Post event report

Strategic Sponsors

2|SEC Consulting

Acuity Risk Management

ColorTokens

OneTrust Privacy Management Software

Zimperium Mobile Threat Defense

Education Seminar Sponsors

clearswift RUAG Cyber Security

CNS A Six Degrees Company

datadivider

illumio

netwrix

PCIpal

SecureTrust a Trustwave division

semafone securing data · protecting reputations

silver lining Communication Innovation

tripwire

Networking Sponsors

COMSEC Your Cyber Security Partner

Data Protection People

Gemserv

One Payment

WhiteSource

"I want to say thank you for a very professional, informative and enjoyable conference! Live discussions, great contacts, knowledge sharing between peers is priceless for me. All around it was very rewarding – thank you for including me."
PCI Officer, Swedbank

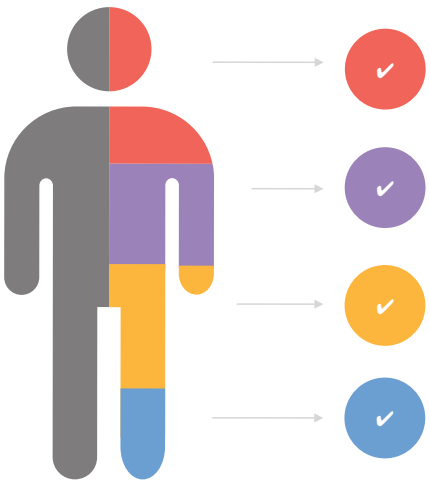
"Yet again I found PCI London really interesting and useful to me in my role. I will definitely be at the 20th edition next year."
Information Security Compliance Analyst, Virgin Trains

Inside this report:

Key themes

- Tracking and monitoring access
- Access automation and control
- Smart segmentation and scoping
- (Cost-)effective testing
- Securing payment innovations
- Automated compliance solutions

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

Adrian Beckham, Information Security Consultant, ASDA

Simon Brady, Managing Editor, AKJ Associates

Dr Guy Bunker, Chief Technology Officer, Clearswift

Dave Burleigh, Principal Consultant – UK and Ireland Global Compliance and Risk Services, SecureTrust

Efrain Castaneda, Global Privacy Researcher, OneTrust

Nick Clansey, PCI and ISA, The Open University

Geoff Forsyth, CISO, PCI Pal

David Froud, PCI Lead Consultant, 2|SEC Consulting

Charles Husbands, Head of PCI, Vodafone

Mark James, Compliance Principal, Silver Lining Convergence

Alan Jenkins, Head of Advisory Services, 2|SEC Consulting

Neira Jones, Independent Advisor & International Speaker

Jeremy King, International Director Europe, PCI Security Standards Council

Richard Kirk, Vice President EMEA, Illumio

Nick Lambert, Communications Director, Thoburns

Chris Leppard, Managing Consultant, CNS Group

Branko Lolich, PCI Project Manager, King's College London

Oussama Louhaidia, Head of Information Security, Curve

Simon Marvell, Partner, Acuity Risk Management

David Matthews, Vice President EMEA, ColorTokens

Russell McDermott, Solutions Engineer, Netwrix

Laura Morgans, Information Security, Risk & Compliance Manager, Which?

Yulia Nayda, Payments & Compliance Project Manager, Badoo

Colin Neale, Data Security Specialist, Netwrix

Paul 'PJ' Norris, Senior Systems Engineer, Tripwire

Allan Packer, Managing Director, Silver Lining Convergence

Dominic Paisley, Information Security Manager, London North Eastern Railway

Ashish Patel, VP Sales UK & Northern Europe, Zimperium

Ben Rafferty, Chief Innovation Officer, Semafone

Graham Thompson, VP Sales & Marketing, DataDivider

Jon Townsend, CIO, National Trust

Simon Turner, PCI DSS Compliance Manager, BT

Agenda

08:00 Breakfast networking and registration

08:50 Chairman's welcome

09:00 **The latest in PCI DSS**

Jeremy King, International Director Europe, PCI Security Standards Council

- Unadultered interpretation of the PCI DSS standard straight from the Council
- Highlighting the most pertinent changes since last year in PCI
- What does this mean for industry?

