ISSUE 7 / SPRING 2015

BLACKFOOT QUARTERLY

WELCOME TO THE SPRING 2015 BLACKFOOT NEWSLETTER.

Your risks in context

Over the last three months, we've been explaining real-world risks, identifying trends and discussing the implications in our regular series of webinars. Our article on **internet organised crime** summarises the key findings of a recent Europol report on cybercrime, which was the subject of a recent webinar. We also explore **security in the cloud**, the changing remit of internal IT departments and what this may mean.

The external landscape is always changing, so we repeat our webinar programme regularly. We also upload the recordings to the Blackfoot UK YouTube channel for as many of our customers to watch as possible. Let us know if there are topics you'd like to see covered in future webinars.

Your risks in review

External factors may be more difficult to influence and control compared to internal risks. However, therein lies the source of competitive difference. Regulation is the archetypal external factor that affects all players costs, but may do so differently depending on your organisation's approach and readiness. An example of this is the proposed amendments to card interchange fees, discussed in our last newsletter.

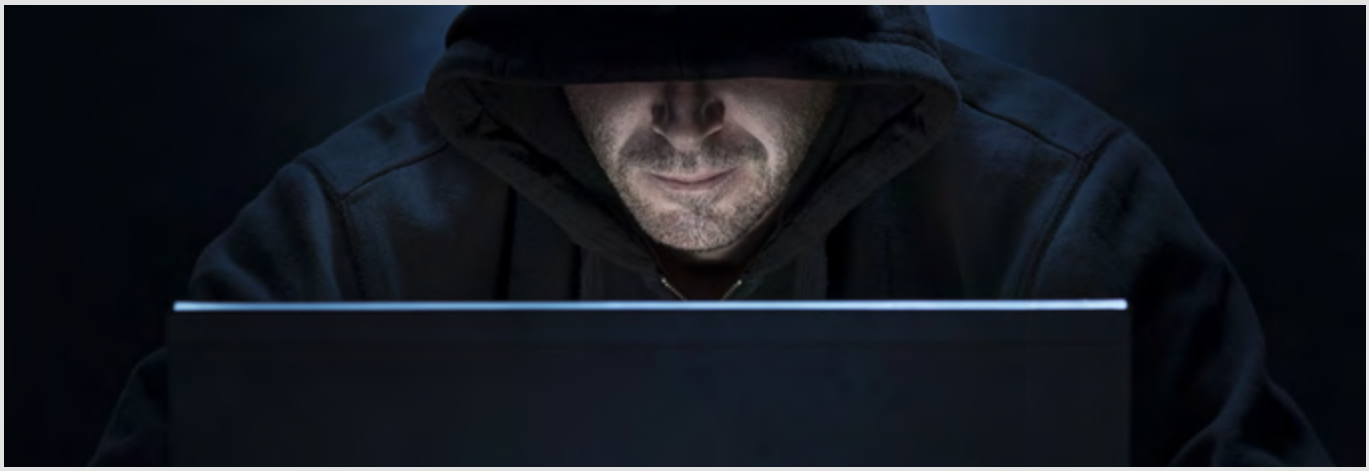
Merchant service charges (MSC) are a significant cost to those who accept payment cards - often larger than entire IT budgets. To that end, we're pleased to announce a new service to review the impact and future implications of **card interchange amendments** on your business. Our strategic payment review ensures that your total cost of taking payments is as efficient as it can be. It considers various cost lines, including fraud and chargeback processing.

Elsewhere we continue our series by examining **what makes a good risk assessment**, and the importance of reviewing your risks regularly as part of this process.

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



INTERNET ORGANISED CRIME

We summarise the key findings of the recent Europol report on internet organised crime and discuss the evolving threats and need for collective action

The 2014 iOCTA (Internet Organised Crime Threat Assessment) report published by Europol confirmed what many within the security industry had long suspected. Cybercrime is becoming more organised and more commercial, which is lowering the barriers to entry for criminals.

