

Blackfoot Updates + News in Brief

THE EVOLUTION OF THIRD-PARTY RISK MANAGEMENT

How TPRM is changing, and why your business needs to act now

In an era of increasing digital interconnection and complex supplier ecosystems, traditional approaches to third-party risk management simply aren't keeping pace. As outlined in our latest blog, Third-Party Risk Management: The Evolution, the landscape of TPRM is undergoing a fundamental shift, and organisations must evolve with it to protect themselves.

Why the Old Model No Longer Works

Most third-party risk programmes fail not because of a lack of tools, but because supplier risk moves faster than the models used to manage it. Traditional methods; spreadsheets, periodic questionnaires and point-in-time checks, provide a static picture that's quickly out of date. Suppliers change, access expands, services grow, and risk evolves, often without any formal reassessment.

The Reality Today

- **Supply chains are dynamic:** New vendors are onboarded frequently, existing partners broaden their services, and systems change rapidly, outpacing traditional risk reviews.
- **Point-in-time due diligence isn't enough:** Initial onboarding checks matter, but they don't reflect what's happening now. Many suppliers originally deemed "low risk" become critical over time without updated scrutiny.
- **Tooling by itself won't fix it:** Tools are only effective when paired with ownership, governance and continuous activity. Without a clear operating model, even the best platforms fall short.

The Future of Effective TPRM

Modern TPRM is continuous, contextual and actively owned. It's no longer a periodic compliance exercise, it's an ongoing operational capability that must adapt in real time.

Key characteristics of leading programmes include:

- Ongoing risk visibility rather than snapshot assessments.
- Clear ownership and decision rights across the supplier lifecycle.
- Automation and integrated data flows that keep pace with change.
- Supplier risk viewed in context with internal cyber risk and business impact.

What this Means for You

Effective third-party risk management enables businesses to:

- Detect changes in supplier risk early
- Prioritise based on real business impact
- Respond proactively to emerging threats
- Build trust with partners through clearer expectations and transparency

This evolution transforms third-party risk from a compliance "tick-box" into a strategic advantage.

PRODUCT FEATURE PAGE

Third-Party Risk Management

Continuous confidence in supplier cyber risk

Third-party cyber risk is one of the most common causes of security incidents, yet it remains one of the least mature threats in many organisations.

What is TPRM?

Third-party risk management (TPRM) is the continuous process of identifying, assessing, managing and monitoring the cyber, data protection and operational threats introduced by third parties.

Effective TPRM answers four key questions:

- ✓ Who are our third parties?
- ✓ Which suppliers pose the greatest risk?
- ✓ What risks do they introduce?
- ✓ Are those risks being actively managed over time?

Our third party risk management service helps organisations identify, assess and continuously monitor supplier cyber risk.

We move you away from spreadsheets and one-off questionnaires towards a scalable, defensible and ongoing approach to managing third-party risk.

Why organisations choose Blackfoot



Managed,
not DIY



Reduce risk, show
value, quickly



Built for continuous
assurance



Risk-based, not
checkbox-driven



Aligned to recognised
frameworks



Designed to
scale

Start with a Third-Party Risk Management Readiness Assessment to understand your current supplier risk exposure and define a practical, scalable path forward.

PCI DSS: WHY EMPLOYEE CHURN MATTERS

When most people think about PCI DSS, they picture firewalls, encryption, and penetration tests. Technical controls naturally dominate the conversation. But in practice, one of the most significant risks to PCI DSS compliance isn't found in your firewall or code, it's in your people.

High staff turnover, or the revolving door problem, quietly undermines compliance programmes every year. If your people come and go faster than your processes can keep up, the chances are you're carrying risk without realising it. This isn't just a theoretical issue. As QSAs, we see it first-hand: environments where good people have left, their knowledge has gone with them, and compliance has become fragile.

Let's explore where churn hits hardest, why it matters for PCI DSS, and what you can do about it.

Where Employee Churn Undermines PCI DSS

Policy and awareness:

PCI DSS requires annual security awareness training. That's fine on paper, but in a high-churn environment, you constantly have new staff who may never have been onboarded into PCI DSS responsibilities. The risk? Policies that look good in an audit pack but don't reflect reality on the shop floor or in the call centre.

