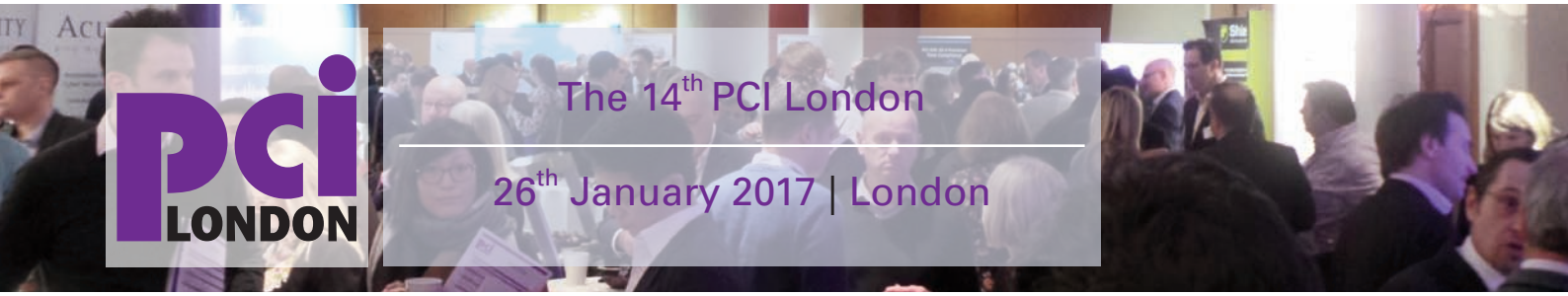
Post event report



Strategic Sponsors

blackfoot
ips International Payment Services
SRM Cyber Security Suppliers to HM Government
silver lining communication innovation

Education Seminar Sponsors

Aeriandi
ARMOR
datadivider
DATAMATICS Data to Intelligence
Foregenix
GROUNDLABS
observe it
SIRIUM SECURE · SCALE · SIMPLIFY
PCIpal
SIS
Card Easy Keypad payment by phone From Syntec
tripwire CONFIDENCE: SECURED
Trustwave Smart security on demand

Networking Sponsors

2SEC
ACUITY RISK MANAGEMENT
comforte
COMSEC Consulting UK Cyber & Information Security
Eckoh
ecsc more secure
NTA FORENSICS
mastercard payment gateway services
Pay360 by Capita
PHOENIX DATACOM NETWORK PERFORMANCE AND SECURITY
spectracom
securityMETRICS
semafone securing data · protecting reputations
ShieldQ Delivering data compliance
ultracomms

Branding Sponsor

IRM INFORMATION RISK MANAGEMENT

Website Sponsor

GROUNDLABS

“As usual PCI London provided insightful sessions, excellent networking opportunities, and a focused selection of exhibitors offering PCI related products and services. With industry attention now on GDPR, the content allowed attendees to position PCI compliance as a building block to meeting the latest regulations. Unmissable!”

Head of Information Security, Travis Perkins

“Informative, interesting, intriguing, inspirational. The speakers and break-out sessions were excellent, as was the overall theme of the conference. A well organised event and one to which I will definitely plan to return.”

Information Security Manager, Coventry Building Society

“I found the PCI London 2017 event a great stage for learning more about the impact that the changes in regulations, legislation will be having, not only on the payment card industry but in general for all businesses. The presentations were good and presented a good mix of organisations. The ability to talk with vendors in a non-pressured environment and network with other likeminded individuals from different companies was an opportunity that doesn't happen on a day to day basis. For this alone it is very valuable.”

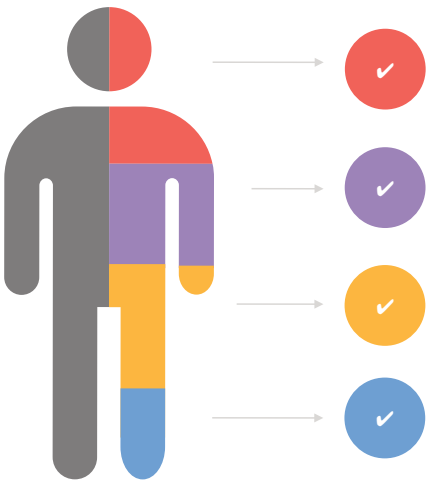
Information Security Manager, Teleperformance

Inside this report:

