ISSUE 11 / SPRING 2016

BLACKFOOT QUARTERLY

WELCOME TO THE SPRING 2016 BLACKFOOT NEWSLETTER

It comes as no surprise to know that fraudsters exploit the weakest link. A decade after we implemented EMV chip and PIN in the UK, criminals are diverting their efforts away from face-to-face card fraud towards remote banking fraud.

Whilst cloning payment cards is a great way to obtain cash from ATM machines, any fraud that requires a physical interaction from the criminal is higher risk than one they can commit over the internet. The latest figures published by **Financial Fraud Action UK** bear this out.

Remote banking fraud is up a whopping 72 per cent. Internet banking fraud is up 64 per cent. And telephone banking fraud is up 92 per cent. Whilst this encouraging for brick-and-mortar retailers and those who have invested in EMV and 3D secure, it's bad news for anyone with a bank account as both consumer and corporate accounts are increasingly being targeted.

Plenty more phish in the sea

Zero-day exploits and advanced persistent threats may be headline-grabbing but the mundane reality is that fraudsters will always take the route of least resistance. This is frequently human. With 23 per cent of recipients opening phishing messages and 11 per cent clicking on attachments, according to the *Verizon 2015 Breach Investigations Report*, fraudsters have little need to evolve tried and tested deception methods to steal money.

In this quarter's newsletter we outline **the five most common frauds and scams** that exploit the human factor. Training colleagues to recognise and understand the risks of phishing e-mails and CEO fraud helps them play an active part in combatting these threats. With **training now a mandatory requirement** in PCI DSS, training a lot of staff consistently has never been more challenging.

C-suite cybersecurity awareness

Senior management must also be cybersecurity informed and ready. After all, the buck for data security and privacy stops with the C-suite executives, board members or non executive directors. We have recently developed a half-day interactive workshop aimed at this audience. Let me know if you would like more details.

We hope you enjoy this issue of the *Blackfoot Quarterly*. This is your newsletter, so if you have any comments on it or suggestions for future articles, please let me know.

Matthew Tyler
CEO, Blackfoot UK

IN THIS ISSUE

Compliance assessments >

Combatting fraud and scams >

Training >

WHAT MAKES A GOOD COMPLIANCE ASS

Our approach to compliance assessments simplifies the task of achieving and maintaining compliance, and often helps cut compliance spend

Compliance can be complex. Organisations have multiple regulatory requirements, some of which meet specific threats, others exist in or are shared across regulations and geographies. The requirements and the risks associated with non-compliance change frequently and reflect the changing landscape.

Consequently, organisations cannot easily determine what standards and regulations they are required to comply with, what budget and projects are needed, and how to manage the delivery, implementation and ongoing maintenance of compliance.

Based on our experience of conducting all types of compliance assessments, we summarise what makes a good one.

Conduct a discovery and planning exercise

What is the intent of the standard? How does it apply to your business, particularly in terms of the scope of different systems and parts of the business? Must an organisation adopt all elements of a compliance standard, or simply the elements that are relevant to the intent of the standard?

> ***"I will never forget a five-minute conversation at the project board where we proposed a number of actions costing approximately £500k. The Blackfoot consultant challenged them, made us rethink, and the final cost to achieve the same end came out at £10k!"*** **— Finance Director and Blackfoot customer.**

Your business needs to grapple with these questions to comply with any compliance standard in an effective and efficient manner.

Typically our consultants conduct an onsite discovery exercise to establish three things. Firstly, we determine the organisational structure and key information assets and systems. Secondly, we map the information captured to a compliance matrix or tool to identify the controls required. And finally, we define the organisation's existing compliance obligations, and identify the presence and maturity of controls.

Explore the different compliance options

Standards and regulations deal with controls and rarely identify ways of changing business processes to reduce compliance and risk. They are more focused on implementing and maintaining controls, which are overlaid on current business practices. We review your organisation's existing security posture and identify ways to reduce the scope and applicability of compliance to reduce cost and complexity.

We work up the different compliance options available and build decision matrices based on key factors, such as your organisation's ability to achieve and maintain compliance, the maturity of existing security, the cost of achieving compliance, customer experience and business strategy.