Access control and user management:

One of PCI DSS's fundamentals is ensuring only the right people have the proper access at the right time. When joiners, movers, and leavers processes don't keep pace with reality, dormant accounts linger and excessive privileges build up. These are red flags for both security risk and compliance failure.

Knowledge gaps:

In many businesses, a handful of individuals are the ones who really understand how cardholder data is stored, transmitted, or protected. When they leave, entire chunks of operational knowledge disappear. Their replacements may not know why something was configured a certain way, which makes assessments more painful and ongoing compliance much weaker.

Evidence continuity:

Compliance lives and dies on evidence. If last year's team gathered logs, screenshots, and records one way, and that person has since moved on, there's often no repeatable process in place. We frequently find ourselves asking, "How did you demonstrate this control last year?" – only to be met with blank stares.

You Can Read More Here



UK GOVERNMENT LAUNCHES AMBITIOUS CYBER ACTION PLAN

Securing public services in an era of evolving digital threats

In an age where cyber threats are increasingly sophisticated and disruptive, the UK Government has unveiled its Government Cyber Action Plan, setting out a bold vision to protect public services, enhance resilience, and build trust in digital government. Published in January 2026, the plan responds to escalating threats from hostile states and organised crime, alongside systemic vulnerabilities revealed by past cyber incidents.

"Public services must be secure, resilient, and trustworthy," the government states. This plan represents a decisive step toward that goal.

Why Now? The Growing Threat Landscape

Cyber threats are no longer hypothetical. From ransomware attacks that cripple critical services to sophisticated breaches targeting national infrastructure, the risks are real and escalating. Legacy IT systems and inconsistent cyber practices across government departments have left digital services exposed.

The UK Government Cyber Action Plan recognises this challenge and seeks to build a system capable of preventing, detecting, and responding to cyber threats in real time. Its aim is not only protection but also public confidence, citizens and businesses need to trust that government services can withstand digital threats.

Four Strategic Objectives

At its core, the plan revolves around four strategic priorities:

Better Risk Visibility – Establish consistent, data-driven insight into cybersecurity and resilience across government. Understanding risk is the first step toward managing it.

Address Critical Vulnerabilities – Prioritise and tackle severe and complex risks that cannot be solved by single departments alone.

Enhance Responsiveness – Improve the ability to detect, respond to, and recover from fast-moving cyber incidents.

Scale Cyber Resilience – Replace outdated systems, implement effective security controls government-wide, and share lessons learned across departments.

These objectives aim to create a cohesive, government-wide approach to cyber security that moves beyond reactive measures to proactive, data-driven strategies.



Government

A New Operating Model

The plan introduces a centralised cyber operating model, led by the Government Cyber Unit (GCU), backed by over £210 million in funding. Its mission is to support departments, standardise practices, and drive accountability.

The delivery will unfold in three phases:

- **Build (2026–2027):** Establish governance, leadership, and a Government Cyber Profession to attract and retain talent. Launch central services and set performance targets.
- **Scale (2027–2029):** Expand services, refine risk prioritisation, and enhance cross-government incident response capabilities.
- **Improve (2029 onwards):** Continuously refine cyber capabilities, strengthen supply chain security, and embed professional development across the government cyber workforce.

This phased approach has been designed to ensure a sustained, evolving improvement rather than a one-off fix.

Supporting Departments and Public Services

While departments remain responsible for their own cyber security, the plan strengthens accountability and support:

- A centralised service catalogue will help organisations access guidance, tools, and services efficiently.
- Shared solutions will tackle common challenges across the public sector.
- Cross-government incident response and recovery procedures will be standardised, ensuring fast, coordinated action when incidents occur.
- A structured Government Cyber Profession will provide career pathways, training, and skills development, raising awareness and capability across the workforce.

What This Means for Public Sector Partners

The implications are clear: departments and wider public sector organisations, including local authorities and NHS trusts, will need to align with central standards, improve cyber resilience planning, and leverage shared services.

Collaboration with industry and international partners is also emphasised, recognising that cyber threats are borderless and collective defence is essential.

The plan positions the UK to respond quickly, recover efficiently, and learn continuously from incidents and successes alike.

