Post event report

Strategic Sponsors

Pay360 by Capita

gemalto
security to be free

SRM
Smart Security. Smart Compliance.

Education Seminar Sponsors

ARMOR

barclaycard

δ/δ datadivider

Card Easy™
Keypad payment by phone
From Syntec

CRYPTOMATHIC

pcipal

TOKENEX

Networking Sponsors

Aeriandi
Voice Matters

blackfoot

it governance™

f5

Infradata

RIVINGTON INFORMATION SECURITY

semafone®
securing data · protecting reputations

silver lining
communication innovation

" I did find this event extremely well organised and all speakers and presentations were smooth and seamless. It was a pleasure to be there! I found it very thoughtful to have short seminars in between too. "
Risk and Compliance Manager, Wirex Ltd

" Another great PCI event with excellent speakers from various backgrounds and industries. Thought the panel discussions were particularly thought provoking and came away with lots of food for thought. "
Lead IT Auditor, Camelot Group

" Another worthwhile PCI London with plenty of insights on best practice to maintain compliance with PCI DSS as well as a look ahead to the future of payments, and emerging compliance and security benefits from AI technology. Well done. "
Head of Information Security, Travis Perkins

" As a project manager new to both PCI and GDPR, I found the PCI London seminar extremely useful. The speakers were informative and educational whilst the seminars provided an insight to real-life case studies from security professionals. A thoroughly interesting day. "
Project Manager, The Travel Corporation

Inside this report:

Sponsors

Who attended?

Speakers

Agenda

Education Seminars

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 Beeching, Business Development Director, Syntec

Manoj Bhati, Pre-Sales Consultant, Gemalto

Bruna Bonomi, Programme Delivery Director, Metropolis Group

Simon Brady, Managing Editor, AKJ Associates

Paul Brennecker, Principal QSA, SRM

Michael Christodoulides, VP Payment Security Product, Barclaycard

Crispin Edwards, VP, Barclaycard

Jon Forrow, Chief Information Security Officer, Mapfre Abraxas

Anne Godbold, Compliance and Regulatory Change Specialist, Accenture

John Greenwood, Consultant, Pay360 by Capita

Kurt Hagerman, CISO, Armor

Sarah Harvie, Head of Information Security, Merlin Entertainments

Nicholas Howard, Head of Information Security, First Rate Exchange Services

Dilshad Hussain, CEO, Universal Data Protection

William James, Head of Payments Team, Addleshaw Goddard

Neira Jones, Independent Advisor & International Speaker

David Mason, Senior Risk Manager, BGL Group

John Noltensmeyer, Head of Privacy and Compliance Solutions, TokenEx

Ninva Ponsonby, Former Group Head of Technology Compliance, OCS Group

David Porter, Head of Innovation, Security and Privacy, Bank of England

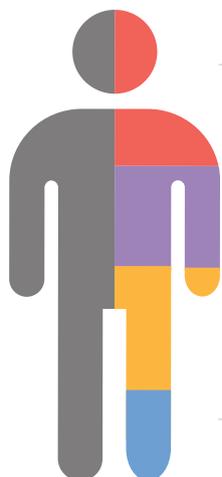Geoff Smith, Head of IT, The Works

Tony Smith, Director of Sales EMEA, PCI Pal

Rob Stubbs, Director of Sales EMEA, Cryptomathic

Graham Thompson, VP Sales and Marketing, DataDivider Inc

James Turrell, Business Information Security Manager, John Lewis Partnership

Sandip Zala, Director of Information Technology, Bulgari Hotels

Agenda

08:00	Breakfast networking and registration
09:00	Chairman's welcome

09:10	**CASE STUDY** **A PCI DSS and GDPR compliance journey**
	Nicholas Howard, Head of Information Security, First Rate Exchange Services
	• An in depth-case study on the implementation of PCI DSS and GDPR at First Rate Exchange Services
	• What went well, what were the biggest challenges we faced and how were these overcome
	• Synergies exploited and cost-effective compliance

09:30	**Real world encryption simplified**
	Manoj Bhati, Pre-Sales Consultant, Gemalto
	• Data economics
	• Compliance vs Security
	• PCI data security challenges and the changes that GDPR brings with it
	• Encryption in the real world – simplified

