JANUARY 2026

inside zh=ro

Win £50

Defend As One

UK Cyber Action Plan

The Future Secured

Zhero Talks 2026

Quantum Cyber Phoenix

Cyber London's Quantum-Safe Train

Message from Izak

Welcome to the first edition of Inside Zhero in 2026.

As we head into another year of exciting developments in the cyber world, I'd like to take this opportunity to wish one and all a belated Happy New Year. Exciting times are ahead, with the best yet to come from Team Zhero.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Defend As One" examines the impact of the new UK Government Cyber Action Plan.

58 critical UK public systems have been identified with serious cyber resilience gaps.

"I welcome the UK Government's Cyber Action Plan. It represents a bold, much-needed step toward strengthening the resilience of public services and protecting citizen data. By prioritising accountability, rapid response, and skills development across government, this plan not only addresses today's threats but also lays the foundation for a safer, more secure digital future. At Zhero, we're ready to support this initiative and help ensure these goals become a reality."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

50% discount **cyberzhero542**

DEFEND AS ONE

In an era where digital services underpin almost every function of modern government, the United Kingdom has recognised a stark reality: cyber resilience across public services remains critically high-risk. On 6 January, the Government Cyber Action Plan was published, setting out a bold strategy to transform how government protects its digital infrastructure and public services against an increasingly sophisticated landscape of cyber threats. The Plan forms a central pillar of the UK's Roadmap for a Modern Digital Government, the wider blueprint for secure, trusted, and resilient digital public services.

At its heart, the Cyber Action Plan represents a concerted effort to move beyond guidance and aspiration, embedding mandatory standards, clear accountability, centralised support, and measurable outcomes for cybersecurity across government departments and public bodies. Supported by over £210 million in central investment, the initiative reflects both the urgency and scale of addressing vulnerabilities that have persisted despite previous strategic frameworks.

The Threat Landscape

Modern governments face a spectrum of cyber threats that range from organised criminal gangs to hostile state-linked actors. Incidents such as ransomware attacks, supply-chain infiltrations, and breaches of critical infrastructure have underscored the consequences of inadequate security. As services become more interconnected — and as citizens increasingly interact with government online — the stakes are higher than ever: service disruptions can damage public trust, threaten national security, and have tangible real-world effects on healthcare, welfare, and critical infrastructure. Despite years of prior strategies and guidelines, the Plan acknowledges that government cyber risk remains critically high, hampered by fragmented accountability, underinvestment in digital infrastructure, and reliance on outdated systems. This reality frames the urgency and ambition of the new cybersecurity agenda.

Strategic Vision and Purpose

The Government Cyber Action Plan sets out to achieve a simple yet powerful goal: to secure public services so they are trustworthy and resilient for citizens and businesses alike. It does this by specifying what government organisations must do to manage cyber risk effectively, moving past voluntary guidance toward mandatory expectations, structured support, and clear leadership.

The Plan is led by the Department for Science, Innovation & Technology (DSIT) and is implemented through a newly established Government Cyber Unit. This central body exists to coordinate activity, enforce accountability, provide expert support, and ensure consistent standards across all government departments, agencies, and associated public bodies.

Strategic Objectives

The UK Government Cyber Action Plan sets out four strategic objectives to strengthen cyber resilience across public services.

- **Better Visibility of Cyber Risk -** Effective action begins with a clear understanding of vulnerabilities. Historically, departments have held fragmented views of risk. The Plan seeks to integrate data across government, apply consistent metrics, and embed risk insights into decision-making and investment, enabling targeted interventions where they will have the greatest impact.
- **Addressing Severe and Complex Risks -** Certain threats, such as persistent nation-state activity or systemic software vulnerabilities, exceed the capacity of individual departments. The Plan establishes central oversight, coordinated remediation, and investment in capabilities that protect multiple organisations, shifting from reactive defence to proactive, government-wide risk management.
- **Improving Responsiveness to Fast-Moving Events -** Cyber incidents can escalate rapidly. Strengthened responsiveness includes a Government Cyber Incident Response Plan, enhanced cross-department collaboration, and accelerated recovery efforts, ensuring damage is contained quickly and efficiently.
- **Rapidly Increasing Cyber Resilience Across Government -** Every public body must be able to resist and recover from threats. Central services, remediation of legacy systems, and knowledge-sharing underpin this objective. Continuous improvement, evaluation, and cross-government community building ensure resilience is sustained and strengthened over time.

Together, these objectives provide a coordinated, data-driven, and actionable framework to protect the UK's digital infrastructure and public services from evolving cyber threats.

Phased Delivery

Recognising the scale of transformation required, the Plan unfolds over three sequenced phases — each with specific milestones and targets.

Phase 1: Building - by April 2027

During this phase, the groundwork is laid by:

- Establishing the Government Cyber Unit at full operational strength.
- Refreshing governance and accountability across departments.·Implementing early central services and support capabilities.
- Setting clear, measurable standards and targets for organisational cybersecurity.

The emphasis is on creating the model that future scaling and improvement will depend on.