Key themes

- Latest contact centre challenges
- Improving internal awareness
- Understanding the small print of new regulation
- Maintaining compliance through automation
- Coping with contactless

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

James Barham, Divisional Managing Director, PCI Pal

Simon Beeching, Business Development Director, Syntec

Andrew Bontoft, Director, Foregenix

Paul Brennecker, Principal Information Security Consultant, SRM

Matthew Bryars, CEO and Co-founder, Aeriandi Ltd

John Cassidy, Global Head of Sales, Ground Labs

Kevin Dowd, Syntec's QSA

Vincent Di Giambattista, Former Director Information Security and IT Compliance, Walgreens Boots Alliance

John Elliott, Head of Payment Security, easyJet

Gill Fenney, Senior Information Security Consultant, ASDA

Andrew Fletcher, Customer Solutions Director, IPS; and Stuart Golding, Consultant, IPS

Andy Harris, Engineering Director, Osirium

Mark James, PCI Contact Compliance specialist, Silver Lining Convergence Ltd

Neira Jones, Independent Advisor & International Speaker, Strategic Advisor, Cognosec

Rodney Julius, Security Operations Analyst, Boden

Jeremy King, International Director, PCI Security Standards Council

Tracey Long, Senior Payment Security Manager PCI DSS Compliance, Worldpay

Dave Lund Yates, Deputy Head of Income (Payment Strategy and PCI DSS Compliance), University of Southampton

Alexander Norell, Director of Global Compliance and Risk Services, EMEA, Trustwave

Paul 'PJ' Norris, Senior Systems Engineer, Tripwire

Micky Oland, Director of Product Management, ObservelT

Simon Price, Global PCI Lead, BP

Jeff Schilling, Chief of Customer Operations and Security, Armor

Tony Smith, Head of Enterprise Sales, PCI Pal

Graham Thompson, Sales & Marketing Director, DataDivider Inc

Matthew Tyler, CEO, Blackfoot UK

Robert Walker, Managing Director, AKJ Associates

Peter Wignall, Director of SIS Retail

Agenda

08:00	Registration
08:50	Conference welcome
09:00	**An introduction to the PCI London Awards** **Robert Walker,** Managing Director, AKJ Associates
09:20	**Magecart: Industrialised malware targeting direct post and other 'out of scope' implementations** **John Elliott,** Head of Payment Security, Easyjet • e-Commerce architectures susceptible to attack • Giving your consumers browser-based malware: How the magecart attack works • Practical steps you can take to defend yourself
09:40	**Understanding the true nature of changing payment providers** **Andrew Fletcher,** Customer Solutions Director, IPS; and **Stuart Golding,** Consultant, IPS • Understanding what needs to be changed – planning for success • Areas for consideration – what areas merchants should consider when changing provider • Choosing the right solution to meet your needs
10:00	**PCI DSS – incident response and forensic readiness** **Paul Brennecker,** Principal Information Security Consultant, SRM • If your systems/networks were hacked, would you know and how would you respond? • Prepare – a PCI compliant infrastructure will reduce the likelihood of an attack • Respond – an effectively designed incident response framework will dramatically increase the effectiveness of any forensic investigation, saving significant amounts of time, effort and money during the recovery from an incident • Recover – rapid implementation of incident response processes will ensure minimal impact on your day to day business operations
10:20	**Education Seminars | Session 1**

Aeriandi	**Detect fraud on your telephone channel whilst achieving PCI compliance** **Matthew Bryars,** CEO and Co-founder, Aeriandi Ltd
Armor	**The evolution of ransomware** **Jeff Schilling,** Chief of Customer Operations and Security, Armor
Ground Labs	**Preparing for GDPR – real business strategies for GDPR implementation** **John Cassidy,** Global Head of Sales, Ground Labs
ObservelT	**Puff! The abracadabra of transforming your employees from being your weakest security link into your strongest compliance custodians. And how to pave an effective internal culture towards GDPR compliance** **Micky Oland,** Director of Product Management, ObservelT
Tripwire	**PCI 3.2 and the regulation storm: Thinking beyond the checkbox** **Paul 'PJ' Norris,** Senior Systems Engineer, Tripwire
Trustwave	**P2PE, NESA and E2EE update** **Alexander Norell,** Director of Global Compliance and Risk Services, EMEA, Trustwave

