

Post event report



The 22nd PCI London^{VR}
30th June 2021 | Online

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors

Branding Sponsor

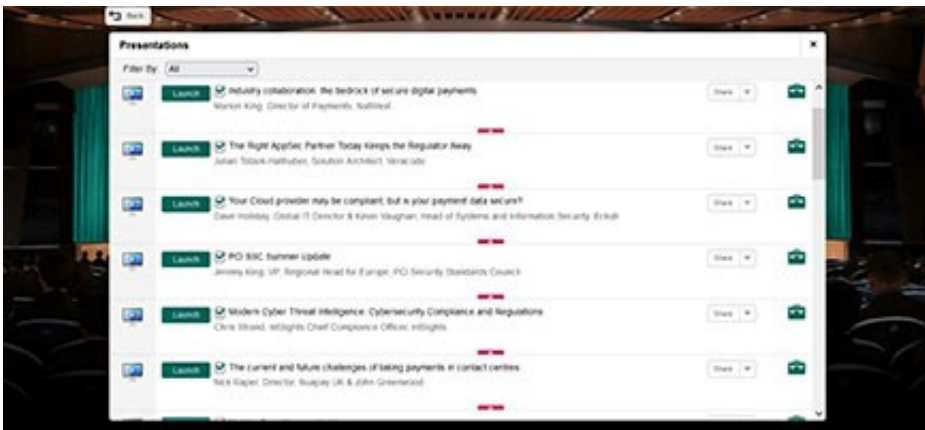


“ Thank you for this. I really did enjoy PCI London yesterday. Yet again, AKJ Associates produced an outstanding virtual conference. The speakers were first rate and the range of topics they covered were so varied that there was something for everyone. I was particularly glad to hear Jeremy King give 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

- Foiling card-based fraud
- Test, test and test again
- Securing the store
- Post-Brexit privacy problems
- Getting Cloud right
- Keeping up with the criminals
- Picking the right payments partners
- Accidents with apps and APIs
- Managing the security stack
- Authentication and access
- Why PCI DSS 4.0 matters
- Contact centre compliance

Who attended?



Speakers

- Debbie Bicker, Product Lead, **SVL**
- Simon Brady, Managing Editor, **AKJ Associates Ltd**
- Scott Bridgen, GRC Consulting Director, **OneTrust**
- Matthew Browning, Head of Cyber Oversight, **Direct Line Group**
- Graham Cluley, Security Analyst, **grahamcluley.com**
- Innes French, Data Protection Officer, **PCI Pal**
- Stephen Gardner, Managing Consultant, **Synopsis**
- Stuart Golding, PCI Compliance Manager, **Retail Organisations**
- Jane Goodayle, SVP Global Marketing, **PCI Pal**
- John Greenwood
- Michelle Griffey, Chief Risk Officer, **Communis**
- Dave Holliday, Global IT Director, **Eckoh**
- Kennet Johansen, Manager Solutions Engineering EMEA & APAC, **Netwrix**
- Marion King, Director of Payments, **NatWest**
- Jeremy King, VP, Regional Head for Europe, **PCI Security Standards Council**
- Jon Marler, Product Manager, **SecureTrust**
- Russell McDermott, Solutions Engineer, **Netwrix**
- Raghu Nandakumara, Field CTO EMEA, **Illumio**
- Peter O'Sullivan, Principal Security Consultant, **Nettitude**
- Candice Pressinger, Director of Customer Data Security, **Elavon**
- Rashpal Rai, Compliance Project Manager, **Bumble**
- Nick Raper, Director, **Nuapay UK**
- Martin Rolls, Consultant and Former Programme Director, Global Voice Development, BT on behalf of **Semafone**
- Chris Strand, Chief Compliance Officer, **IntSights**
- Julian Totzek-Hallhuber, Solution Architect, **Veracode**
- James Vale, Head of Payment Security Products & SME PCI DSS Compliance Programme, **Barclays**
- Kevin Vaughan, Head of Systems and Information Security, **Eckoh**