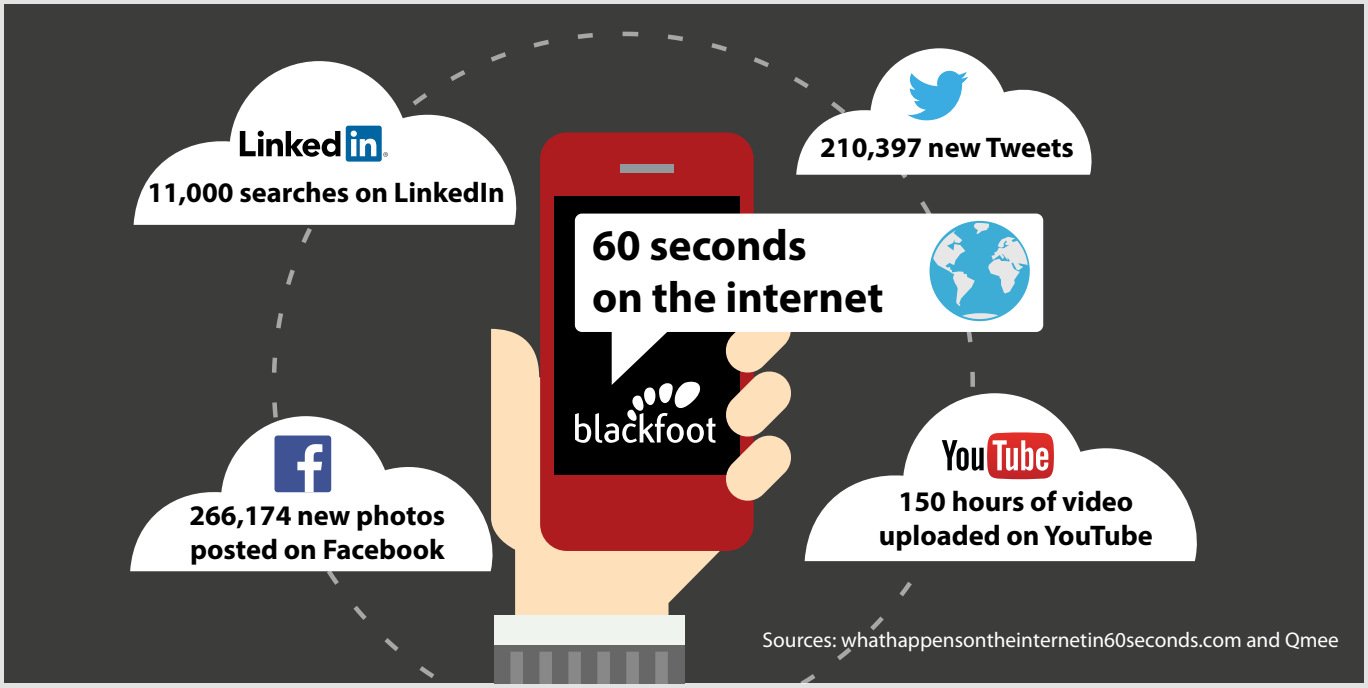
Always on. Always connected. Always generating data.

We're increasingly online and connected. More than 2.8 billion people use the internet worldwide on ten billion internet-facing devices. And it's not just individuals, businesses and governments that are connecting via the internet.

The Internet of Things enables previously unconnected things without computing power to connect. In the not-too-distant future your fridge could re-stock itself. Your washing machine or car could book its own service. Your smart electricity meter could submit its own readings. The internet is becoming part of our lives. And with social networking, our lives are becoming part of the internet. We're generating data at an unprecedented level. What happens in 60 seconds alone on the internet is mind-boggling.

We're having to find new names and storage solutions for data. Who'd heard of a petabyte, exabyte or zettabyte of data ten years ago? (They are 1,000 bytes to the power of five, six and seven respectively). How many businesses had heard of or were using cloud storage a decade ago?