A Transformative Vision for Cybersecurity

The Government Cyber Action Plan represents a major shift in approach. By moving from fragmented, reactive defences to a centralised, accountable, and data-driven system, the plan seeks to protect the backbone of public services. In essence, it's about building trust in digital government, ensuring that citizens and businesses can rely on the UK's public services, even in the face of increasingly complex cyber threats.

With a clear roadmap, strong leadership, and a focus on people, processes, and technology, the UK is setting a benchmark for how modern governments can tackle the cyber challenge in a coordinated and sustainable way.

Who will be responsible for what?

Government Departments will:

- Understand, manage and report against the cyber risks of their department, ALBs, and wider public sector in alignment with government-wide risk appetites and direction
- Meet specified Accounting Officer responsibilities through establishing roles and responsibilities, governance structures, strategies, plans and processes to support accountability and risk management
- Apply mechanisms to ensure suppliers appropriately manage government risks

ALBs and wider public sector organisations will:

- Understand, manage and report against cyber risk in alignment with government-wide and LGD risk appetites and direction
- Apply mechanisms to ensure suppliers appropriately manage government risk

The Government Cyber Unit will:

- Understand and manage government wide risk on behalf of Government Technology Risk Owners through mandatory policy and assurance against requirements
- Provide departments with specific direction and practical support on how to manage their risk within central and local appetites
- Engage strategic suppliers to ensure resilience outcomes are met and standards raised

NCSC will:

- Provide authoritative technical advice and assessment on management of risk and advise the Government Cyber Unit on setting policies, standards, and baseline appetites

Suppliers will:

- Understand and proactively manage risk in alignment with direction and expectations set out by their contracting authorities or, for strategic suppliers, in line with strategic partnerships expectations



Human Risk Management

Transform Your Workforce into a Proactive Security Asset

"It's enlightening and really easy to use! HRM makes it so much easier to be able to understand and mitigate people-related risk in cybersecurity."

The Challenge: Supporting People in a Complex Threat Environment

- Phishing, social engineering and data mishandling remain the #1 cause of cyber incidents
- Traditional security awareness training is generic, unengaging, manual and ineffective
- Security teams lack visibility into where human risk is coming from and how to reduce it
- Resources are stretched, making personalisation and continuous risk evaluation very difficult

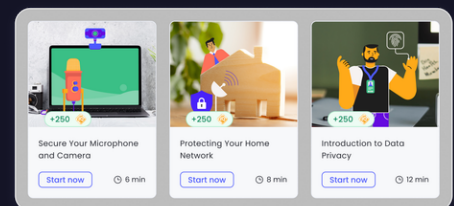
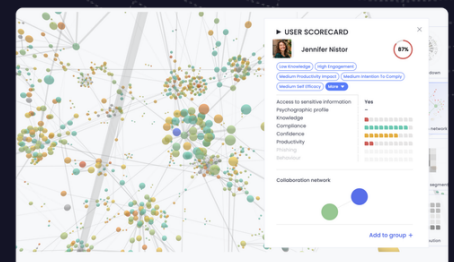
The Solution

Combine and automate the best of adaptive training and adaptive security to prevent human-initiated security incidents.

- ✓ **Human Risk Intelligence**
Real-time dashboards showing risky behaviours, trends, and high-risk groups.
- ✓ **Adaptive Security Training**
Personalised, role-specific learning that actually changes behaviour.
- ✓ **Smarter Phishing Simulations**
AI-generated simulations mirroring real attacker tactics.
- ✓ **Behaviour-Driven Security Controls**
Connect user risk scores to identity platforms to reduce exposure automatically.

Business Impact

- ✓ **Reduce Human-Initiated Incidents**
Fewer phishing clicks, fewer data handling mistakes, fewer breaches.
- ✓ **Improve Workforce Resilience**
High engagement and measurable behavioural improvement.
- ✓ **Focus Security Resources**
Prioritise the right people and prove ROI to leadership.



Trusted by enterprise CISOs, Security Teams, GRC Professionals and Awareness Leaders across all sectors

GLOBAL CYBERSECURITY OUTLOOK 2026:

KEY INSIGHTS FOR LEADERS

The World Economic Forum's Global Cybersecurity Outlook 2026 underscores a rapidly evolving cyber risk landscape that now sits at the intersection of technology, geopolitics, and business strategy. Cybersecurity is increasingly a board-level concern, with threats moving beyond traditional technical domains into areas that impact trust, finance and organisational resilience.