Agenda		
08:00	Login and networking	
08:50	Chairman's welcome	
09:00	Industry collaboration: the bedrock of secure digital payments	
	<p>Marion King, Director of Payments, NatWest</p> <ul style="list-style-type: none"> • Payments transformation – in a digital age customers expect frictionless, smart and SAFE payments • Addressing the balance of instant payments and the security and privacy of customer data • Collaboration – how to beat our common enemy – the fraudsters... 	
09:20	The right AppSec partner today keeps the regulator away	
	<p>Julian Totzek-Hallhuber, Solution Architect, Veracode</p> <p>The software supporting today's payment systems must be reliable and secure. Without secure payment platforms, payment transactions and data could be compromised.</p> <ul style="list-style-type: none"> • Learn how Veracode Static Analysis maps against PCI requirements • Learn how to determine which software security controls and features best serve your organisations specific business needs • Understand the importance of automated AppSec as a means of keeping up with the faster and more iterative payment systems of today • Gain best practice in setting up an effective application security programme with consideration for both traditional and modern payment platforms and evolving development practices 	
09:40	Your Cloud provider may be compliant, but is your payment data secure?	
	<p>Dave Holliday, Global IT Director, Eckoh, and Kevin Vaughan, Head of Systems and Information Security, Eckoh</p> <ul style="list-style-type: none"> • Who is responsible for payment data security – your cloud provider or you? • Which areas are left vulnerable after cloud contact centre implementation? • When managing third party and cloud risk, do generic infosec questionnaires cover what's needed? • How can you protect payment data in the cloud for long-term security and compliance? 	
10:00	PCI SSC summer update	
	<p>Jeremy King, VP, Regional Head for Europe, PCI Security Standards Council</p> <ul style="list-style-type: none"> • PCI DSS V4.0 latest news • PA DSS migration to Software Security Framework • Software Security Framework latest news • Training <ul style="list-style-type: none"> ◦ Informational training ◦ Work from home • Remote assessments • PCI at a glance 	
10:20	Education Seminars Session 1	
	<p>IntSights</p> <p>Modern cyber-threat intelligence: Cybersecurity compliance and regulations</p> <p>Chris Strand, IntSights Chief Compliance Officer, IntSights</p>	<p>Nuapay</p> <p>The current and future challenges of taking payments in contact centres</p> <p>Nick Raper, Director, Nuapay UK, and John Greenwood</p>
		<p>PCI Pal</p> <p>Making compliance a habit</p> <p>Innes French, Data Protection Officer, PCI Pal, and Jane Goodayle, SVP Global Marketing, PCI Pal</p>
10:50	Refreshments and networking	
11:20	Ghosts in the machine	
	<p>Graham Cluley, Security Analyst, grahamcluley.com</p> <p>In a series of real-life stories, computer security veteran Graham Cluley takes a look at the threats that should be giving you sleepless nights.</p> <ul style="list-style-type: none"> • Cyber-extortion and the future of ransomware • From fakes to deepfakes: pretending to be the government • Do you even know who your third parties are? • An employee spurned is a big security problem 	
11:40	PCI meets DevSecOps: Hazard or opportunity	
	<p>Stephen Gardner, Managing Consultant, Synopsys</p> <ul style="list-style-type: none"> • Under pressure to build software faster and cheaper, engineering teams are adopting DevOps • Does this ruin the pathway to application security, or does DevSecOps enable new efficiencies for security as well as engineering? • We'll discuss DevSecOps best practices, and how these align with application security elements of PCI, including PCI DSS requirement 6.3, the Software Security Framework, and the Secure Software Lifecycle 	
12:00	PCI DSS – Goldilocks and the three service providers?	
	<p>Peter O'Sullivan, Principal Security Consultant, Nettitude</p> <ul style="list-style-type: none"> • Is the information in the AoC too much, too little or just right? • Is your due diligence of service providers actually reducing your business risks? • Is the cloud your best friend or biggest enemy of the future – will it steal your porridge? 	