Yet the downside to the changes in internet usage and the willingness to share information is, according to the report, "a broader attack surface and multiple areas of people's lives for criminals to exploit."



Cybercriminals, their motives and crimes

The cybercrime underground is complex, dynamic and fragmented. There is no typical cybercriminal. Attacks can come from activists, terrorists, competitors, disgruntled employees or even nation states. The motives for attack are as varied, ranging from economic, political or ideological reasons to espionage, sabotage and extortion.

Underground forums and marketplaces continue to be critical in bringing together buyers and sellers to exchange information and trade. These platforms, usually accessed anonymously, function as online bazaars for illicit goods and services, including weapons, drugs, hitmen for hire, but also malware, proxy services and stolen card data.

Criminals are increasingly packaging their services into off-the-shelf or 'crime as a service' kits. The prices for these malware, ransomware and wifi intercept kits are falling on underground forums and darknets. Consequently, barriers to entry for cybercriminals without specialised knowledge or technical skills are falling, too.

Besides crime as a service, the iOCTA report highlights seven other major crime areas. These are malware, child sexual exploitation online, payment fraud, criminal finances online (principally money laundering), social engineering, data breaches and network intrusions, and vulnerability of critical infrastructure.

Cybercrime is the archetypal external risk that affects all players, but may do so differently depending on the organisation's approach and readiness

The need for collective action

Our internet usage and online behaviours make everyone — governments, businesses and individuals — part of the cybercrime problem. And, to an extent, there is a moral imperative for us all to be part of the solution.

Various activities are already underway. In the UK, MI5 and GCHQ are encouraging FTSE350 companies to undertake cyber health checks. The UK government introduced a cyber kite mark for businesses in 2014, which all suppliers to government will need to attain. Whilst regulators at a national, European and industry-wide level continue to strengthen legislation and standards relating to internet payments, data security, privacy and stewardship.

We're aware that regulations evolve, standards overlap and cross-border cases can be complex. Compliance with multiple standards cannot be done in silos. At Blackfoot, we're well-versed with industry changes, including the most recent changes to the **PCI DSS v3.1 announced in early February 2015**. If you'd like to schedule a briefing on how regulatory changes impact your business, please contact your Blackfoot sales representative.

For more information

To find out more about the cybercrime and its impacts, view our webinar **Internet organised crime and the case for security** on the Blackfoot UK YouTube channel.

We have also prepared a three-minute video about the cybercrime threat and its implications, which is available **here.**

INTERCHANGE UPDATE

Some clarity on the complexities of card payment interchange fees

Interchange is complicated. There's no getting around it. The situation is also changing apace — every 90 days from 1 April 2015 until the same time next year in the case of some MasterCard rates. Whilst interchange rates are generally falling, this does not necessarily mean that those who accept payment cards will be better off.

We've been asked by a number of our retail customers to provide practical support on interchange. So, we're pleased to announce a new service, which we hope will provide some much-needed clarity.

It's complicated

Each card scheme has a slightly different formula for calculating interchange. Rates also differ depending on the type of card used (e.g. debit, credit, commercial), the security of the transaction (e.g. EMV, magnetic stripe only, card not present), merchant sector, country and so the list goes on.

Everyone has a view on the subject: banks, the merchant lobby, the card schemes, the regulators. Unsurprisingly these views differ — sometimes widely. And what is published on the subject can be confusing, partly due to the complexities detailed above, and partly due to individual agendas and what the speaker chooses to omit as much as include.

It's changing

In summary, both MasterCard and Visa Europe, the two main card schemes operating according to a four-party model, have already lowered interchange fees, and will continue to do so over the coming years.

Visa Europe has introduced a cross-border domestic interchange programme, enabling acquirers to offer lower domestic rates to their merchants domiciled in a different European country. These rates apply to consumer cards only. They are 0.2% for debit cards and 0.3% for credit cards. Visa Europe acquiring members have to comply with various criteria to participate, which may have a knock-on effect on their merchants. Provisions are included around registration, licensing, billing structure and identification of merchants. The changes are already effective.

