Issue 5 - May 2014

The blackfoot Quarterly

ADVISE >
ASSESS >
ASSURE >

Hello and welcome to the Spring 2014 Blackfoot newsletter. Following a very busy and equally wet start to the year, we look back on the activities that kept Blackfoot on the radar of information security specialists and report on the some key pieces of information you'll want to know about in 2014, including upcoming Blackfoot events.

To start off this review James Walker, Blackfoot's Director in charge of Business Development, shares a few thoughts on the last period and introduces this edition of the Blackfoot Newsletter.

Somehow its' Spring 2014 already. I say already, because the last time I checked, it was definitely 2009.

I can't be the only one who suffers from "where has the past 5 years gone?" but it's hard to believe it's been 5 years since Blackfoot arrived bringing some much needed "Clarity in Compliance" to the PCI and [information] security space.

Over the last 6 months Blackfoot has been particularly active and we are proud to have supported the industry and clients in so many ways. Since the last newsletter we have invested a great deal of time and effort observing the industry trends, presenting at events, educating our clients on current and planned changes and developing educational content. You can see this in the presentations we delivered at the last PCI London event, the white papers we've authored, our hugely successful cyber events and the production of the open source card game from OWASP which helps software teams identify website security requirements through gamification. In this newsletter we dig into these in a little more detail but also look to bring clarity to some important changes in PCI version 3, while raising awareness of a well hidden and little known government initiative, the cyber security kitemark.

It seems fitting to dig into what these revisions and new standards mean on Blackfoot's 5th anniversary; clarity in compliance it seems has never been a more valued commodity.

Enjoy the newsletter.

James Walker
Director

Blackfoot welcomes Howard Scott

As Blackfoot continues to grow and demand for formal assessment against an increasing number of standards approaches, the Blackfoot team is delighted to welcome Howard Scott. Howard joined the Blackfoot team on 24th March 2014 as an Information Security Consultant and brings with him a wealth of relevant security experience. To read more about Howards experience, visit the Blackfoot website at **http://www.blackfootuk.com/consultants.html**

In this quarterly review, we shine a light on an area of change within the PCI Data Security Standard (PCI DSS) V3.0 that is of particular interest to retailers and service providers, as it centres on requirements for outsourcing. We also touch on a recently announced government Cyber-security kitemark initiative and welcome some new additions to the Blackfoot team.

PCI DSS V3 Requirement 12 clarifications and additions.

Version 3.0 of the PCI Data Security Standard (PCI DSS) came into effect on 1st January 2014 and runs alongside version 2 until the 31st December 2014. During a period of transition, organisations will benefit from the opportunity of readying themselves for later reviews against the new standards clarifications and additions. As of 1st January 2015 all audits must be version 3.

Although there are several tweaks and changes, by far the largest organisational change relates to outsourcing and the contractual management of 3rd parties. We see this as having a substantial impact to both merchants and service providers as they will have a need to agree enhanced contracts ahead of 2015 PCI V3 audit deadlines.

In a summary of changes note supplied by the SSC, it was explained that Requirement 12.8 clarified an intent to implement and maintain policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

This requirement was further supported by a clarification surrounding the applicable responsibilities for the service provider's written agreement/acknowledgement (Requirement 12.8.2) and a new requirement (12.8.5) that details the need to maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. These changes are followed with a new requirement (Requirement 12.9) from 1st July 2015 for service providers to provide the written agreement/acknowledgment to their customers as specified at requirement 12.8.

But what does this mean? In essence, contracts between business process outsourcers and the compliant entities that last beyond January 2015 will need to be amended to include the delineation of responsibility, or will be deemed non complaint at the point of audit. Unlike previous changes this will affect the compliant as well as the non compliant sections of the market. Service providers will need to substantially bolster their contracts if they wish to maintain their compliance status through to V3. Additionally merchants under 'safe harbor' will need to examine their 3rd party contacts and then renegotiate them mid contract.

Cyber security kitemark for the UK

In a move intended to encourage companies to better protect themselves against an increasing threat of online attacks, the UK Dept of Business Skills and Innovation recently announced it's intention to raise cyber standards through the use of a Cyber security kitemark. The Cyber security kitemark is expected to become a supplier requirement of all government departments during 2014, so those wanting to continue or begin supplying central government with goods and services will want to explore the requirements in more detail. While the more cynical amongst us (Ed: Matthew!) make a big sigh at the thought of more red tape and greater regulation without joined up thinking, there is much to be said about raising standards and encouraging leading UK businesses to understand cyber threats and develop strategies for protecting themselves. The costs of cyber threats are estimated to cost the economy a staggering £27 Billion each year.

For those wanting to understand the Cyber security kitemark in more detail, please contact your Blackfoot Account Manager for more information.

For those wanting to learn more about the increasing threat of online attacks and the cyber risk landscape, check out the Blackfoot events section at the end of this newsletter where you will be able to register for our next afternoon briefing session on the 16th July 2014.

