Post event report

Strategic Sponsors

blackfoot

BULLET PROOF

THE BUNKER Arcturus
Part of the CYBERFORT group

Education Seminar Sponsors

Data Protection People

datadivider

Eckoh

GROUND LABS

PCIpal

SureCloud

Card Easy™
Keypad payment by phone
From Syntec

TOKENEX

Networking Sponsors

ecsc more secure

GO ANYWHERE®
A HelpSystems Solution

netwrix

semafone®
securing data · protecting reputations

silver lining
COMMUNICATION INNOVATION

SRM
Smart Security, Smart Compliance.

ultracomms

Branding Sponsor

SecureTrust™
a Trustwave® division

"PCI London was yet another highly enjoyable and informative day. There were some lively discussions around the challenges of PCI compliance, and useful education sessions covering encryption, tokenisation etc which gave some great insight into controls not only for card data, but for wider data security as well. Great chance to catch up with peers in the industry and share thoughts and ideas."

Bupa Global – Security Expert

"This was the first PCI event that I have been able to attend and I didn't know what to expect. My only real aims were to take away a few points from the presentations and speak to likeminded people about the current challenges facing the PCI community. When Jon Hawes kick-started the day in tremendous fashion with his rollercoaster paced delivery, I could see looking around the room that there was a real buzz amongst the audience. I had not expected so much crossover with GDPR during the agenda; however, it was all relevant and if anything reinforced the need to collaborate or closely align with more internal departments owning those responsibilities."

Information Systems Security Analyst, SGBD UK IT Security

"Great event with a very warm and welcoming atmosphere. Lots of professionals attending who seem passionate about what they do – a great networking opportunity."

DPO – The Institution of Engineering and Technology

"It was a brilliant hosted event, with a diverse range of speakers, topics and formats. All this provided a wide range of insight for me into PCI, and really helped with my knowledge of the Regulation."

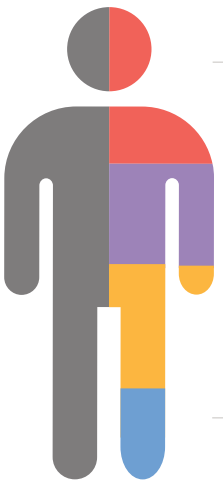
QVC, Senior Security Engineer

Inside this report:

Key themes

- Demonstrating the value of your PCI programme
- Dealing with growing pains
- Descoping – the holy grail of compliance?
- Building integrated GDPR/PCI DSS frameworks
- Automating compliance at scale
- One size fits none

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

Trevor Axiak, Director
Kyte

Simon Brady, Managing Editor
AKJ Associates

John Cassidy,
Director of Corporate Development
Ground Labs

Dan Chapman, GDPR Manager
bet365

Thomas Chappelow,
Principal Consultant, PCI and Information Security
Data Protection People

Tim Gillott, Head of Compliance
Atos

Jon Hawes, Head of Detect
Photobox

Gary Hibberd, Managing Director
Agenci – part ofThe Cyberfort Group

Paul Holland,
Information Security Leader
Hiscox

Alex Hollis, GRC Practice Director
SureCloud

Charles Husbands,
PCI Programme Manager
Vodafone

Neira Jones, Independent Advisor & International Speaker

Phil Jude,
Strategic Partnerships Manager
PCI Pal

Jeremy King,
International Director – Europe
PCI Security Standards Council

John Noltensmeyer,
Head of Privacy and Compliance Solutions
TokenEx

Oli Pinson-Roxburgh, Managing Director
Bulletproof

Tony Porter, Head of Global Marketing
Eckoh

Bob Spence, Head of Projects
Syntec

Graham Thompson,
VP Sales & Marketing
DataDivider

Matthew Tyler, CEO
Blackfoot UK

Steve Wright, GDPR Advisor to the
Bank of England

Stuart Wright,
Principal Programme Manager
lastminute.com

Agenda

08:00 Breakfast networking and registration

09:00 Chairman's remarks

09:20 **A strategy to protect your business against more than an auditor**

Jon Hawes, Head of Detect, Photobox

- Why delivering business value from security spend and explaining what this thing called 'cyber''means to the Board is hard
- How to build a security strategy and operational plan that shows you are in control of your situation and priorities, (as well as helping you negotiate budget and resources)
- 3 practical examples of how this works in the real world: how to execute on what matters and stay sane while you're doing it