Meanwhile in the UK, new rates are applicable for Visa UK debit cards and MasterCard UK credit cards. From 1 March 2015, the new Visa debit rates differentiate between so-called secure and non-secure transactions, and between consumer and business cards. (There are four separate rates). From 1 April 2015, the new MasterCard credit rates for consumer credit cards will reduce to 0.8%. There will be further rate reductions every 90 days, until 1 April 2016 when the rate will be 0.3%.

How Blackfoot can help

We're not going to opine on the legitimacy of the core principles of interchange, the legal arguments, or the mathematics underpinning the various interchange formulae. We'll leave that to the regulators, the lawyers and the mathematic professors.

In response to customer demand, we're going to focus on what we do best: providing honest, independent advice in plain English. And helping you to make the most intelligent use of your time, resource and budget.

We've engaged a specialist consultant, who can work alongside customers to review the interchange you're paying as a proportion of your merchant service charge (MSC), the potential impact of proposed changes, and to recommend appropriate responses.

The proposed changes will bring potential cost savings for UK Retail plc, but there'll be winners as well as losers...

To find out more about the new Blackfoot interchange service, or to commission a review, please contact your Blackfoot sales representative.

SECURITY IN THE CLOUD

Our webinar on cloud computing in February was popular and we'll be repeating it on 11 May 2015. We recap the main points

Cloud technology is heralding a new era of business and working practices. Growing numbers of organisations are meeting these challenges through secure managed service and infrastructure providers. But what are some of the implications?

IT departments: they are a-changin'

Many businesses are investigating cloud technology as a way to reduce IT spend and realise efficiencies. This may be as a result of improving resilience, backup, scalability and access across devices and geographies.

At the same time the price and availability of compute power is falling, due to the proliferation of consumer devices. Employees increasingly expect to use their own devices in an office environment. Suddenly it's become feasible to operate without the massive up-front investment in mainframe computers, and other IT resources that only a large organisation could afford. The roles, responsibilities and expectations of an IT department are changing, too. Gone are the days when it was the monopoly supplier of IT.

"Our five year forecast for IT departments is that they will begin to manage risk and outsource partners," says Matthew Tyler, CEO, Blackfoot UK.

"They will include a data protection officer and will have to contend with increased transparency requirements. IT departments will have to concern themselves with how data is secured, but also what it is used for."

To cloud, or not to cloud. Is that the question?

Whether you should adopt cloud technology (or not) is probably not the right question. If you use corporate Facebook or LinkedIn, you're probably already using the cloud. So, it becomes less a question of internal versus external data access and storage, and more how you can get cloud technology working most effectively for your business.

"Do you know what data you have, and where it is?" asks Matthew. "I've yet to meet a company, apart from start-ups, who can answer those two very simple questions. So, you could look at cloud technology as a way of understanding what information you've got, and where it is."

What have you got, and where is it?

Any organisation of any size will suffer 'data proliferation'.

"'Local copy' are two of the scariest words in the English language when it comes to data discovery." continues Matthew. "We did an exercise for a client and found that their finance department had 750 copies of customer orders over three years taken from the main finance system to enable employees to work during their commute."

Different data carries different penalties if lost, stolen or unavailable. The loss or theft of some types of data (i.e. in a data breach) carries fines of up to five per cent of turnover or €100 million, according to EU Data Protection Regulation. And fines of up to £500,000 for serious breaches of the UK Data Protection Act.

Mandatory breach notifications are already law in some countries. The trend towards adopting them is increasing. This means potentially more operational costs for data custodians if data is lost, stolen, disclosed by human error or a disgruntled employee. It's costly to write out to 200 customers, let alone to two million customers — quite apart from paying a third party to monitor their credit histories.