Agenda				
12:20	<p>Risk quantification – you are what you measure</p> <p>Scott Bridgen, GRC Consulting Director, OneTrust</p> <ul style="list-style-type: none"> Understand how you can use risk metrics as a planning tool beyond mitigation tactics Identify five simple steps to apply and guide your quantification strategy Account for the ‘new normal’ businesses are navigating for today and tomorrow Take a mixed approach to quantification to help retain qualitative risk insights 			
12:40	<p>Education Seminars Session 2</p> <table border="1"> <tr> <td> <p>IntSights</p> <p>Modern cyber-threat intelligence: Cybersecurity compliance and regulations</p> <p>Chris Strand, IntSights Chief Compliance Officer, IntSights</p> </td> <td> <p>Netwrix</p> <p>5 things you need to know to future-proof your data security today</p> <p>Russell McDermott, Solutions Engineer, Netwrix, and Kennet Johansen, Manager Solutions Engineering EMEA & APAC, Netwrix</p> </td> <td> <p>SVL</p> <p>Understanding PCI SSC 4.0’s impact on contact centres</p> <p>Debbie Bicker, Product Lead, SVL, and John Greenwood</p> </td> </tr> </table>	<p>IntSights</p> <p>Modern cyber-threat intelligence: Cybersecurity compliance and regulations</p> <p>Chris Strand, IntSights Chief Compliance Officer, IntSights</p>	<p>Netwrix</p> <p>5 things you need to know to future-proof your data security today</p> <p>Russell McDermott, Solutions Engineer, Netwrix, and Kennet Johansen, Manager Solutions Engineering EMEA & APAC, Netwrix</p>	<p>SVL</p> <p>Understanding PCI SSC 4.0’s impact on contact centres</p> <p>Debbie Bicker, Product Lead, SVL, and John Greenwood</p>
<p>IntSights</p> <p>Modern cyber-threat intelligence: Cybersecurity compliance and regulations</p> <p>Chris Strand, IntSights Chief Compliance Officer, IntSights</p>	<p>Netwrix</p> <p>5 things you need to know to future-proof your data security today</p> <p>Russell McDermott, Solutions Engineer, Netwrix, and Kennet Johansen, Manager Solutions Engineering EMEA & APAC, Netwrix</p>	<p>SVL</p> <p>Understanding PCI SSC 4.0’s impact on contact centres</p> <p>Debbie Bicker, Product Lead, SVL, and John Greenwood</p>		
13:10	Lunch and networking break			
14:00	<p>EXECUTIVE PANEL DISCUSSION PCI DSS 4.0: What do businesses need to know?</p> <p>PCI DSS v4.0 promises us a new and flexible approach to card data security. The updated standard will continue to provide the critical foundation for securing payment data whilst considering the rapidly developing payment technology ecosystem and evolving cyber-threat landscape. So, what do organisations need to prioritise? What are the challenges they are facing? And how are they proving the value of PCI 4.0 in the business?</p> <p>Matthew Browning, Head of Cyber Oversight, Direct Line Group Michelle Griffey, Chief Risk Officer, Communis Rashpal Rai, Compliance Project Manager, Bumble Chris Strand, Chief Compliance Officer, IntSights</p>			
14:20	<p>How micro-segmentation can help solve your PCI problem</p> <p>Raghu Nandakumara, Field CTO EMEA, Illumio</p> <ul style="list-style-type: none"> Organisations that process and store PCI data often find it challenging to define the scope of their PCI audit, which in turn leaves them at risk of being out of compliance with PCI DSS It can be hard to understand how micro-segmentation controls can assist with properly identifying what is in scope for PCI, establishing a boundary around these assets and limiting their exposure to other systems Zero-trust segmentation helps organisations achieve PCI compliance and provides better security for these high-value assets and the data that resides on them 			
14:40	<p>Card brands seek to eliminate anonymous adult content monetisation</p> <p>Jon Marler, Product Manager, SecureTrust</p> <ul style="list-style-type: none"> Mastercard sets new standards for monetising adult content How will these new rules impact the payment ecosystem? How do I protect my portfolio? 			
15:00	<p>Managing PCI DSS compliance in an era of digital transformation</p> <p>Martin Rolls, Consultant and Former Programme Director, Global Voice Development, BT <i>on behalf of Semafone</i></p> <ul style="list-style-type: none"> How enterprises can overcome the challenges that come with implementing complex digital transformation Best practices that can secure, PCI DSS compliant omnichannel payments in your business Future-proofing your contact centre and how to embrace changes in consumer behaviour How British Telecom worked with Semafone to transform their contact centres and enable their agents to take omnichannel payments 			
15:20	Refreshments and networking			