09:20 **PCI: A means to an end, not an end in itself**

Alan Jenkins, Head of Advisory Services, 2|SEC Consulting, and **David Froud,** PCI Lead Consultant, 2|SEC Consulting

- Compliance is not security, but a good compliance programme is an important foundation
- How PCI DSS can be used to kick-start a wider security programme
- Identifying and implementing the critical elements of PCI DSS

09:40 **Case study: Global retailer – from card data breach to PCI audit**

David Matthews, Vice President EMEA, ColorTokens

A talk through how we helped a customer out of a messy situation.

- Context and what did not work?
- Risk containment
- Identifying & isolating PCI in scope infrastructure
- PCI audit process – being ever ready

10:00 **EXECUTIVE PANEL DISCUSSION** **PCI within compliance**

Where does PCI DSS stand for the organisation's requirements, what are the appropriate PCI resourcing priorities for the senior compliance function?

Adrian Beckham, Information Security Consultant, ASDA
Laura Morgans, Information Security, Risk & Compliance Manager, Which?
Dominic Paisley, Information Security Manager, London North Eastern Railway
Jon Townsend, CIO, National Trust

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

Clearswift	Illumio	PCI Pal	Tripwire
Why digital imaging is the next generation threat to PCI compliance	**Using Zero Trust to match PCI compliance to the true threatscape**	**Compliance in the cloud – how PCI Pal met the compliance challenges of moving to the cloud**	**Three key challenges to being PCI 3.2 compliant and how to resolve them**
Dr Guy Bunker, Chief Technology Officer, Clearswift	**Richard Kirk,** Vice President EMEA, Illumio	**Geoff Forsyth,** CISO, PCI Pal	**Paul 'PJ' Norris,** Senior Systems Engineer, Tripwire

11:00 Morning break and networking

11:30 **Me and Mrs Jones: can RegTech solve the PCI DSS stalemate?**

Neira Jones, Independent Advisor & International Speaker; **Simon Brady,** Managing Editor, AKJ Associates

- Are the costs and complexity of the regulatory burden becoming unsustainable?
- The state of play in compliance automation/RegTech
- Can RegTech help boost PCI DSS compliance, make maintaining compliance easier and reduce the costs?

11:50 **Vendor risk management: Overcoming today's most common security & privacy challenges**

Efrain Castaneda, Global Privacy Researcher, OneTrust

- Review the drivers and challenges organisations face when managing third-party vendor risk
- Identify priorities before, during and after vendor procurement
- Take away a six-step approach for automating the third-party vendor risk lifecycle
- Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk

Agenda

12:10 — Quantifying the value of implementing PCI controls and measures

Simon Marvell, Partner, Acuity Risk Management

- Prioritising remediation of non-compliances in financial terms
- Cost benefit analysis on proposals for new security solutions
- Reporting on compliance and security risks in business language

12:30 — Education Seminars | Session 2

CNS Group	DataDivider	Netwrix	Silver Lining Convergence
Using Aegis (Cyber Security Maturity Benchmarking) to address PCI DSS assessment issues **Chris Leppard,** Managing Consultant, CNS Group	**Multifaceted payments** **Graham Thompson,** VP Sales & Marketing, DataDivider	**Back to data security basics: what's getting lost in all the buzz** **Colin Neale,** Data Security Specialist, Netwrix, and **Russell McDermott,** Solutions Engineer, Netwrix	**Privacy by Design & Default – 'Integrating GDPR and other regulation'** **Mark James,** Compliance Principal, Silver Lining Convergence, and **Allan Packer,** Managing Director, Silver Lining Convergence

13:10 — Lunch and networking

14:10 — EXECUTIVE PANEL DISCUSSION | PCI DSS under the microscope

Getting to grips with some of the most stubborn and difficult technical challenges of achieving and maintaining PCI DSS with PCI leaders from global brands.

Charles Husbands, Head of PCI, Vodafone
Simon Turner, PCI DSS Compliance Manager, BT
Branko Lolich, PCI Project Manager, King's College London
Nick Clansey, PCI and ISA, The Open University

14:40 — Mobile; Yes it is another endpoint!