11:00	Refreshments and networking break
11:30	**Me and Mrs Jones: Exposing the truths of PCI** **Neira Jones,** Independent Advisor & International Speaker, Strategic Advisor, Cognosec In this honest, high calibre dialogue, Neira Jones and Simon Brady, Managing Editor of AKJ Associates will discuss key issues, and the need-to-know solutions of PCI. The discussion will then be open to the floor, giving delegates a chance to interact, and be part of this important information sharing session.
11:50	**PCI in the contact centre: What's the big deal?** **Mark James,** PCI Contact Compliance specialist, Silver Lining Convergence Ltd • Live PCI solution demo: Keeping it simple • Analysing de-scoping customer trends across business environments with real world examples • The challenge and implications of PCI DSS • Investigating elements for driving a comprehensive security programme • Using telephony infrastructure knowledge to increase the benefits of strategic collaboration
12:10	**New kids on the block: PCI DSS is joined by raft of emerging regulations** **Tracey Long,** Senior Payment Security Manager PCI DSS Compliance, Worldpay • How will these potentially affect our customers, and how does this overlap with PCI DSS? • Uncertain times: What next – is this the end of PCI DSS? • If only I had a crystal ball: What impact are the new and emerging regulations going to have on the payments ecosystem?

Agenda

12:30	**Education Seminars | Session 2**	
	Armor	**Cloud security roadmap: Mitigating risks and building for long-term success** **Jeff Schilling,** Chief of Customer Operations and Security, Armor
	Ground Labs	**Preparing for GDPR – real business strategies for GDPR implementation** **John Cassidy,** Global Head of Sales, Ground Labs
	PCI Pal	**Real world challenges of PCI compliance in multi-channel contact centres** **James Barham,** Divisional Managing Director, PCI Pal
	SIS Retail	**Can store PCI DSS and P2PE PIM compliance procedures ever really be effective?** **Peter Wignall,** Director of SIS Retail
	Syntec	**Contact centre de-scoping. Research, advice and case studies from a leading QSA and hosted systems provider** **Simon Beeching,** Business Development Director, Syntec; and **Kevin Dowd,** Syntec's QSA
	Trustwave	**PCI DSS 3.2 update** **Alexander Norell,** Director of Global Compliance and Risk Services, EMEA, Trustwave
13:10	Lunch and networking	
14:10	**EXECUTIVE PANEL DISCUSSION** | **PCI and the retail Industry: What you need to know**	
	Simon Price, Global PCI Lead, BP **Gill Fenney,** Senior Information Security Consultant, ASDA **Rodney Julius,** Security Operations Analyst, Boden	
14:30	**2017 and beyond. PCI in an increasingly challenging world**	
	Matthew Tyler, CEO, Blackfoot UK • A look back at key events in 2016 • The Brexit effect and a peek at the challenges ahead • PCI 2017 and beyond	
14:50	**Why would you not want to be compliant?**	
	Dave Lund Yates, Deputy Head of Income (Payment Strategy and PCI DSS Compliance), University of Southampton • Where did we start? • We'll take the 'risk-based' approach – or will we? • What have we done? • Where are we now?	
15:10	**Education Seminars | Session 3**	
	DataDivider	**PCI DSS is dead, long live PCI DSS** **Graham Thompson,** Sales & Marketing Director, DataDivider Inc
	Foregenix	**Incident readiness: A perspective from the field** **Andrew Bontoft,** Director, Foregenix
	Osirium	**Good digital hygiene is key to delivering PCI compliance** **Andy Harris,** Engineering Director, Osirium
	PCI Pal	**Customer experience versus compliance the perennial struggle!** **Tony Smith,** Head of Enterprise Sales, PCI Pal
15:50	Refreshments and networking break	
16:10	**Security and PCI DSS compliance for e-commerce**	
	Vincent Di Giambattista, Former Director Information Security and IT Compliance, Walgreens Boots Alliance • External threat landscape and dark web monitoring • Business requirements and expectation • Key success factors to build and maintain a secure and compliant website	
16:30	**Bridging the gaps: The PCI community and cross-continental influences**	
	Jeremy King, International Director, PCI Security Standards Council • Latest developments in the USA and what that means for the future of PCI • The PCI community: How does America affect Europe and what can we learn from each other? • Solutions and international information sharing: What do you need to know, and what's around the corner	
16:50	Closing remarks by AKJ Associates	
17:00	Conference close and drinks reception	