Where processes could be changed to reduce the risk and compliance overhead, we evaluate the cost and impact of process change against the cost and impact of compliance overhead.

We document and present our findings in a way that allows you to easily understand and evaluate the various options. Naturally, our experienced consultants are on hand at this stage to support your internal discussions and to agree an approach.

Because we assess how your policies and procedures contribute to your own compliance, we are often able to reduce your liability, compliance spend or both at this stage. This is frequently by challenging internal assumptions to prompt a rethink and save money.

Achieve compliance

We work with your compliance and technical teams to create a high-level programme of works towards achieving compliance. This is based on a prioritised approach. We also identify the best use of internal and external resources.

Optional access to our Compliance Management Platform (CMP) for three months is also included. This is where we input the compliance objectives, which gives you a clear roadmap of where you are and what is left to do.

Carry the learnings forward

Anything could change in your business or that of a supplier or third party. Similarly, external changes at an economic, social or technology level could also shape the character of the opportunities and risks your organisation faces. Compliance is a process of continual improvement, not a one-off exercise. Therefore monitoring your situation is critical.

Blackfoot assurance services also include exercises to help customers test their policies and compliance in a controlled environment and carry the learnings forward. We can run on-site crisis management tests to put your incident response plans through their paces and make improvements.

We also have virtual compliance office (VCO) service available to customers via an ongoing support contract (see box).

For more information

If you are interested in commissioning a compliance assessment, please contact your Blackfoot account manager.

Compliance Management Platform

Blackfoot's compliance management platform (CMP) allows customers to view and manage compliance projects across various standards via a single, easy-to-use, web-based application. The CMP helps streamline the process of compliance, saving you time, money and effort.

The CMP is available as a hosted service for internal customer use, or as an external service for managed service providers, wishing to to manage compliance projects on behalf of their customers. The CMP is ideal for anyone who wants to manage compliance tasks, have an overview of project progress, collect evidence centrally or prepare for an upcoming audit.

Virtual compliance office

Blackfoot's virtual compliance office gives customers access to the expertise of our skilled consultants via a web-based portal. Subscribers to the service also receive periodic onsite governance reviews facilitated by a Blackfoot consultant.

Service areas include:

- Expert advice
- Managed governance reviews
- Planning meetings
- Knowledge share workshops

COMBATTING FRAUD AND SCAMS

We outline the five most common frauds and scams that exploit the human factor to help you fight them

The use of zero-day exploits and advanced persistent threats to hack an organisation make for great news headlines. But the reality is much more mundane and low-tech. Criminals are lazy and if the old ways into an organisation still work, why evolve them?

23 per cent of recipients open phishing messages and 11 per cent click on attachments, according to the *Verizon 2015 Breach Investigations Report*. So, whilst delivery mechanisms may change and approaches become more targeted, phishing is still an extremely effective tool to extract cash from unprotected or unprepared targets.

CEO e-mail scams, in which criminals impersonate the e-mail accounts of chief executives, has affected around 12,000 businesses worldwide at a cost of more than $2 billion in the last two years. Around $1.2 billion was lost globally between October 2013 and August 2015, at an average loss of $120,000, say the FBI.

We recap five of the most common frauds and scams that exploit the human factor to help prevent you and your colleagues becoming the next easy target.

Courier fraud — you receive a call from someone claiming to work for your bank or the police. They dupe you into revealing your PIN number and then send a courier or taxi to collect your card. Once they have your card and PIN they can spend your money.

Overpayment fraud — you have an unexpected cheque in your pending account balance and soon after are contacted by someone claiming to have put the wrong details on their cheque. They ask you to return the funds to them. You make the payment. The next day the cheque bounces.

Phishing — you receive a fraudulent e-mail purporting to be legitimate, which tricks you into revealing usernames, passwords or financial details. These e-mails may include links or documents containing malware.

Spear phishing — a more targeted form of phishing as the e-mail purports to come from a colleague in a trusted department, such as HR or finance. You are asked to change your password or confirm your details, and re-directed to a bogus version of the company website or intranet.