15:50	<p>Delegates will be able to choose from the following topics:</p> <table border="1"> <tr> <td> <p>How to avoid a call centre catastrophe</p> <p>Candice Pressinger, Director of Customer Data Security, Elavon</p> <ul style="list-style-type: none"> The latest card fraud risks to consider in the contact centre Descope to de-stress: simplifying compliance to reduce managerial headaches Outsourcing correctly: how to successfully manage third-party audits What does the future hold for card data security in the call centre? Hybrid models, cloud-based call centres and the IoT </td> <td> <p>PCI DSS accountability: The key to continuous compliance</p> <p>Stuart Golding, PCI Compliance Manager, Retail Organisations</p> <ul style="list-style-type: none"> Maintaining PCI compliance across the year between audits, and upholding documentary evidence to support it, is a key trend expected in PCI DSS V4.0 As compliance programmes move away from project-based work, to focus on maintenance, a different skill set is needed for PCI stakeholders to embed PCI DSS into the business New innovations and ways of taking payments require a ‘security-by-design’ approach, and a payment security culture championed by the PCI management team So, which business function should hold ultimate responsibility for PCI? What does effective board level buy-in look like? And how can cross-functional collaboration ensure organisations avoid compliance decline? </td> </tr> </table>	<p>How to avoid a call centre catastrophe</p> <p>Candice Pressinger, Director of Customer Data Security, Elavon</p> <ul style="list-style-type: none"> The latest card fraud risks to consider in the contact centre Descope to de-stress: simplifying compliance to reduce managerial headaches Outsourcing correctly: how to successfully manage third-party audits What does the future hold for card data security in the call centre? Hybrid models, cloud-based call centres and the IoT 	<p>PCI DSS accountability: The key to continuous compliance</p> <p>Stuart Golding, PCI Compliance Manager, Retail Organisations</p> <ul style="list-style-type: none"> Maintaining PCI compliance across the year between audits, and upholding documentary evidence to support it, is a key trend expected in PCI DSS V4.0 As compliance programmes move away from project-based work, to focus on maintenance, a different skill set is needed for PCI stakeholders to embed PCI DSS into the business New innovations and ways of taking payments require a ‘security-by-design’ approach, and a payment security culture championed by the PCI management team So, which business function should hold ultimate responsibility for PCI? What does effective board level buy-in look like? And how can cross-functional collaboration ensure organisations avoid compliance decline? 	
<p>How to avoid a call centre catastrophe</p> <p>Candice Pressinger, Director of Customer Data Security, Elavon</p> <ul style="list-style-type: none"> The latest card fraud risks to consider in the contact centre Descope to de-stress: simplifying compliance to reduce managerial headaches Outsourcing correctly: how to successfully manage third-party audits What does the future hold for card data security in the call centre? Hybrid models, cloud-based call centres and the IoT 	<p>PCI DSS accountability: The key to continuous compliance</p> <p>Stuart Golding, PCI Compliance Manager, Retail Organisations</p> <ul style="list-style-type: none"> Maintaining PCI compliance across the year between audits, and upholding documentary evidence to support it, is a key trend expected in PCI DSS V4.0 As compliance programmes move away from project-based work, to focus on maintenance, a different skill set is needed for PCI stakeholders to embed PCI DSS into the business New innovations and ways of taking payments require a ‘security-by-design’ approach, and a payment security culture championed by the PCI management team So, which business function should hold ultimate responsibility for PCI? What does effective board level buy-in look like? And how can cross-functional collaboration ensure organisations avoid compliance decline? 			
16:10	<p>Delegates will be able to choose from the following topics:</p> <table border="1"> <tr> <td> <p>The great PCI DSS conundrum: should I stay or should I go?</p> <p>Simon Brady, Managing Editor, AKJ Associates Ltd</p> <ul style="list-style-type: none"> Compliance in a world of omnichannel customers The practical realities of outsourced accountability Weighing the costs and benefits of compliance Should you be writing your own standards? </td> <td> <p>SMEs & PCI compliance: what’s next?</p> <p>James Vale, Head of Payment Security Products & SME PCI DSS Compliance Programme, Barclays</p> </td> </tr> </table>	<p>The great PCI DSS conundrum: should I stay or should I go?</p> <p>Simon Brady, Managing Editor, AKJ Associates Ltd</p> <ul style="list-style-type: none"> Compliance in a world of omnichannel customers The practical realities of outsourced accountability Weighing the costs and benefits of compliance Should you be writing your own standards? 	<p>SMEs & PCI compliance: what’s next?</p> <p>James Vale, Head of Payment Security Products & SME PCI DSS Compliance Programme, Barclays</p>	
<p>The great PCI DSS conundrum: should I stay or should I go?</p> <p>Simon Brady, Managing Editor, AKJ Associates Ltd</p> <ul style="list-style-type: none"> Compliance in a world of omnichannel customers The practical realities of outsourced accountability Weighing the costs and benefits of compliance Should you be writing your own standards? 	<p>SMEs & PCI compliance: what’s next?</p> <p>James Vale, Head of Payment Security Products & SME PCI DSS Compliance Programme, Barclays</p>			
16:30	Closing remarks, refreshments and networking			
17:00	Conference close			