Education Seminars

Aeriandi

Detect fraud on your telephone channel whilst achieving PCI compliance

Presenter: Matthew Bryars, CEO and Co-founder, Aeriandi

What attendees will learn:

- Leverage the telco integration beyond PCI to reduce fraud
- Lockdown the telephone gateway to reduce e-commerce fraud
- Contact centre fraud statistics

Armor

The evolution of ransomware

Presenter: Jeff Schilling, Chief of Customer Operations and Security, Armor

If the threat landscape of 2016 proved anything, it's that ransomware is here to stay. And worse yet, we have yet to glimpse the full potential of this efficient, and possibly lethal tactic. But how did a software that originated with small-time threat actors looking to exploit vulnerable individuals grow into one of the, if not the most, significant cyber threat facing organisations today? Join Jeff Schilling, CISM, Armor, for an exploratory session on the evolution of ransomware from petty crime to something that should be keeping both security and business leaders up at night as well as techniques to protect yourself.

What attendees will learn:

- How ransomware became a household name
- Why every organisation, and everyone for that matter, is a target
- What security leaders need to do if they hope to keep their data safe

Armor

Cloud security roadmap: Mitigating risks and building for long-term success

Presenter: Jeff Schilling, Chief of Customer Operations and Security, Armor

Let your inner control freak go. The 'we control everything' security strategy does not apply to the cloud, especially not multi-cloud. How do you prevent the loss of sensitive data while enjoying the cost reduction and flexibility a multi-cloud strategy can bring? Join Jeff Schilling, CISM, Armor, to learn how you can embrace a cloud security roadmap and achieve your multi-cloud objective.

What attendees will learn:

- How to build your comprehensive cloud security strategy
- How to ensure a consistent security posture across multiple clouds
- How to evaluate your cloud security investment in 2017

DataDivider

PCI DSS is dead, long live PCI DSS

Presenter: Graham Thompson, Sales & Marketing Director, DataDivider Inc

This presentation explores the impact of the issuer driven initiates for Dynamic CVV and 3D Secure 2.0 will have to current and future merchant invests in PCI DSS. Having looked at the mechanics of Dynamic CVV the presentation then looks at payment work flows with for both Cardholder Present (CP) and Cardholder Not Presentation (CNP) transactions. With these understood we look at the roll out and timelines for global adoption.
Next we look at 3D Secure 2.0 and what benefits that is brings in reducing risk to cardholder data. How will the authentication of devices and the optional challenge capabilities lead to more frictionless payments and risk based authorisations? We then investigate if and when cardholder data becomes devalued to fraudsters and look at the reduced effort to achieve PCI DSS as standard evolves to reflect the benefits in such an ecosystem.

Finally the presentation wraps up on the merits of the security controls required to evidence compliance with PCI DSS and how these same controls can be reused to evidence the privacy and protection of all personal data in a wider context than cardholder data. Lessons learned within PCI DSS including from tokenisation and reducing scope will be explored in terms of protecting privacy data. A demonstration will be provided on how desktops and networks where critical privacy information is captured and transmitted can be secured in a manner to take the desktop and network out of the controls scope.

What attendees will learn:

- How exactly will Dynamic CVV operate in both CP and CNP environments?
- How and when this issuer-led initiate of Dynamic CVV will be rolled out across the globe
- What capabilities will be provided with 3D Secure 2.0 and how will these contribute to frictionless payments?
- How will Dynamic CVVs and 3D Secure 2.0 eliminate the value of cardholder data to fraudsters?
- What will be the impact to PCI DSS if and when cardholder data becomes de-valued to fraudsters?