Security in the cloud: a shared responsibility

Once you have established what data you have and where it is, you can determine whether your security is fit for purpose, and what type of cloud service may be appropriate.

Consider due diligence and who's responsible for what when negotiating with cloud suppliers. Depending on your contract, you may outsource various activities, but retain all the responsibility for their actions and the financial liability if things go wrong. With regard to cloud boarding, we advise a collaborative approach to ensure you have the right levels of assurance. Finally, dedicate sufficient resource to the outsource relationship across your business. And when changes are planned, work together to manage them.

For more information

We'll be repeating our webinar Security in the cloud: a shared responsibility? on 11 May 2015, **register now**

What is cloud technology?

Cloud technology is storing and accessing data and programmes on the internet, rather than locally on a computer's hard drive or home/office network. 'Cloud' could be regarded as a synonym for 'internet' as the name is thought to come from depictions of the the internet in presentations — it was frequently shown as a cloud. Software, platforms, networks and infrastructure services are available to buy or rent via the internet/cloud. There are four main types of cloud: public, private, community and hybrid (two or more of the aforementioned types).

WHAT MAKES A GOOD RISK ASSESSMENT?

Our risk-based approach helps save customers 70 per cent on average on their compliance budgets. We explain how

What are your business objectives? And how certain are you that you'll achieve them?

If you're at all uncertain, the effects of this uncertainty may be termed 'risks'. This is where a risk assessment comes in. It helps you understand and manage uncertainty through effective decision-making, thereby increasing the chances of achieving your objectives.

Risk assessments are a cornerstone of the Blackfoot consultancy approach, and how we generate robust, real-world recommendations for our customers. We summarise what makes a good risk assessment.

Often we find that customers are spending more to control their risk than the cost of the risk itself, or are implementing controls to manage other people's risks not their own

Agree a common purpose

Firstly, consider why you're undertaking a risk assessment and agree a common understanding internally. Essentially it is to understand the likelihood and impact of an event happening. You work through an accurate, repeatable, standardised methodology to obtain information to guide your business response.

A risk assessment is not the same as a controls assessment or a gap analysis. The objective is not to completely eliminate all risk from your business. This is neither possible nor desirable. At Blackfoot we're used to demystifying risk to staff at all levels, so we can help you position a risk assessment effectively and secure buy-in to the process and output.

Determine your risk appetite

Risk appetite means the amount and type of risk your organisation is willing to seek, accept and hold in pursuit of your objectives. Getting the balance right is important, because too small an appetite could be as detrimental to your business as too great.

Opinions will vary. What is acceptable within one business unit or function may not be acceptable (or appropriate) at an organisational level. What is acceptable within one industry may not be within another.