09:50	**Me and Mrs Jones: Busting the myths of PCI DSS and GDPR**
	Neira Jones, Independent Advisor & International Speaker; and **Simon Brady,** Managing Editor, AKJ Associates
	In this honest, high-calibre dialogue, Neira Jones, and Simon Brady, Managing Editor of AKJ Associates, will discuss what businesses really need to be aware of in the new security and compliance environment.
	• Is GDPR destined to be another PCI DSS – unenforced and with less than 50% compliance?
	• How can 'normal' companies realistically maintain PCI DSS/GDPR compliance in the Cloud?
	• Is mandatory disclosure the biggest risk (think Ticketmaster)?
	• Does companies' increased reliance on third-party payment platforms affect PCI DSS and GDPR compliance and security?

10:20	**Education Seminar	Session 1**	
	Armor	**Threat actors don't care if you're compliant** **Kurt Hagerman,** CISO, Armor
	Barclaycard	**Creating the right PCI environment** **Crispin Edwards,** VP, Barclaycard; and **Michael Christodoulides,** VP Payment Security Product, Barclaycard
	Cryptomathic	**My keys are safe … aren't they? Mitigating risks and achieving compliance** **Rob Stubbs,** Director of Sales EMEA, Cryptomathic
	DataDivider	**Leveraging your PCI DSS investment for GDPR** **Graham Thompson,** VP Sales and Marketing, DataDivider Inc
	PCI Pal	**Solving iFly's compliance challenges from the cloud: a case study** **Tony Smith,** Director of Sales EMEA, PCI Pal
	TokenEx	**Using tokenisation for data protection by design and by default** **John Noltensmeyer,** Head of Privacy and Compliance Solutions, TokenEx

11:00	Networking and refreshments break

11:30	**The future of payments: What's in store for 2019 and beyond?**
	William James, Head of Payments Team, Addleshaw Goddard
	• Alternative payments, blockchain, payment data intermediation: the payments landscape is changing quickly. What is happening and what is around the corner?
	• What should PCI professionals be aware of: insights from a payments industry expert
	• The challenge of PSD2 and Open Banking – more data more of the time?
	• Tokenisation and encryption vs friction free payments – reliance on PCI or technology based solutions?

11:50	**Aligning payments compliance strategy with digital transformation. Approach and key considerations.**
	John Greenwood, Consultant, Pay360 by Capita
	• Building on Pay360's previous presentations on the power of delivering payments in the digital channel and enabling payments innovation in the digital channel
	• How should entities approach PCI DSS compliance across their customer contact points?
	• What are the key considerations in approaching people, process and technology?
	• Where are the big gains in terms of technology selection and cost reduction?