09:40 **PCI and compliance: the customer doesn't always know best**

Dan Chapman, GDPR Manager, bet365

- Data privacy challenges. How to balance information security, business efficiency and customer demands
- The fines aren't fine. What is the real impact of organisations being threatened by regulators' fines. How will it affect disclosure? Are the fines too little too late? Or not enough?
- Customer data = customer loyalty. Data privacy as a competitive advantage that can win, or lose you business

10:00 **PCI in the brave new world of data protection, regulation and law suits**

Matthew Tyler, CEO, Blackfoot UK

- The UK HMG's 5-year digital strategy
- What the implications are for UK organisations
- How PCI fits into the picture
- How to take a holistic approach

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

Eckoh	PCI Pal	SureCloud	TokenEx
How broad should your de-scoping be?	**The compliance challenge**	**PCI & beyond**	**Best practices for PCI scope reduction and ongoing compliance**
Tony Porter, Head of Global Marketing, Eckoh	**Phil Jude,** Strategic Partnerships Manager, PCI Pal	**Alex Hollis,** GRC Practice Director, SureCloud	**John Noltensmeyer,** Head of Privacy and Compliance Solutions, TokenEx, and **Trevor Axiak,** Director, Kyte

11:00 Networking and refreshments

11:30 **Some things are worth waiting for**

Jeremy King, International Director – Europe, PCI Security Standards Council

- Updated guidance document for protecting telephone-based payments
- PCI SSC priorities for 2019 – including details of new standards and programmes

11:50 **Compliance vs reality**

Oli Pinson-Roxburgh, Managing Director, Bulletproof

- Through dissecting real attacks, what are the key failings that allow hackers to get through and has this changed over time or are we still seeing the same things?
- From Bulletproof's position as both an attacker and a defender, what are we seeing? (often hackers go after the same things, which we see in our daily alerts from our SIEM)
- Where does compliance fit into all of this?
- Compliance has to evolve along with the challenges. Being compliant as it stands, whilst beneficial, does not mean a company is 100% secure

Agenda

12:10 — PCI compliance war stories

Gary Hibberd, Managing Director, Agenci – part of The Cyberfort Group

- V for vulnerability – how do you know where you are most vulnerable? It might not be where you think
- We can do IT – why IT is important, but not the whole story in your PCI DSS armoury
- Keep calm and carry on – how to respond effectively when bad things happen
- Loose lips, sink chips – what policies should look like to improve security
- Your company needs you – importance of engaging with the whole organisation to protect you

12:30 — Education Seminars | Session 2

Data Protection People	DataDivider	Ground Labs	Syntec
Service providers and security: a sanity check **Thomas Chappelow,** Principal Consultant, PCI and Information Security, Data Protection People	**The impact of the new PCI SSC Information Supplement on Telephone Payments** **Graham Thompson,** VP Sales & Marketing, DataDivider	**Data discovery: The key to customer integrity** **John Cassidy,** Director of Corporate Development, Ground Labs	**Managing execution risk in contact centre PCI projects** **Bob Spence,** Head of Projects, Syntec

13:10 — Lunch and networking

14:10 — Me and Mrs Jones: 2019 – the inconvenient truths of PCI DSS

Neira Jones, Independent Advisor & International Speaker; **Jeremy King**, International Director – Europe, PCI Security Standards Council; and **Simon Brady,** Managing Editor, AKJ Associates

14:50 — It's all about you: aligning PCI with your business priorities

Paul Holland, Information Security Leader, Hiscox

- How managing regulatory compliance can also help improve your operational resilience
- How security differs across different businesses and why this is important
- How can compliance help drive risk appetite?
- Aligning PCI with your business priorities. How this helps

15:10 — Education Seminars | Session 3

Ground Labs	PCI Pal	TokenEx
Data discovery: The key to customer integrity **John Cassidy,** Director of Corporate Development, Ground Labs	**The compliance challenge** **Phil Jude,** Strategic Partnerships Manager, PCI Pal	**Continuous PCI and GDPR compliance with data-centric security** **John Noltensmeyer,** Head of Privacy and Compliance Solutions, TokenEx

15:50 — Networking and refreshments

16:20 — EXECUTIVE PANEL DISCUSSION — Why is PCI DSS compliance so hard and what to do about it?

Charles Husbands, PCI Programme Manager, Vodafone

Stuart Wright, Principal Programme Manager, lastminute.com

Tim Gillott, Head of Compliance, Atos

Graham Thompson, VP Sales & Marketing, DataDivider

16:40 — Setting your own standards: how well are you really doing?