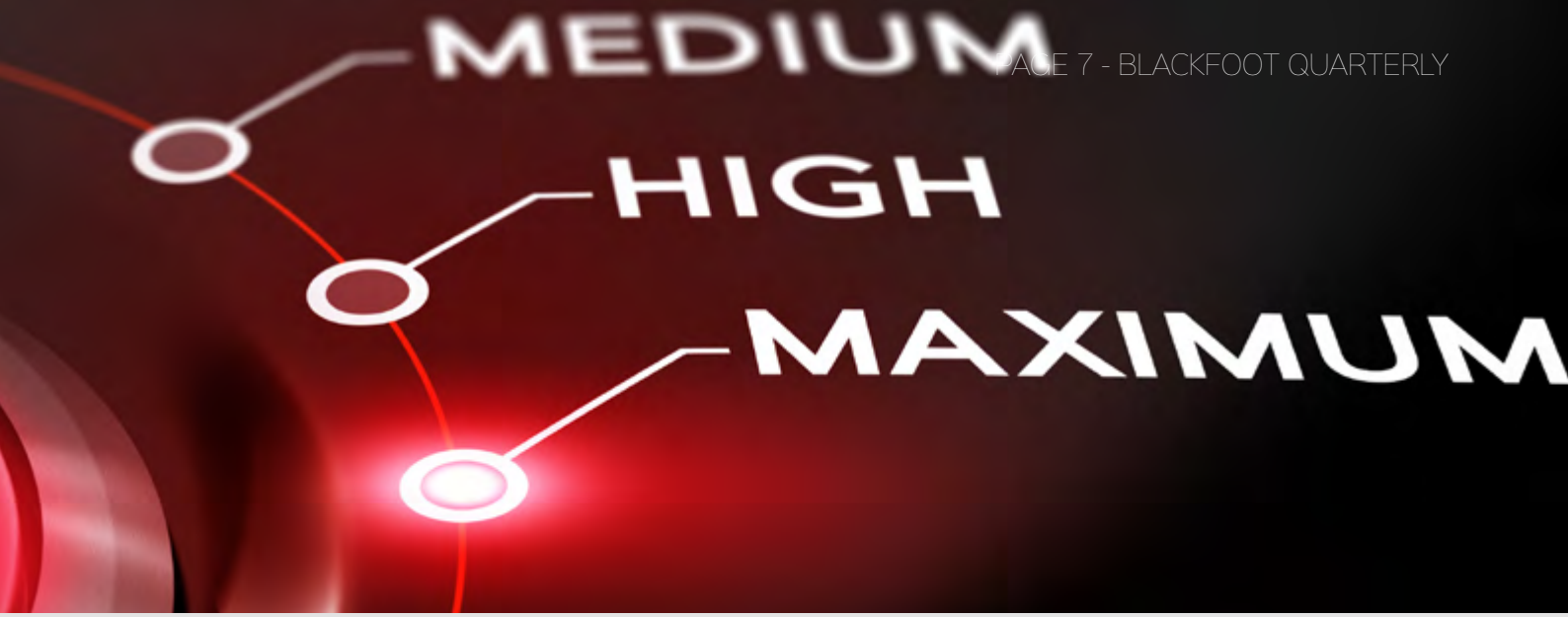
Similarly, risk appetite may vary over time, with corporate culture, with your ability to control it and to turn it from a theoretical, strategic concept into a practical day-to-day reality within your organisation.

We offer advice on suitable risk appetite benchmarks for your business and industry sector.

Assess and evaluate your assets

Next, assess what is of value to your business. Is it critical systems, market advantage, profit and loss data, customer data? Then assess what is of value to others, for example to your customers or to criminals trying to make illicit use of data.

As part of our risk assessment we help you evaluate the impact of confidentiality, integrity and availability breaches on your information assets. We also help identify the threats (e.g. external, internal or accidental) and map these for each asset.



By this stage, you will understand your gross risk — sometimes also known as 'pre-control' or 'inherent' risk. This will help determine your focus, how you develop your controls and how you manage your resources.

Identify your risks

Identifying all your threats is critical. If a threat remains unidentified, there is no opportunity to do anything to prevent or mitigate it. Furthermore, errors at the identification stage could detrimentally impact the process that follows, potentially causing bigger risks later on.

Our consultants are experienced at conducting thorough risk audits. In a information security risk assessment, we focus on three main questions during the identification or discovery stage. What information have you got? Where is it? And who has access to it?

Assess likelihood

Not all risks are created equal. Not all risks will materialise or have the same impact. Once you have identified all your potential risks, assess their likelihood and impact, and agree the appropriate scales by which to measure this.

Measurement scales are part of our tried and tested risk assessment methodology. They range from critical to negligible and consider financial loss, adverse publicity, reputational damage, legal and regulatory exposure. Our scales are customisable and help you short-cut the process of devising your own.

Determine risk management options

There are always several options for managing your risk. Customer feedback indicates that this is where you value the expertise of Blackfoot consultants most.

Often we find that customers are spending more to control their risk than the cost of the risk itself, or are implementing controls to manage other people's risks not their own. Our recommendations in this area regularly save customers significant sums — on average 70 per cent on their annual compliance budgets.