Agenda

Time		
12:10	**Retained forensic & incident response service: How planning for the worst can add value to your business**	
	Paul Brennecker, Principal QSA, SRM	
	• Coping with the challenges of managing third parties to achieve and maintain compliance to data standards, particularly procurement • 'Plan for the worst but hope for the best' – this has never been so true as with incident response. Knowing how to react in the unfortunate event of a data breach is the biggest hurdle • How to plan ahead to ensure that you get the maximum return for your outlay and also secure the service that is best for your business	
12:30	**EXECUTIVE PANEL DISCUSSION**	**Preparing for annual assessments and audits**
	Bruna Bonomi, Programme Delivery Director, Metropolis Group **Jon Forrow,** Chief Information Security Officer, Mapfre Abraxas **Geoff Smith,** Head of IT, The Works	
12:50	**Education Seminar	Session 2**	
	Armor	**What GDPR means for the cyber underground** **Kurt Hagerman,** CISO, Armor
	Barclaycard	**Creating the right PCI environment** **Crispin Edwards,** VP, Barclaycard; and **Michael Christodoulides,** VP Payment Security Product, Barclaycard
	PCI Pal	**Solving iFly's compliance challenges from the cloud: a case study** **Tony Smith,** Director of Sales EMEA, PCI Pal
	Syntec	**How DTMF technology is becoming the new contact centre compliance standard, for payment by phone & call recordings** **Simon Beeching,** Business Development Director, Syntec
	TokenEx	**Using tokenisation for data protection by design and by default** **John Noltensmeyer,** Head of Privacy and Compliance Solutions, TokenEx
13:30	Lunch and networking	
14:30	**Ensuring PCI DSS and GDPR are aligned with business and customer needs**	
	Sandip Zala, Director of Information Technology, Bulgari Hotels	
	• Burgeoning information security compliance requirements can mean creating a balance between complying with regulation and business/customer needs • Making sure IT security works harmoniously with employees who need to access data • How a luxury hotel chain is securing guests' data, whilst also putting customer services and ease of use of IT systems as a priority	
14:50	**Solving the 'illusion of compliance' problem**	
	Ninva Ponsonby, Former Group Head of Technology Compliance, OCS Group	
	• How to create an organisational culture supportive of PCI DSS and GDPR compliance • Creating 'continuous compliance', rather than staff taking the view that it is an exam that needs to be passed • Can PCI DSS be used as a framework for GDPR? How should they be approached? • From PCI to the P&L: compliance is not just about avoiding cost, it is about driving revenues	
15:10	**EXECUTIVE PANEL DISCUSSION**	**A realist's guide to compliance**
	Sarah Harvie, Head of Information Security, Merlin Entertainments **David Mason,** Senior Risk Manager, BGL Group **James Turrell,** Business Information Security Manager, John Lewis Partnership	
15:30	Networking and refreshments break	
15:50	**Errare machinale est: from intelligence to resonance**	
	David Porter, Head of Innovation, Security and Privacy, Bank of England	
	Security leaders are being urged to be innovative and exploit the potential of artificial intelligence technology. But what is the reality behind the AI hype and where can such innovation take us?	
	• Innovation through structured experimentation • AI as a securely-harnessed and transparent capability • Better understanding non-compliance and artificial error	
16:10	**AI to comply: using technology capabilities like AI in regtech and the compliance effort**	
	Anne Godbold, Compliance and Regulatory Change Specialist, Accenture	
	• How can new technology capabilities like AI help the compliance effort • Case study: Using AI provided by a regtech to test and deploy an innovative financial crime surveillance solution • How to utilise these new capabilities to support wider compliance use-cases	
16:30	**People, policy, processes. Lessons in data governance, compliance and AI**	
	Dilshad Hussain, CEO, Universal Data Protection	
	• Data Governance & GDPR • Improve Business and IT collaboration in terms of compliance • Transformation programmes including digital, machine learning systems and AI. How can they balance this with compliance and regulations	

16:50	Closing remarks	17:00	Drinks reception	18:00	Conference close

Education Seminars

Armor

Threat actors don't care if you're compliant

Kurt Hagerman, CISO, Armor

Ever since men started crafting laws, there has been a constant conflict on how people carry out the 'letter of the law' such that it also achieves the 'spirit of the law' – which is to secure the data. Many compliance regulations lack specificity and don't fully address security. This results in an inherent conflict between security and compliance. Too often organisations prioritise compliance over security opting for a check the box approach, often resulting in bad outcomes.

In this session:

- Understand the fundamental differences between security and compliance
- Learn why you should put security first, especially with GDPR in effect, and how you can do it

Armor

What GDPR means for the cyber underground

Kurt Hagerman, CISO, Armor

Organisations in breach of GDPR can be fined €20 million or greater. That just gave threat actors holding your data – and your secret of having been breached – for ransom the perfect price.

In this session:

- Learn how the cyber underground economics work
- Understand the implications of cybercrime-as-a-service
- Take away measures to mitigate your risk

Barclaycard

Creating the right PCI environment

Crispin Edwards, VP, Barclaycard; and **Michael Christodoulides,** VP Payment Security Product, Barclaycard

Join us for this interactive session, hosted by Michael Christodoulides and Crispin Edwards from Barclaycard. During the session, attendees will learn about the top security challenges that customers are currently facing, and how they can protect themselves against these issues.

You will also discover:

- Why legacy systems could be your downfall
- Some of the threats you need to be aware of
- The real cost of a security breach to your company
- How an industry leading security strategy is easy to achieve

Cryptomathic

My keys are safe … aren't they? Mitigating risks and achieving compliance

Rob Stubbs, Director of Sales, EMEA, Cryptomathic

Businesses are becoming increasingly dependent on cryptography to protect their digital assets, communications and transactions. Whole new technologies, such as blockchain and IoT, utilise cryptography at their very heart. Cryptography, in turn, critically depends on the secure management of the underlying cryptographic keys. The compromise of just a single key could lead to a massive data breach with consequential reputational damage, punitive regulatory fines and loss of investor and customer confidence.