AI: The Leading Driver of Cyber Risk

AI is identified by 94 % of global leaders as the biggest driver of change in cybersecurity. At the same time, 87 % report that AI-related vulnerabilities grew faster than any other risk category over the past year. AI is a double-edged sword: while it improves detection and response, it also enables sophisticated threats, from automated social engineering to generative AI data exposure. Notably, the share of organisations that have integrated AI risk into governance has nearly doubled, rising from roughly 37 % to 64 % year-on-year, reflecting growing awareness of AI's security implications.

Geopolitics Is Now a Core Cyber Factor

Cybersecurity strategies are increasingly influenced by geopolitical tensions. 91 % of large organisations have adapted their cyber approaches in response to geopolitical uncertainty, while only 31 % of leaders express high confidence in their nation's ability to respond to a major cyber incident. This shift signals that cyber risk can no longer be viewed in isolation, economic and political factors must be integrated into risk assessments, planning and cross-border operations.

Turning Cyber Strategy into Measurable Business Outcomes

There is a growing gap between cybersecurity ambition and execution. While most organisations now recognise cyber risk as a strategic priority, far fewer are able to measure cyber resilience in business terms. Many leaders report difficulty demonstrating return on security investment, linking controls to reduced risk, or quantifying preparedness for major incidents. This lack of clear metrics weakens decision making, slows investment and can leave boards with limited visibility of true exposure. The importance of moving beyond technical indicators and towards business-aligned metrics, such as operational disruption, financial impact, regulatory exposure and recovery capability, enabling cybersecurity to be governed with the same discipline as other enterprise risks.

Organisations that succeed will be those that:

- Treat AI security and governance as core risks
- Integrate geopolitical and business risks into their cyber frameworks
- Align security priorities with executive leadership concerns
- Invest in supply chain risk management

Cyber Fraud Surpasses Traditional Threats

The rise in cyber-enabled fraud has resulted in 73 % of organisations reporting experiences of fraud during the past year, placing it above more familiar threats such as ransomware in executive risk priorities. The elevation of fraud reflects its direct financial and reputational impact and highlights a widening gap between executive concerns (fraud and business impact) and technical teams' focus (ransomware and system attacks). Effective communication between security and leadership is now essential to align priorities and investments.

Supply Chain Risk and Capability Gaps

Supply-chain vulnerabilities remain a top challenge, with 65 % of large organisations citing third-party risk as their greatest barrier to resilience, up from 54 % in the prior year. These dependencies extend risk across ecosystems, making strong third-party risk programmes and continuous monitoring indispensable. The report also highlights persistent cyber capability gaps, with many organisations still lacking sufficient skilled personnel and mature controls, reinforcing systemic fragility across sectors.

BLACKFOOT UPDATES

PRIVACY IMPACT SHOP PODCAST



Your essential podcast on data protection and privacy, hosted by Blackfoot's Shaab Al-baghdadi and Ben Stevens, simplifying complex topics and featuring industry guests.

Stay informed by watching on YouTube or listening on Spotify, Apple, Amazon, RSS Podcast, and Podcast Addict.



PCI LONDON 2026

Blackfoot were delighted to return to PCI London 2026.

As a long-standing sponsor and partner of PCI London, Blackfoot brought nearly 15 years of involvement in supporting this annual event. It was a pleasure to connect with industry peers and partners once again in January



CUSTOMER ROADSHOWS

Our team have been busy supporting our clients with a series of customer cybersecurity awareness roadshows.

Blackfoot provided complimentary training to help employees recognise cyber threats and stay secure at work and home, at locations including Heathrow, Gatwick, and Manchester airports.



PECB CDPO TRAINING



9-11 MARCH

PECB is a globally recognised certification body providing education, certification and certificate programmes across a wide range of disciplines. Its credentials are supported by numerous accreditation bodies, giving professionals strong recognition in both domestic and international markets.

The **PECB Certified Data Protection Officer (CDPO)** training course equips individuals with the knowledge and skills required to effectively perform the role of a Data Protection Officer (DPO) within an organisation. The programme focuses on ensuring compliance with the General Data Protection Regulation (GDPR) and other relevant regulations, covering key areas such as GDPR principles, regulatory requirements and the responsibilities of a DPO.