Education Seminars	
Foregenix **Incident readiness: A perspective from the field** Presenter: Andrew Bontoft, Director, Foregenix	Statistics show that the average time between the point of compromise to the point of incident detection is 5.5 months. With considerable volumes of payment card and customer personal information being stolen, victim organisations face expensive and disruptive mitigation and financial penalties. In this session, Andrew will provide insight into bridging the gap between compromise to detection, along with recommendations from one of the leading digital forensics teams. What attendees will learn: • A view into incident response: Only a very small number of hacked organisations have been found to have an effective, well-tested incident response plan in place • The consequences of not prioritising incident response: Challenges to decision making, confusion, unnecessarily slow response times and increased financial pressures • Solutions: How to form an efficient and effective incident response plan and what you need to know when doing so
Ground Labs **Preparing for GDPR – real business strategies for GDPR implementation** Presenter: John Cassidy, Global Head of Sales, Ground Labs	PCI and GDPR compliance is mandatory (GDPR legislation comes into force May 2018) – failure to comply with these standards can result in hefty fines; PCI fines from $5,000 to $100,000; GDPR fines can reach up to 4% of global annual turnover. And of course, getting hacked is a costly affair – the average cost per record lost is $194. Even losing a few thousand records is enough to bankrupt a small-sized company. Compliance is not a one-time event, it's your responsibility to keep it going. On the positive end, there are companies that have managed to get compliant in a matter of months. These companies see the value in compliance, understand what PCI and GDPR is about, and work together as a team to make data security a company-wide priority. Companies like that not only get compliant fast, but are able to stay compliant by securing sensitive data and reducing risk of a data breach. Find out how you can achieve this with minimum effort and maximum efficiency. What attendees will learn: • The relationship between PCI DSS and GDPR • Challenges associated with finding and securing data • Roadmap to GDPR compliance for your business • Practical advice on making GDPR part of your core business
ObserveIT **Puff! The abracadabra of transforming your employees from being your weakest security link into your strongest compliance custodians. And how to pave an effective internal culture towards GDPR compliance** Presenter: Micky Oland, Director of Product Management, ObserveIT	The traditional corporate approach of providing employees with introductory security-policy training, and thereafter relying on their memory and collective 'goodwill', has been shown to be ineffective in upholding PCI and other critical compliance regulations. The task of enforcing internal compliance policies is wrought with challenges, largely due to the inherent human factor. Whether through genuine mistakes, negligence, or a lack of awareness, your internal employees, privileged users, and third-party contractors are prone to violate company policies. In addition, employees often find themselves trapped into performing tasks without the necessary tools or resources, leading to actions that put their organisation at risk. How can you effectively prevent user-based risks to your business using minimal resources and time? What attendees will learn: • Facilitate automated bi-directional communication with your employees including real-time, notifications about out-of-policy activities • Obtain online, valuable feedback from employees that will assist in minimising future PCI and other compliance breaches • Reduce ongoing costs associated with PCI and respond to your two key PCI auditing queries: 'Who did what?' • Implement internal processes and tools to ensure an easy and effective route towards GDPR compliance

Education Seminars	
Osirium **Good digital hygiene is key to delivering PCI compliance** Presenter: Andy Harris, Engineering Director, Osirium	These days it's easier to fool the wetware rather than the software. What attendees will learn: • Separate people from passwords (they can't reveal what they don't know) • Identify people needing access to your PCI systems • Automate the Password Life Cycle for compliance • Build in continuous monitoring as per PCI DSS
PCI Pal **Real world challenges of PCI compliance in multi-channel contact centres** Presenter: James Barham, Divisional Managing Director, PCI Pal	What attendees will learn: • The scope for contact centre customer interaction impacted by PCI • Why is the contact centre environment important in the overall picture? • Outsourcing card data protection to technology services providers • Delivering a PCI de-scoping project – have you given it enough thought?
PCI Pal **Customer experience versus compliance the perennial struggle!** Presenter: Tony Smith, Head of Enterprise Sales, PCI Pal	Traditionally there is always a conflict between offering a great customer experience (CX) and being compliant but does that necessarily have to be the case? What attendees will learn: • What consumers expect in terms of customer experience • Why Omni Channel is a must • Don't forget the agent • How to use compliance to enhance the customer experience
SIS Retail **Can store PCI DSS and P2PE PIM compliance procedures ever really be effective?** Presenter: Peter Wignall, Director of SIS Retail	Are store Pin Entry Device checks & Chain of Custody (CoC) processes giving us a false sense of confidence? Are we sleep-walking into non-compliance and in-store data breaches: What's the reality? Whether you are a tier 1 retailer implementing a P2PE solution or a tier 3 enterprise with bank-owned payment terminals, Section 9 of PCI DSS requires you to periodically check your PEDs for potential compromise and to adhere to the chain of custody requirements. This session looks at what is really happening in store estates, what the key factors for this are and what could be done to increase the level of confidence that adequate checks are being performed and CoC processes are being strictly adhered to. What attendees will learn: • The key requirements for PED checking and Chain of Custody • The key issues preventing stores from performing effective PCI compliance checks and strict chain of custody processes • The risks of failure • What can be done to improve the situation

