sharing the data responsibility whilst increasing sales figure
<p>PCI Pal</p> <p>Why the cloud is the best place to achieve PCI DSS 4.0</p> <p>Geoff Forsyth, CISO, PCI Pal</p>	<p>The compliance landscape has changed, with the release of the updated PCI DSS standard, PCI DSS v4.0. In this session, Geoff Forsyth, CISO at PCI Pal, analyses how the release of 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.</p> <ul style="list-style-type: none"> • Learn what it takes to design and deliver a global cloud platform for achieving PCI DSS compliance • Learn how the release of 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
<p>SureCloud</p> <p>Embedding PCI DSS into your organisation's security compliance programme</p> <p>Matthew Davies, VP of Product, SureCloud</p>	<p>Are you spending all your resources to sustain your Compliance programme? Security Executives face the day-to-day challenge of building, maintaining, and certifying multiple compliance programmes. Organisations must satisfy many information security, IT, and data privacy compliance requirements such as PCI DSS, ISO 27001, ISO 22301, GDPR, NIST 800-53, CMMC, etc.</p> <p>At the same time, are you struggling to unpick overlapping compliance requirements? Are you asking teams to repeatedly test and collect evidence for each regulatory requirement to demonstrate compliance? Could this process be automated through continuous control monitoring? There must be a more straight-forward way. This session will address the need to leverage technology to reduce your compliance burden and dynamically monitor compliance.</p> <p>Attend our session for a practical, how-to guide to:</p> <ul style="list-style-type: none"> • Simplify and streamline the management of compliance requirements • Map requirements to an aligned compliance framework • Embed a test once satisfy many requirements • Proactively monitor compliance requirements and build live compliance documentation