Risk assessments are a cornerstone of the Blackfoot consultancy approach, and how we generate robust, real-world recommendations for our customers

The main ways to manage risk can be summarised as: accept, reduce and transfer.

You could decide that the risk is within your appetite and accept it. You may add the risk to a register and re-assess it periodically, but broadly you're prepared to tolerate it within your business.

There will be some risks that you want to reduce. Consider the policies and controls already in place and whether they are appropriate. If you need to remediate by increasing, updating or removing controls, do so.

Another way to manage risk is to transfer out the responsibility to someone else, either by outsourcing and/or purchasing insurance. For example, you may decide to outsource the collection, transmission and storage of payment data from your e-commerce platform to a certified third party.

Monitor your risk

At its most effective, risk management takes account of changes to remain aligned with your objectives. Therefore ongoing monitoring is essential to managing your risk and making any adjustments as necessary.

We offer advice on key risk and control indicators, internal roles and responsibilities, frequencies and benchmarking to help ensure that a good risk culture becomes embedded within your organisation.

For more information

If you are interested in commissioning a risk assessment, please contact your Blackfoot sales representative.

NEWS IN BRIEF

Blackfoot customer day

We're organising a customer day in October 2015 and would like to include topics of most relevance to you. E-mail us at **info@blackfootuk.com** with your suggestions for the agenda.

Order your free set of updated Cornucopia cards (version 1.1)

Cornucopia is a teaching aid in the form of a card game to help software teams identify website security requirements. Blackfoot UK continues to support this initiative with the updated version 1.1 of the game. Cornucopia is based on the open web application security project (OWASP) standards. Since it was launched in 2013, the cards have helped train around 200 IT professionals in more than 20 countries. Order your free set of cards by e-mailing **cornucopia@blackfootuk.com**.

PCI DSS v3.1 and PA-DSS v3.1 expected soon

In mid-February 2015 the Payment Card Industry Security Standards Council (PCI SSC) issued a bulletin announcing an update to the PCI DSS and PA-DSS.

The National Institute of Standards and Technology (NIST) has identified that SSL v3.0 protocol is no longer acceptable for protection of data due to weaknesses inherent in the protocol. As such, no version of SSL meets the PCI SSC definition of "strong cryptography".

The PCI SCC will soon publish a new version of the standards: PCI DSS v3.1 and PA-DSS v3.1. The former will be effective immediately, but changes to the requirements will be future-dated to allow organisations time to implement them.

If you have questions about the implications of the changes on your business, please contact your Blackfoot sales representative.

Telephone card payments and PCI DSS

We've partnered with Encoded, a leading provider of interactive voice response and automated payment solutions, to produce a white paper.

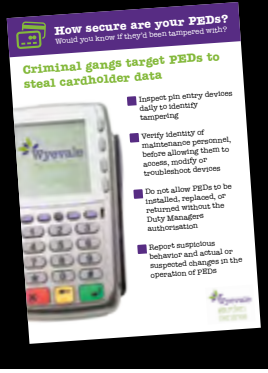
The paper considers the threats of accepting card payment on the telephone, and what can be done to mitigate them. It surveys the various products on the market and how to evaluate their security. Lastly, it discusses what PCI DSS really means and the merchant's responsibility.

Download your copy of the white paper here.

Contactless terminal mandate in Europe

International card scheme, Visa Europe, is understood to have mandated contactless payment acceptance across 37 countries from the end of 2015. The mandate covers terminals in a face-to-face environment, including semi-attended, unattended and mobile point-of-sale devices used in a fixed merchant location.

From 31 December 2015, any terminal installation with a new Visa merchant or upgrade programme with an existing Visa merchant must include contactless payment. From 31 December 2019, all Visa terminals deployed in a face-to-face environment must include contactless payment.