Steve Wright, GDPR Advisor to the Bank of England

- Maintaining an established governance structure and working with regulators and requirements, both for your business and your customers
- Verifying and monitoring of information security protocols
- Adhering to a company-wide data breach response programme. Security and compliance metrics and benchmarking

17:00 — Drinks reception

18:00 — Conference close

Education Seminars

Data Protection People

Service providers and security: a sanity check

Thomas Chappelow, Principal Consultant, PCI and Information Security, Data Protection People

The past 12 months have been called the year of breaches. Data exfiltration attacks that have been attributed to vulnerabilities in third-party code, used within the cardholder data environment of many high-profile merchants, have led many to question, 'how secure can we expect service providers to be?'

Join a QSA for a seminar covering:

- The scoping game: who is and isn't a service provider
- AOC roulet: what a compliant service provider looks like
- Trust or not to trust: deciding whether to take compliance at face value, or to perform additional vetting
- Checks and balances: ensuring security after compliance

DataDivider

The impact of the new PCI SSC Information Supplement on Telephone Payments

Graham Thompson, VP Sales & Marketing, DataDivider

While Jeremy King, the International Director – Europe PCI Security Standards Council, presents the highlights from the PCI SSC's Information Supplement on Telephone Payments, this presentation looks at the detailed impact this guidance document will have on merchants and importantly on their telephony service providers. Long in the waiting this document has serious implications for many merchants as the SSC now provides explicit details on what exactly is in scope for telephone payments.

Attendees to this presentation will gain from understanding:

- Where to look at their potential exposures within their PCI DSS compliance of Telephone Payments
- Why third-party management of outsourced service providers will become critical
- How to determine if a merchant's carrier/hosted telephony provider is in scope for PCI DSS
- What DTMF bleed is and why this potentially brings DTMF tone masking back into PCI DSS scope
- Why historic call recordings with cardholder data will now need to be managed for PCI DSS
- The impact of taking payments through Chat channels

Eckoh

How broad should your de-scoping be?

Tony Porter, Head of Global Marketing, Eckoh

Today, customers expect to be able to engage with an organisation using their channel of choice. They also expect to be able to shift channels throughout the engagement. At the same time, they also want to make sure that their data remains secure when making a payment on the telephone, web, SMS, Chat or eWallets such as Apple Pay, Google Pay and PayPal.

As organisations lock down online and POS payment processing, the Omni-Channel contact centre remains a target for criminals seeking to exploit CNP fraud, which currently costs UK consumers some £409m each year (*Source:* UK Finance 2018).

New vendors entering the PCI DSS market are offering to secure payments, making broad promises about descoping, but to what degree? SAQ A or SAQ D. In Eckoh's experience these promises can be thin, and conveniently, they often rely on compensating controls which, it could be argued, do not constitute de-scoping at all.

Recent research from Contact Babel showed that the majority of compliant organisations are using at least three methods to maintain compliance, none of which on their own would do the job. It also makes the compliance process more complicated. But, compliance doesn't always equal security and the best way to reduce the risk of fraud, or the impact of a data breach, is to make sure that your de-scoping goes as deep as possible.

In this session you'll find out...

- How to identify and review your customer engagement channels
- Understand the impact of these on your PCI DSS scope
- How you can ensure your de-scoping has the breadth it needs.

Eckoh's solutions help reduce the time and effort required to attain PCI DSS compliance and maintain it year on year. As the solutions work with any technology and telephony channel (SIP or PSTN) they can de-scope an entire contact centre or specific parts of it. The best way for Omni-Channel contact centres to achieve and maintain PCI DSS compliance is to remove as much of their environment as possible from the scope of the audit.