CEO scam — you receive a fraudulent e-mail purporting to be from your CEO or CFO instructing you to transfer funds to a bank account (usually controlled by the criminal), settle an outstanding invoice, or informing you that supplier bank account details have changed. You transfer the funds and never see them again.

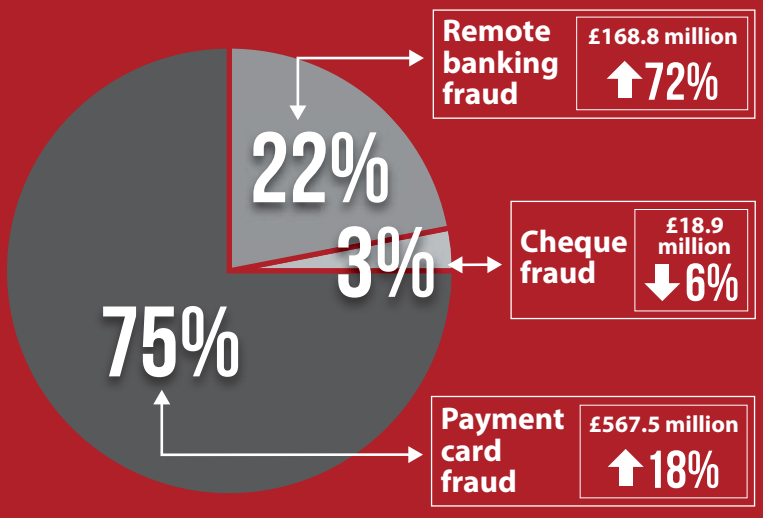
Forewarned is forearmed

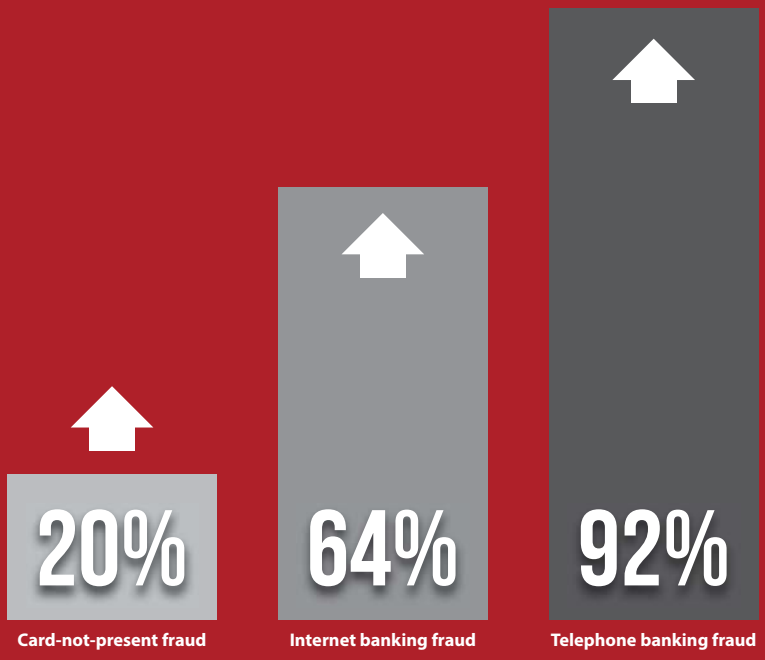
While there is no silver bullet to managing and mitigating risk, a combination of sound awareness training, effective e-mail and web gateway protection, layered controls on finance and banking systems and two-factor authentication are all good controls to consider.

Please see the article on **security awareness training** in this newsletter about Blackfoot's on-demand, easy to understand training content to help educate your staff.

2015 FULL YEAR UK FRAUD LOSSES

Total 2015 financial fraud losses by type





Source: Financial Fraud Action UK, March 2016

Losses to financial fraud last year increased more than a quarter (26 per cent) on 2014 figures. According to to official figures from Financial Fraud Action UK (FFA UK), gross fraud losses across payment cards, remote banking and cheque totalled £755 million in 2015.

The pie-chart to the left shows the breakdown of gross fraud losses in the UK last year by type. Three-quarters (75 per cent) of losses were attributable to payment card fraud (and remote purchase fraud accounted for 70 per cent of these losses). Remote banking fraud made up 22 per cent of gross losses. And cheque fraud three per cent.