Contact us to find out more or to secure your place.



BLACKFOOT UPDATES

BLACKFOOT TURNS 17!

For 17 years, Blackfoot has protected businesses from evolving cyber threats while helping them meet industry standards and regulatory requirements. Entirely director owned and managed, every decision we make is in our clients' best interests, ensuring the delivery of unbiased and trusted solutions.

As cyber-attacks continue to grow in both volume and sophistication, including AI-enabled threats and attempts from increasingly unskilled actors, Blackfoot remains committed to helping organisations stay ahead of emerging risks and safeguarding their digital assets and operations.

17

Your trust, collaboration and partnership are what make our work possible. We're proud to support you and grateful to be part of your security journey.

2026

We have been making significant progress on some exciting developments, and we're looking forward to sharing more with you soon.

Sign up to get your exclusive updates.



A VERY WARM WELCOME TO BLACKFOOT



Harry Hammond

Harry joins Blackfoot with over ten years' experience in the IT sales space, including the last five years specialising in cybersecurity. Working closely with clients across a range of sectors, Harry supports organisations in understanding risk, scoping the right security services, and aligning technical assurance and advisory work to real business needs.

Harry's background includes building long-term client relationships, translating complex cyber concepts into clear commercial outcomes, and collaborating closely with technical and advisory teams to deliver meaningful security improvements.



Tony Unger

Tony joins Blackfoot in the role of Principal vCISO Consultant within our Advisory team. As a recognised technology & security industry expert with over 20 years experience, Tony delivers a broad range of consultancy and advisory offered by Blackfoot, with a particular focus on the Virtual Chief Information Security Officer engagements.

Dedicated expertise consists of real-world hands-on security research & testing through to strategic technology leadership; covering the full end-to-end lifecycle of large scale big data & payment platforms, critical national infrastructure systems, alongside blockchain and artificial intelligence applications.

NEWS IN BRIEF

Our take on the latest industry news

In December 2025, the City of London Police launched a new national fraud reporting service, Report Fraud, replacing the former Action Fraud system, with a full public launch in January 2026. While hosted by the City of London Police, this force is the UK's national lead for fraud and economic crime, meaning the service is designed for everyone across England, Wales and Northern Ireland.



Report Fraud provides a modern, streamlined way for individuals and businesses to report fraud and cyber crime, offering clearer guidance on what to report, how information will be used, and improved support for victims. The service creates a single national reporting gateway, strengthening intelligence sharing, helping law enforcement identify serious and complex cases more quickly, and improving the overall response to fraud across the UK.

Fraud can now be reported online at reportfraud.police.uk or by calling **0300 123 2040**, as Action Fraud is phased out.



A former Google software engineer, has been convicted in the US of economic espionage and theft of AI trade secrets after a federal jury found he stole thousands of confidential documents related to Google's artificial intelligence technology to benefit China-based companies, including a startup he was involved in founding. The jury convicted him on seven counts of economic espionage and seven counts of trade secret theft after evidence showed he transferred more than 2,000 sensitive files from Google systems to his personal cloud account while still employed, then downloaded them onto his own device shortly before resigning.

Prosecutors described this as a serious breach of trust involving advanced AI infrastructure and national security implications, as the stolen material included details about supercomputing hardware and software that underpin Google's AI systems.

He faces decades in prison, with sentencing pending in early February 2026, underscoring how seriously authorities are treating insider theft of strategic technology.



Information Commissioner's Office

The UK's data protection regulator, has launched a formal investigation into the Grok artificial intelligence system over serious concerns about how it handles personal data and whether sufficient safeguards were put in place to stop the generation of harmful content.

The probe covers social media platform X and X.AI (the companies behind Grok) following reports that the chatbot was used to create non-consensual sexualised and deepfake imagery of individuals, including children. These reports raise "serious concerns" under UK data protection law about whether personal data was processed lawfully, fairly and transparently, and whether appropriate protections were built into the system's design and deployment.

William Malcolm of the ICO emphasised the risk of significant harm when people lose control of their personal data. The investigation will assess compliance with data protection requirements and coordinate with other regulators, including Ofcom, as part of wider efforts to ensure safety and privacy in digital services.