Education Seminars	
<p>IntSights</p> <p>Modern cyber-threat intelligence: Cybersecurity compliance and regulations</p> <p>Chris Strand, Chief Compliance Officer, IntSights</p>	<p>Threat intelligence is normally used to enrich the process of security assessment, providing proof on the enforcement of security controls required to be secure and compliant. As threat intelligence technology evolves, it has become more valuable and instrumental to security audit, providing needed context to the process of gap analysis, data collection, threat identification, and prioritisation. During this session we will explore examples based on real world data where contextual threat intelligence can be applied directly to data security, compliance, and regulatory requirements in order to prioritise and accelerate the assessment process, obtain measure of business risk or liability, and reduce threats targeting the business.</p> <p>During the presentation, you will learn the following:</p> <ul style="list-style-type: none"> • What cyber-threat intelligence (CTI) is and why it is important for cybersecurity • How to use CTI to prioritise system security gaps and enhance security posture • How to examine your digital footprint in order to help predict targeted threat patterns • Understanding of how to use CTI findings to accelerate risk assessment
<p>Netwrix</p> <p>5 things you need to know to future- proof your data security today</p> <p>Russell McDermott, Solutions Engineer, Netwrix, and Kennet Johansen, Manager Solutions Engineering EMEA & APAC, Netwrix</p>	<p>What cyber-threats will your organisation face in the coming years? How can you protect your sensitive and business-critical data from malicious insiders, ransomware and targeted attacks, as well as human error? Discover 5 things that can help you orchestrate IT security with your data at its core, and get one step ahead of threats.</p> <ul style="list-style-type: none"> • Reduce the risk of data breaches • Gain better control over your IT environment • Learn the steps to build an intelligent roadmap for protecting your business
<p>Nuapay</p> <p>The current and future challenges of taking payments in contact centres</p> <p>Nick Raper, Director, Nuapay UK, and John Greenwood</p>	<p>This session provides some of the answer by looking at how we pay for goods and services now and how we will pay in the future.</p> <p>We then consider the customer contact centre operational possibilities to help entities reduce risk and cost whilst driving customer experience.</p> <p>The session will help attendees:</p> <ul style="list-style-type: none"> • Understand the current and future payments landscape • Understand the regulatory (as well as PCI DSS v4.0) drivers for change, including PCI DSS v4.0, SCA and Open Banking • Look at the operational benefits of aligning payments capability with your customer engagement strategy • Develop a pathway for change, reducing costs and reducing risk • Support payments transformation and prepare for a digital future
<p>PCI Pal</p> <p>Making compliance a habit</p> <p>Innes French, Data Protection Officer, PCI Pal, and Jane Goodayle, SVP Global Marketing, PCI Pal</p>	<p>According to Verizon, compliance with the PCI DSS has fallen for a third consecutive year, with many organisations ‘slipping up’ after the ‘all-important’ first audit.</p> <p>In this session, PCI Pal’s DPO, Innes French, talks with SVP Global Marketing at PCI Pal, Jane Goodayle, about why compliance is one habit that should be maintained all year round, not just seen as an annual event. And how businesses can build a compliant culture to achieve this.</p> <ul style="list-style-type: none"> • Why compliance rates continue to fall and why few organisations are able to keep a minimum baseline of security controls in place • How companies can turn compliance into a (good) habit • How to plan for the worse, in order to mitigate risk • How to make compliance ‘business as usual’ within your organisation

Education Seminars

SVL

Understanding PCI SSC 4.0's impact on contact centres

Debbie Bicker, Product Lead, SVL, and **John Greenwood**

If your contact centre supports customer payments and is faced with growing cost or revenue pressure (or both) then this session will be essential listening.

Come and join Debbie Bicker and John Greenwood in conversation and discover an approach to PCI compliance that will complement your existing digital transformation programme as well as reduce time, cost and effort to effectively support your customers.

The conversation covers:

- What the current guidance is actually defending
- The barriers to creating a hybrid contact centre operational model and meeting your PCI DSS compliance obligations
- Levering v4.0 opportunities
- Understanding the full scope of SCA and why we will need extra time to prepare