The rise across all fraud loss types during 2015 owes much to the growth of impersonation and deception scams, as well as online attacks such as malware and data breaches. Fraud through remote retail and banking channels is increasing.

Since in-store chip and PIN card payments were rolled out a decade ago, fraudsters are switching to less secure remote purchase channels. They use stolen payment card details fraudulently to make purchases on the internet, over the telephone or through mail order. Losses on purchases made remotely increased 20 per cent to £398.2 million in 2015.

Similarly remote banking losses via online, telephone or mobile channels increased by 72 per cent to £168.6 million in 2015. Typically criminals perpetrate this fraud by duping victims into giving away their personal and security details, which they then use to access victims' remote banking accounts. Businesses and high net-worth customers are increasingly under threat from this type of fraud, shown by the greater increase in the value of losses compared to the volume of cases.

Staying one step ahead of the fraudsters starts with understanding the problem. Secondly, build on this awareness with practical training. Please see the article on **Security awareness training** in this newsletter for more details.

NEWS IN BRIEF

We round up recent Blackfoot and industry news during the last 90 days

Privacy and data protection update

April has been a landmark month for privacy and data protection. The final text of the long-awaited EU General Data Protection Regulation has been published and approved by the EU's LIBE committee, and will formally replace the Data Protection Directive — and therefore the UK's Data Protection Act — in 2018.

The Regulation will align EU Member State laws on data protection, and includes provisions to require the appointment of data protection officers; to enforce rigorous consent checks, particularly for young people's data; to introduce mandatory reporting of data breaches and tough new penalties for data protection failures; and to demand portability of customer data.

Separately, the Article 29 Working Party of Data Commissioners has given tentative approval to the EU-US 'Privacy Shield' that is proposed to replace the defunct 'Safe Harbour' agreement for transfer of personal data to US organisations.

Concerns remain about transparency, monitoring and effective redress for EU residents, but in the absence of alternatives for organisations that cannot apply model clauses or binding corporate rules, the Privacy Shield may be the only viable option for business as usual to continue.

The Article 29 Working Party has recognised the reluctant compromise in its approval by recommending that the arrangement be formally reviewed in two years' time to coincide with enactment of the General Data Protection Regulation.

If you would like to receive our forthcoming briefing note on this topic please **click here** to request a copy.

US Federal Trade Commission probes PCI DSS auditing

In what may prove to be a portent for operators in Europe and the UK, the US Federal Trade Commission (FTC) is investigating how assessors measure compliance with the PCI DSS. In early March, the agency issued orders to nine PCI DSS-accredited assessment firms requesting information and limited set of example PCI DSS assessments.

This request follows a long-running legal battle between the FTC and the hotel chain Wyndham Hotels and Resorts over a series of data breaches in 2008 and 2009. In what is regarded as a test case, the FTC was granted the power to charge Wyndham with "unfair and deceptive practices" in failing to protect consumer payment card data.

The wider implications of this judgement mean that US companies that fail to adequately protect card data could be subject to both contractual penalties from card schemes and acquirers, and FTC regulatory sanctions.

One has to ask whether the regulatory interest shown in cybersecurity Stateside will hold up in court and set a precedent for other national regulators.

Timeline for the introduction of PCI DSS and PA-DSS version 3.2

In view of the deadline extension for secure socket layer (SSL) and early transport layer security (TLS) migration, the PCI Council published PCI DSS 3.2 on 28 April 2016. Other documentation is also available, including report on compliance templates and frequently asked questions.

At the end of May 2016, the PA-DSS and other supporting documentation will be published.

PCI DSS 3.1 will retire six months after the release of PCI DSS 3.2, and from October 2016 all assessments will need to use version 3.2.

The new requirements introduced in PCI DSS 3.2 will be considered best practices until 31 January 2018. Starting 01 February 2018 they are effective as requirements.

For more information about version 3.2 of the PCI DSS, please contact your Blackfoot account manager.

Will you get paid in June?

From 13 June 2016 Bacs, the company behind automated direct debit and credit services in the UK, is adopting new security standards.