Blackfoot on the radar

PCI London – January 2014

Following Blackfoot's controversial 'Keep calm and do nothing presentation' at the PCI London July 2013 event, Matthew was invited back to present at the January 2014 London PCI London event. In a warmly received presentation titled '2014: An Information Odyssey - What a decade of PCI can teach us', Matthew plotted key industry and market milestones dating back as far as 2003 and explored the information security lessons that have been learnt. When considering the future, Matthew concluded that; "change will be constant and risks need to be understood and dealt with in a clear, concise and consistent manner enabling our businesses to innovate"

Interested in seeing this presentation? Look for details in the Blackfoot events section at the back of this newsletter.

Blackfoot Cyber Risk and Cyber threat briefing February & April 2014

At both events Blackfoot gathered together an expert panel of speakers at the Institute of Directors, London EC2M and delivered an essential briefing on cyber threat to some of the UK's largest organisations. The session included presentations from Blackfoot, Visa Europe and Aon Risk Solutions and topics included understanding the threat landscape, what happens when breach comes knocking, methodologies for limiting the likelihood of the risks and the introduction of risk management options.

Wished you'd been there? Look for details in the Blackfoot events section at the back of this newsletter for additional dates.

Articles

In addition to speaking events, Blackfoot has repeatedly been asked to comment on issues across a wide range of security areas. Three recent Blackfoot articles stand out as particularly interesting reads, these are **'Post Snowden – My data, move it or secure it', 'How to ensure your Cloud has a silver lining' and 'The Wild West Web'**

The first article explores whether we should be surprised by the Snowden revelations and how should data be secured in in the future. This article was commissioned by Compare the cloud.net.
To read this article click here.

The second article discusses the issue of moving services to the Cloud and some of important the considerations that relate to card data.
To read this article click here.

The final article identifies the trend for increasingly larger numbers of devices in an increasingly connected world and explores the associated information headaches.
To read this article click here.

Announcing Blackfoot Events

Blackfoot is delighted to announce the Spring 2014 series of events. This season the focus is very much on topics of the moment including cyber risk, regulatory change, and how best to apply the learnings from 10 years of PCI DSS compliance to the current and future information security challenges.

The primary objective of these events is to share knowledge and stimulate discussion. Do you know of someone that would benefit from attending these events? If so, please feel free to spread the word by sharing this communication.

CYBER RISK AFTERNOON BRIEFING

16th July 2014, London

Whilst many organisations have an effective risk assessment and risk management programme, many do not manage or track risk specifically associated with information technology, such as data loss or regulatory penalty.

The cyber risk market is maturing at an astounding rate due to:

- Industrial scale cyber attacks
- Government requests for industry to better understand cyber risk
- Insurance markets offering cyber specific products

To further explore the cyber risk landscape, Blackfoot is hosting an afternoon briefing session.

The event will provide a comprehensive analysis of cyber risk, explore the common misconceptions about what cyber risk is and how to use this deeper level of understanding to interpret, define and apply your organisations cyber risk requirements.

Stay tuned to your Blackfoot Account Manager for event and registration details.

To review the full agenda and register for this FREE event go to **https://www.eventbrite.co.uk/e/cyber-risk-afternoon-briefing-tickets-11580717237**

NEW INFORMATION SECURITY STANDARDS - WEB SEMINAR

Coming to your desktop on 3rd June 2014 – Register now

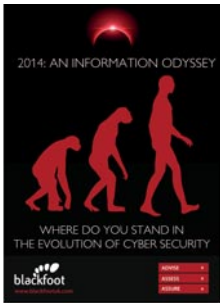
It seems that hardly a day goes by without the announcement of yet another soon to be released information security and privacy standard. With standards being announced with such breath-taking frequency, one might ask questions such as 'are these joined up', 'who do they serve', 'will I be able to keep everyone happy and at what cost' and 'will I need to change my business to accommodate them'.

In this this 45 minute webinar our Matthew Tyler and guest presenter will unpick the new standards and help demystify their intent, main requirements and risks. The presentation will also explore whether regulation is need to be ensure standards are relevant, joined up and appropriately balanced against risk.

To review the full agenda and register for this FREE event go to **https://www.eventbrite.co.uk/e/new-information-security-standards-webinar-tickets-11314498971**

2014 AN INFORMATION ODYSSEY WEB SEMINAR

Coming to your desktop on 9th June 2014 – Register now



In this 45 minute webinar Matthew Tyler will review a decade of PCI DSS from 1.0 to 3.0, explore where we are today and what the emerging trends are, concluding with a glimpse into the future of information security.

To review the full agenda and register for this FREE event go to **https://www.eventbrite.co.uk/e/2014-an-information-odyssey-webinar-tickets-11314348521**

Blackfoot UK Limited
Tel: 0845 805 2409 E-mail: info@blackfootuk.com
Web: www.blackfootuk.com