Ashish Patel, VP Sales UK & Northern Europe, Zimperium

- Liberation at what price
- PCI requirements for mobile
- Compliance without compromising privacy

15:00 — Education Seminars | Session 3

Illumio	SecureTrust	Semafone
Using Zero Trust to match PCI compliance to the true threatscape **Richard Kirk,** Vice President EMEA, Illumio	**The hidden depths of PCI DSS** **Dave Burleigh,** Principal Consultant – UK and Ireland Global Compliance and Risk Services, SecureTrust	**Enabling secure and PCI DSS compliant payments across all your digital channels** **Ben Rafferty,** Chief Innovation Officer, Semafone

15:40 — Refreshments and Networking

16:00 — EXECUTIVE PANEL DISCUSSION | PCI resilience and optimum incident response

The reality is it's impossible to strike out the possibility of a breach, so having an airtight incident response plan is imperative. How do you stay ahead and limit damage?

Yulia Nayda, Payments & Compliance Project Manager, Badoo
Nick Lambert, Communications Director, Thoburns
Oussama Louhaidia, Head of Information Security, Curve
Jon Townsend, CIO, National Trust

16:30 — Outsourcing and insourcing – is it best to leave it to the pros?

Branko Lolich, PCI Project Manager, King's College London

- The best way for merchants to outsource payments processing payment card security
- Covering your PCI responsibilities as a merchant to facilitate the best collaboration with outsourced security teams
- Using PCI DSS requirements as a baseline to protect GDPR sensitive personal data

16:50 — GDPR one year on

Simon Brady, Managing Editor, AKJ Associates

- Enforcement – the real picture
- Costs versus benefits: is it worth it?
- After the transition, what now?

17:00 — Drinks reception and networking

18:00 — Close of conference

Education Seminars	
Clearswift **Why digital imaging is the next generation threat to PCI compliance** **Dr Guy Bunker,** Chief Technology Officer, Clearswift	Join us to discover why images are now one of the biggest unaddressed PCI compliance risks for financial organisations. We often do not give images a second thought, they are in presentations and documents all the time. But in today's world of digital collaboration, what sorts of risks can they pose? • Discover the next generation threats you need to be aware of • How to prevent digital images being the vector for APTs • Learn how to prevent unwanted data acquisition via digital images
CNS Group **Using Aegis (Cyber Security Maturity Benchmarking) to address PCI DSS assessment issues** **Chris Leppard,** Managing Consultant, CNS Group	• The issues faced with PCI – risk assessments, tracking policy and compliance • An overview of the Aegis Risk Management Platform – how organisations can understand their security posture and stance in granular detail • How the Aegis system can be used to provide a real in-depth view of the client environment – going beyond 'tick box' compliance • Examples of the scoring mechanism and reporting
DataDivider **Multifaceted payments** **Graham Thompson,** VP Sales & Marketing, DataDivider	Businesses are expanding their reach and their sophistication of payments. Historically, businesses operated payments for a single merchant ID through a single payment processor for their bricks and mortar, online and MOTO channels. Today, many businesses are extending their reach of payments into field operations and other utilisations of multi-device/mobile payments. Furthermore, businesses are interacting with multiple payment processors and across multiple merchant IDs within each processor. This coupled with the advantages of operating through payment processor independent tokens is increasing the sophistication of payments. This presentation addresses these requirements and how merchants can take advantage of a payment broker architecture, which facilitates the operation of payments across all channels through multiple payment processors. The presentation will look at field operation payments and the additional challenges where mobile devices with card readers operate in a challenging physical environment. This will include how businesses can provide resilient payments in these environments and ensure the ability to continue to take payments despite equipment or networking failures. Attendees to this presentation will gain from understanding: • How to expand the reach of payments within your business • The advantages of operating through multiple payment processors • Why businesses require multiple merchant IDs for a payment processor • Advantages of payment processor independent tokens • How a payment broker architecture works and the advantages delivered by such an solution • Challenges of field operations payments and how to provide resilient payments within such environments
Illumio **Using Zero Trust to match PCI compliance to the true threatscape** **Richard Kirk,** Vice President EMEA, Illumio	According to the 2018 Verizon Data Breach & Incident Report, there were 2,236 confirmed breaches in 2017. In many instances, these organisations had passed their PCI audits prior to the discovery of the breach. During this presentation, we will show how to effectively combine Zero Trust security with risk frameworks to align your PCI compliance with your true threat environment. More specifically we will cover: • The state of PCI compliance and breaches • Understanding your threat environment • How to disrupt lateral movement attacks • Segmentation with Illumio