Education Seminars	
Ground Labs **Data discovery: the key to customer integrity** **John Cassidy,** Director of Corporate Development, Ground Labs	2018 became the year of huge data breaches, with some household names admitting to a breach and explaining how and what was stolen. Due to this unprecedented rise in breaches the general public were schooled on privacy and cybersecurity and how their data needed to be protected from hackers. Companies doing nothing is not an option if they want to avoid becoming the next news headline. Visit Ground Labs educational seminar to see how the key to improving customer integrity is data discovery. 1. Headline breaches of 2018 2. Fines are now a reality 3. Market observations for 2019 4. What keeps CISOs up at night
PCI Pal **The compliance challenge** **Phil Jude,** Strategic Partnerships Manager, PCI Pal	In this session, we will present how Business Process Outsourcer, DDC (OS) UK, overcame compliance challenges, created efficiencies and improved overall customer experience by integrating PCI Pal's Agent Assist solution. What attendees will learn: • The challenges faced by DDC (OS) UK in achieving compliance in their contact centres • How DDC (OS) UK ensured they had the right technologies in place to safeguard data while meeting the requirements of the latest legislation • How agents were able to take card payments securely utilising DTMF masking technology, while maintaining full conversation with the customer at all times • How DDC (OS UK) can now demonstrate full and thorough compliance with the PCI DSS to their clients
SureCloud **PCI & beyond** **Alex Hollis,** GRC Practice Director, SureCloud	Alex Hollis, SureCloud's GRC Practice Director, will be sharing some of his experiences and strategy when combining PCI compliance programmes more broadly at PCI London later this month. PCI professionals will rightly constrain their thinking and approach to only satisfying PCI, and, with the goal of efficiency, reducing the effort as far as possible. This strategy works well in smaller, but with the ever-increasing demand of regulatory and industry compliance, often the areas that fall outside the scope for PCI may still be in scope for other compliance needs such as GDPR or ISO Standards. When looking at overall corporate compliance, some of the rules and techniques that PCI professionals excel at must be ignored otherwise the efficiency gain will just be temporary as the problem into another team or function. Four key aspects to this are: • Ensuring that you are not limiting efforts around system inventories • Building a model for your control framework that allows controls to be defined and managed once, which when compliant answer multiple compliance needs • Creating control compliance as part of the business as usual activities within the first line teams, making the accountability for controls and ease of management accessible to those who have other priorities within the business • Managing the compliance of third parties with appropriate assessments, avoiding assessment fatigue while getting high-quality, honest answers quickly and with as little impact to both sides
Syntec **Managing execution risk in contact centre PCI projects** **Bob Spence,** Head of Projects, Syntec	Change is always risky and understanding risk is the first step to managing it. PCI compliance projects in contact centres have unique characteristics that can create unexpected obstacles to successful project completion. The PCI solution provider must be able to spot risk early and advise their customers on the most effective way to mitigate these risk. What attendees will learn: • Understanding five common sources of execution risk: complexity, edge cases, stakeholders, third parties, testing • Developing strategy and tactics to counter the threats to successful project completion

Education Seminars

TokenEx

Best practices for PCI scope reduction and ongoing compliance

John Noltensmeyer, Head of Privacy and Compliance Solutions, TokenEx, ISA, CIPP/E, CISSP; and **Trevor Axiak,** Director, Kyte, QSA, CISA, ISO27001 Lead Auditor, SSCP

Any organisation that has undergone a PCI audit can appreciate the value of decreasing its PCI scope. By limiting the size of the card data environment (CDE), organisations can potentially reduce risk and lower the cost of PCI compliance. Some are even able to remove card data from their systems entirely – while still accepting payments.

Join Kyte Director, Trevor Axiak, as he draws from his experience as a QSA to discuss best practices for reducing your organisation's PCI scope. TokenEx Head of Privacy and Compliance Solutions, John Noltensmeyer, will also be on hand to describe the PCI scope-reduction and data-security benefits of tokenisation, including how you can tokenise across all your payment-acceptance channels and utilise the gateway and payment processors of your choice.

Attendees will learn:

- The pros and cons of various PCI scope-reduction techniques
- How to completely remove your e-commerce payments from PCI scope
- Best practices for remaining compliant between PCI assessments
- The differences between encryption and tokenisation
- How to extend PCI compliance technologies like tokenisation to meet your obligations under the GDPR for 'data protection by design and by default'

TokenEx

Continuous PCI and GDPR compliance with data-centric security

John Noltensmeyer, Head of Privacy and Compliance Solutions, TokenEx, CIPP/E, CISSP, ISA

From industry standards like the PCI DSS to privacy regulations like the GDPR, the increasing array of compliance obligations can be difficult to satisfy. Even when organisations achieve compliance, many struggle to maintain it between assessments, and it is seldom sufficient to secure an environment. However, by taking a data-centric security approach, it's possible to meet compliance challenges while truly securing a company's most valuable data assets.

Join TokenEx Head of Global Privacy and Compliance Solutions, John Noltensmeyer, to learn how protecting sensitive data at the point of acceptance can help you reduce risk, achieve PCI compliance, and meet your obligations under the GDPR for 'data protection by design and by default' – while still supporting day-to-day business processes.

Attendees will learn:

- How to rationalise your compliance efforts by optimising common controls
- Why traditional perimeter-focused security strategies continue to fail
- Methods of data protection that meet multiple compliance obligations
- How to extend PCI compliance technologies like tokenisation to include the GDPR
- What does pseudonymisation actually mean?