At the same time, it will withdraw support for older connection protocols, such that after 13 June 2016, only TLS 1.1 and 1.2 will be supported.

This will have implications for any UK business wanting to use Bacs to make salary or supplier payments or to collect funds via direct debit.

Direct submitters to Bacs are recommended to contact their software suppliers.

Those who use a Bacs-approved bureau are recommended to contact their bureau to ensure their web browsers and operating systems will support the changes.

Blackfoot staff news

As spring heralds the start of a new financial year, boardrooms worldwide are grappling in earnest with information security. This is increasing the urgency and demand for specialist information security support. This hasn't taken Blackfoot by surprise, in fact we have been preparing the business to support the increased demand for the last 18 months.

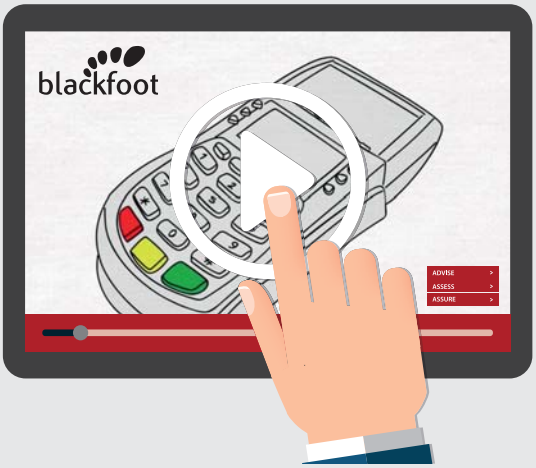
We are pleased to announce that between the last quarter of 2015 and first quarter of 2016, the consultancy team has increased in size by a third.

The expanded team is supported by Tom Boxall in a dedicated project management role and new hire, Richard Huggins, as Head of Delivery. Richard will be focusing on the efficiency and timeliness of consultancy delivery. Alex Dewar is moving to Head of Consultancy with responsibility for the quality and consistency of our consultancy service.

The new team is also supported by Gesa Grabis, who joins as a specialist HR and recruitment associate, focussed on meeting our ambitious recruitment plans across all divisions.

This means that Blackfoot is even better positioned to support customers throughout 2016 and beyond.

SECURITY AWARENESS TRAINING



How to simplify the task of meeting regulatory training requirements, make best use of scarce training budget and maximise productivity

Here's the conundrum: your colleagues are not experts on security but well-trained staff are less likely to lose data.

Undertaking organisation-wide training is easier said than done. As anyone who works in a business with a large, dispersed workforce knows, there are productivity issues around taking tens of thousands of staff away from their core duties for training. Frequent staff turnover, changes in technology and legislation, and the technical subject matter do not make security training any easier.

However threats are evolving. Criminals are wily and the attack surface is broad. Moreover there are now seven training controls in the PCI DSS version 3.2 that have moved from best practice to an audit point.

Section 6 — Develop and maintain secure systems and applications — 1 control

Section 9 — Restrict physical access to cardholder data — 2 controls

Section 12 — Maintain an information security policy — 4 controls

The Blackfoot approach

Blackfoot's training take a fresh approach to learning. We deliver on-demand, easy to understand educational content. Created by Blackfoot experts, the training is designed to improve employee awareness of data security issues, but also to meet a range of compliance standards and best practice.

The training modules include memorable video content that is delivered in minutes, vastly reducing the operational cost of training a large, dispersed workforce. We can also provide content for break-room posters, messages on the homepage of the company intranet, key messages for staff meetings, competitions and quizzes. These all help reinforce the learnings.

The modules addressing PCI requirements include:

Section 6

- Cornucopia (a training aid in the form of a card game to help software teams identify website security requirements)

Section 9

- Face-to-face payment security

Section 12

- Core cyber security awareness
- Mail order / telephone order (MOTO) payment security
- Face-to-face payment security

Other training modules

- Handling personal data
- Security for remote workers
- Fraud prevention

For more information
To find out more about Blackfoot's security awareness training or to receive a quotation, please contact your Blackfoot account manager.

blackfoot

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

ADVISE >
ASSESS >
ASSURE >