New posters available

Retail staff are the front line to prevent the tampering of PIN entry devices (PEDs) used as part of any card acceptance set-up. So, it's important that they're aware that criminals pose as maintenance personnel to tamper with card acceptance equipment. And they're trained to recognise the tell-tale signs of PED tampering.

We've designed an A3 poster for display in staff break areas and a check-list for training purposes. These are available as print-ready, high resolution pdfs and are free to Blackfoot customers from your Blackfoot sales representative.

EVENTS

BEEN & GONE

Webinar: Internet organised crime and the the case for security

Originally broadcast 01 December 2014 and 09 March 2015.

Now available on the Blackfoot UK Ltd YouTube channel.

Webinar: Data privacy

Originally broadcast 19 January 2015. This webinar will be repeated on 06 April 2015, see below for registration details.

Webinar: Security in the cloud: a shared responsibility?

Originally broadcast 09 February 2015. This webinar will be repeated on 11 May 2015, see below for registration details.

Workshop: Risk and reward

PCI London 2015, 22 January 2015.

Now available on the Blackfoot UK Ltd YouTube channel.

Keynote speech: Can I trust cloud security?

SC Congress London, 03 March 2015.

Panel discussion: The evolution of advanced threats

Information Security Careers Network (ISCN), 18 March 2015.

COMING SOON

WEBINAR: DATA PRIVACY

Monday 06 April 2015, 12.00-12.45pm

Hardly a day goes by without another information security or privacy standard being announced, or so it seems. This begs the question, are the standards joined up? Moreover, who do they serve, how does an organisation balance the needs of the business, customers and regulators, and what will this cost?

Matthew Tyler will demystify the main requirements of the new standards, their intent and risks. He will also explore whether regulation, and more regulation, is the answer.

> **https://www.eventbrite.co.uk/e/data-privacy-web-seminar-6th-april-registration-15301788060**

WEBINAR: SECURITY IN THE CLOUD: A SHARED RESPONSIBILITY?

Monday 11 May 2015, 12.00-12.45pm

Changes in technology and working practices are heralding a new era of BYOD (bring your own device) as well as WOAD (work on any device) made possible by cloud computing. Growing numbers of organisations are meeting these challenges through secure managed services and infrastructure providers. But are roles and responsibilities adequately defined, and do they comply with emerging regulation?

Matthew Tyler will examine the drivers for change, the impact of evolving data privacy and governance relations on security, and how your business can position itself for success.

> **https://www.eventbrite.co.uk/e/security-in-the-cloud-a-shared-responsibility-11th-may-2015-registration-16167810356**

WEBINAR: INFORMATION SECURITY AND THIRD PARTY SUPPLIERS

Monday 08 June 2015, 12.00-12.45pm

Criminals are increasingly targeting third party suppliers. Their own information may be valuable. And if they also have authorised access to systems and sensitive data, such third parties may be a stepping stone for an attack on another entity — a practice known as 'island-hopping'.

Version 3.0 of the PCI DSS clarifies and tightens some of the requirements around third party service providers and outsourcing arrangements. Quite apart from this, it is sound business practice to understand who has access to your environment and could affect the security of it, and where responsibilities lie if things go wrong.

Matthew Tyler will explore the background to outsourcing and extended enterprise risk, and the essential elements of third party management.

> **https://www.eventbrite.co.uk/e/information-security-and-third-party-suppliers-8th-june-2015-registration-16154018103**

WORKSHOP: CYBERCRIME - IS YOUR BUSINESS SECURE?

Tuesday 31 March 2015, 08.00am-12.30pm

Plus Accounting, Chartered Accountants, myhotel, Brighton

The internet is increasingly becoming part of of our personal and professional lives — and so is internet crime. Security doesn't have to be only about IT. It can also be about people and protecting your business against data loss and breaches. In this workshop, we discuss cybercrime and how you can protect your business.

> **https://www.eventbrite.co.uk/e/cyber-crime-is-your-business-secure-tickets-157409666550**

blackfoot

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

ADVISE >
ASSESS >
ASSURE >