Education Seminars	
Syntec **Contact centre de-scoping. Research, advice and case studies from a leading QSA and hosted systems provider** Presenters: Simon Beeching, Business Development Director, Syntec; and Kevin Dowd, Syntec's QSA	What is today's best practice to ensure MOTO card payments in call centres are compliant? And how can you de-scope the whole call centre environment, including agents; home/remote workers; outsourcers; PCs; network; screen & call recordings? What attendees will learn: • The PCI DSS challenge in call centres – a real world QSA view • Potential solutions and their associated issues and challenges • De-scoping your contact centre, call recordings and remote workers from PCI DSS, avoiding partial solutions such as 'clean rooming' and 'pause & resume' • How to reduce the on-going burden of compliance • Research highlighting that consumers want new technology to prevent fraud • Syntec's CardEasy 'keypad payment by phone' DTMF payment options: Mid-call/live in conversation with the agent; and/or Autopay customer self-service IVR (including video demo) • Hosted versus on-premise and other flexible deployment options • Protecting the customer experience and improving customer trust – case study feedback
Tripwire **PCI 3.2 and the regulation storm: Thinking beyond the checkbox** Presenter: Paul 'PJ' Norris, Senior Systems Engineer, Tripwire	There is never a dull moment for compliance and security. Case in point, amidst a brewing storm of regulation (think GDPR), version 3.2 of the PCI DSS announced in late spring of 2016 articulates good data security intent that goes beyond checkbox compliance. In this session, learn how to move your organisation beyond a compliance mentality into risk-based security and see how selecting foundational controls can make PCI DSS compliance easier. Passing PCI compliance can be a painful experience. According to Verizon's 2015 PCI report, only 9% of breached organisations were compliant with Requirement 11 – a fundamental requirement that ensures that an organisation is prepared for a range of attack types. Does your organisation have the change detection requirement under control? Join Tripwire's Senior Systems Engineer, Paul 'PJ' Norris in a session reviewing the latest updates in PCI 3.2 and learn how to go beyond the checkbox to easily achieve continuous compliance. What attendees will learn: • The latest updates in PCI 3.2 • The top 3 mistakes that provide PCI pain and how to avoid them • The PCI and CIS Critical Controls overlap • How implementing foundational controls can make PCI DSS compliance easier • Practical guidelines on how technology can help achieve PCI compliance and support continuous compliance • Live POS demo showing credit card malware at work and more
Trustwave **P2PE, NESA and E2EE update** Presenter: Alexander Norell, Director of Global Compliance and Risk Services, EMEA, Trustwave	This session will cover the latest developments and the crucial need-to-knows about P2PE updates and statistics. Any business that stores, processes or transmits cardholder data is required to be PCI compliant. Like any compliance regime, the PCI DSS can be complex and difficult to manage. Understanding of integral P2PE NESA and E2EE solutions and updates is important for any organisation taking PCI DSS seriously. What attendees will learn: • P2PE solution, component and application validation • P2PE from a merchant perspective • NESA – Non-Listed Encryption Solutions Assessment – how will NESA help you as a solution provider and how will NESA affect the scope of PCI DSS for a merchant

Education Seminars	
Trustwave **PCI DSS 3.2 update** **Presenter:** Alexander Norell, Director of Global Compliance and Risk Services, EMEA, Trustwave	As promised, the Payment Card Industry Security Standards Council (PCI SSC) recently released version 3.2 of its payment card requirements. This release is arguably more significant for the way it is being introduced and the underlying message than for the changes themselves, which are few and have been recommended security best practices for some time. This session will explore the recent PCI DSS 3.2 update, the key highlights of PCI DSS 3.2 and their impact on you. What attendees will learn: • e-Commerce insights – Using re-direct or iFrame from your e-commerce site to your payment service provider? The latest updates and clarifications on how PCI DSS 3.2 affect e-commerce merchants • Multifactor authentication – have you planned the implementation on multifactor authentication that will become mandatory on 1st February 2018? Insights on how the new requirements affect your environment • PCI SSC – guidance for PCI DSS scoping and network segmentation – what does PCI DSS say about the scope and what does the new guidance mean to you?