With the growing reliance on cryptography, the ever-present vulnerabilities in modern computing systems, the escalation of cyber attacks, and the demands of regulations such as PCI DSS and GDPR, it has never been more important, nor more challenging, to protect these keys.

What attendees will learn:

- The nature and life cycle of cryptographic keys
- How keys can be compromised
- The potential consequences of compromise
- Mitigating risks and achieving compliance

Education Seminars

DataDivider

Leveraging your PCI DSS investment for GDPR

Graham Thompson, VP Sales and Marketing, DataDivider Inc

This presentation addresses how organisations can leverage their PCI DSS investment when effectively and efficiently meeting their GDPR obligations. Most organisations have initially focused their GDPR projects in identifying the privacy data they manage and implementing the necessary opt-in policies together with the capabilities of privacy data disclosure to meet the GDPR requirements. Whilst this is definitely necessary unless this is coupled with implementing the security requirements for this privacy data the organisation is leaving itself exposed to a GDPR breach.

GDPR is not a prescriptive standard like PCI DSS so organisations have to determine themselves the necessary security controls that should be applied to protect privacy data. Organisations should be encouraged to deploy the same security controls they applied in securing sensitive cardholder data to GDPR privacy data. The presentation covers how the techniques to de-value data and de-scope PCI data can be applied to GDPR in order to minimise risk and reduce the implementation costs.

Furthermore, the presentation covers how end points that manage the capture and maintenance of privacy data can be secured in a manner that doesn't expose this privacy data to the local device. The presentation wraps up with some demonstrations on how end point devices can be best secured for GDPR.

Attendees to this presentation will gain from understanding:

- Why organisations should not be relying on existing security for GDPR privacy data
- How to de-value privacy data and de-scope infrastructure from GDPR
- Why applying the prescriptive PCI DSS security controls will aid GDPR success
- Why securing privacy data at end points simplifies GDPR

Attendees will have the opportunity to receive a 3,000 word detailed white paper on this subject.

PCI Pal

Solving iFly's compliance challenges from the cloud – a case study

Tony Smith, Director of Sales, EMEA, PCI Pal

In this session, we will share how we assisted iFly, the global indoor skydiving company, with their PCI compliance challenges whilst taking their customer experience to new heights.

What attendees will learn:

- The PCI compliance challenges faced by iFly
- How PCI Pal worked with iFly to achieve compliance and enhance CX
- Descoping for success
- Achieved results

Syntec

How DTMF technology is becoming the new contact centre compliance standard, for payment by phone & call recordings

Simon Beeching, Business Development Director, Syntec

De-scoping the contact centre environment from PCI DSS controls, ensuring MOTO card payments are fully secure and also helping with GDPR – from a leading QSA and managed services provider.

What attendees will learn:

- The regulatory and compliance challenge in call centres – a real world QSA view
- How to reduce the on-going burden of compliance
- Freeing yourself from PCI audits, monitoring and controls for the contact centre, call recordings, remote workers & outsourcers
- Improving customer experience and trust
- With case studies and merchant feedback

Education Seminars

TokenEx

Using tokenisation for data protection by design and by default

John Noltensmeyer,
Head of Privacy and Compliance Solutions, TokenEx

Join TokenEx Head of Privacy and Compliance Solutions, John Noltensmeyer, to learn how you can reduce risk, achieve PCI compliance, and meet your obligations under the GDPR for 'data protection by design and by default' by tokenising sensitive data at the point of acceptance, while still supporting day-to-day business processes. Organisations are securing PCI data using tokenisation as well as protecting personal data using pseudonymisation.

This session will showcase how you can secure both card payment and personal data across all your data acceptance channels – websites, web services, batch files, contact centres, and more.

What attendees will learn:

- How cloud-based vs. on-premise tokenisation affects PCI compliance and reduces data security risk
- The benefits of tokenisation at the 'point of acceptance'
- How to implement tokenisation across an omni-channel environment
- Ways tokenisation can be used for pseudonymisation of personal data
- Where pseudonymisation can be used to help meet GDPR data and privacy requirements