Education Seminars	
Netwrix **Back to data security basics: what's getting lost in all the buzz** **Colin Neale,** Data Security Specialist, Netwrix, and **Russell McDermott,** Solutions Engineer, Netwrix	As data usage grows exponentially, many organisations are struggling with information security because they are short on time, money, staffing or all of the above. At the same time, the buzz from vendors about the latest attack vectors makes data security appear more complicated than it needs to be. This never-ending pursuit of defence against the hottest threats leads organisations to neglect basic aspects of data security, such as realising that not all data requires the same level of protection. In this session, we'll explain how getting back to basics can strengthen security controls and reduce the risk of breaches.
PCI Pal **Compliance in the cloud – how PCI Pal met the compliance challenges of moving to the cloud** **Geoff Forsyth,** CISO, PCI Pal	The cloud brings lots of advantages to businesses, but also lots of its own challenges. Geoff Forsyth, CISO at PCI Pal, discusses designing and delivering a global cloud platform for achieving PCI DSS compliance, with a focus on the compliance aspects of the build and considerations for companies when embarking on their own cloud journey. What attendees will learn: • How automation of cloud deployments can simplify compliance testing • How SMEs can piggyback on the security power of cloud platforms built to keep the likes of Netflix, Microsoft, Facebook and GSK secure
SecureTrust **The hidden depths of PCI DSS** **Dave Burleigh,** Principal Consultant – UK and Ireland Global Compliance and Risk Services, SecureTrust	There is a lot more to securing your customers cardholder data than just PCI, not least the provisions of the Data Protection Act (DPA) 2018. In this seminar, we will take a deep dive into the following: • 'Should we be doing more?' – what additional precautions are critical? • Securing a modern, multi-faceted, e-commerce programme • The hidden exposures it's easy to miss
Semafone **Enabling secure and PCI DSS compliant payments across all your digital channels** **Ben Rafferty,** Chief Innovation Officer, Semafone	Customers now want to engage with merchants across multiple digital engagement channels, such as webchat, IM & social media, email and more. For a superior customer experience, organisations should be able to communicate with customers in their channel of choice, without diverting them to alternative channels for payment. The challenge for organisations is to create a seamless and frictionless customer experience across all channels, while keeping secure and PCI DSS compliant.
Silver Lining Convergence **Privacy by Design & Default – 'Integrating GDPR and other regulation'** **Mark James,** Compliance Principal, Silver Lining Convergence, and **Allan Packer,** Managing Director, Silver Lining Convergence	'Privacy by Design' and 'Privacy by Default' have been frequently discussed topics related to data protection. The Information Commissioner's Office reminds us that "The GDPR requires us to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights". But what does the term 'Privacy by Design' mean practically? Is it more than data protection through technology design? Our educational seminar will cover: • What the ICO says – Accountability & Privacy by Default • The ethical & customer experience of AI so agents 'DO have to' • Considering the evolving landscape of regulation/technology • Developing a culture of compliance without risk

Education Seminars	
Tripwire **Three key challenges to being PCI 3.2 compliant and how to resolve them** **Paul 'PJ' Norris,** Senior Systems Engineer, Tripwire	Despite the benefits, compliance with PCI 3.2 is not without its challenges. The session will demonstrate how rather than a point-in-time approach to PCI compliance, it is important that organisations take the approach of continuous compliance, leveraging PCI not just for compliance purposes but actually as a means to improving security posture. This session will consider three key challenges: • Tedious audits • Configuration drift • Technical skills gap Join us to learn more, and explore how to: • Take advantage of digital channels to enhance your omni-channel strategy while increasing revenue and customer loyalty • Keep these channels secure and embrace big data, AI and machine learning technologies without compromising security or PCI DSS compliance • Avoid complicated e-commerce platforms, costly hardware or closed payment ecosystems, while simplifying your audit process and managing risk