Phase 2: Scaling - April 2027 – April 2029)

With the model in place, phase two focuses on:

- Expanding and maturing cyber services across government.
- ·Embedding data-driven decision-making and investment processes.
- Strengthening the incident response and recovery ecosystem.
- Developing structured career pathways and learning programmes in cyber professions.

This phase operationalises the central standards and enables departments to align with them at scale.

Phase 3: Improving - April 2029 and beyond

In the third phase, the Plan shifts toward continuous improvement, emphasising:

- Evidence-led investment in cross-government platforms.
- Sustainable service delivery models tailored to persistent needs.
- Proactive assurance of cyber resilience across supply chains.
- Integration with national security and economic growth strategies.

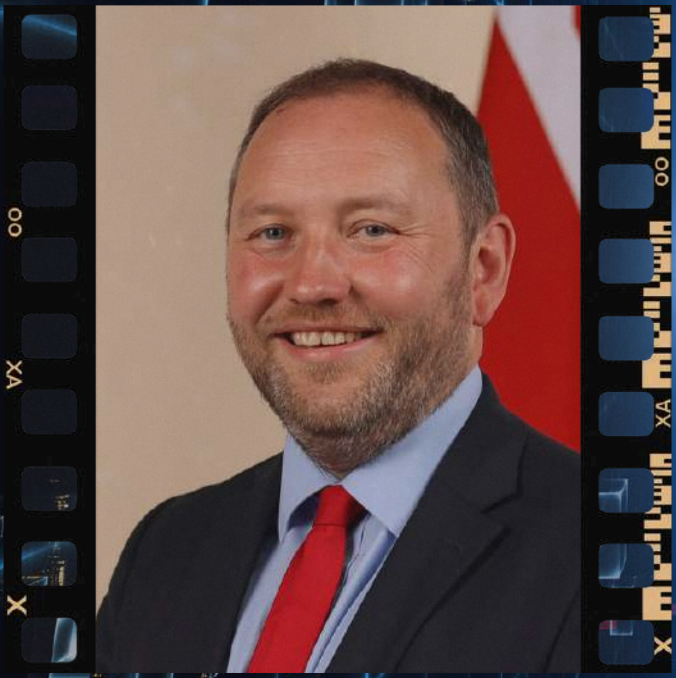
This enduring effort reflects the reality that cyber threats will evolve and require ongoing attention.

Workforce Transformation

Technical tools and standards alone are insufficient. People are central to defence. The Plan therefore establishes a Government Cyber Profession, the first cross-government professional body for cyber security and resilience. The goal is to:

- Attract top talent with competitive job offers and structured recruitment pathways.
- ·Upskill existing employees through formal learning and accreditation.·Retain skilled professionals through career development, community building, and competitive frameworks.
- Support all government staff with awareness training to reduce human-factor vulnerabilities.

This emphasis acknowledges that workforce shortages and skills gaps are among the most persistent barriers to effective cyber defence.



"We are not starting from scratch; we are scaling what works, learning from successes across the public sector and our international partners. This plan will go further than we have before, prioritising cyber resilience and ensuring we have strong central leadership driving cross-government response.."

Ian Murray
~ Minister of State for the Department for Science, Innovation and Technology

Public Confidence and Trust

A recurring theme throughout the Plan is the need to safeguard public trust in government digital services. As vital functions, from tax filing to healthcare booking, move increasingly online, citizens must be confident that these interactions are secure and reliable. This urgency is underscored by recent national cyber threat data showing that the UK's National Cyber Security Centre handled an average of four nationally significant cyber attacks every week, with 204 such incidents recorded in the year to September 2025, which is more than double the number from the previous year. The Plan's holistic thrust towards visibility, responsiveness, resilience and accountability is ultimately aimed at ensuring that technology works for people and not against them. By improving risk visibility across departments, enhancing rapid incident response, coordinating remediation of complex risks, and strengthening resilience in every public body, the Cyber Action Plan seeks to underpin citizens' confidence in digital public services. This comprehensive approach not only strengthens the protection of government infrastructure but also fosters a culture where public trust in online services is actively reinforced and maintained in the face of evolving cyber threats.

FACT

- **£210m committed by the UK Government to tackle critically high cyber risk across public services**
- **28% of the government technology still runs on outdated legacy systems**
- **200+ nationally significant cyber attacks handled in a single year, roughly 4 per week**
- **43% of UK businesses suffered a cyber attack or breach in the last 12 months**
- **Up to 93% of cyber incidents involved phishing as the initial attack vector**

LOOKING AHEAD

The Government Cyber Action Plan marks a significant shift in UK public-sector cybersecurity policy, recognising that broken silos, legacy technology and light-touch guidance are no longer sufficient in a world of active and evolving threats. The Plan embeds mandatory expectations, unified accountability, centralised support and a skilled workforce to not only defend but future-proof government cyber resilience. Its success will hinge on sustained investment, cross-government cooperation, regular evaluation and, crucially, the ability to adapt as the threat landscape changes. The urgency of this shift is reflected in data showing that 60 per cent of UK public-sector IT leaders believe a successful cyberattack on their organisation is only a matter of time without proactive measures. For citizens, officials and industry partners, this Plan signals a renewed commitment to protecting the digital foundations of public life, strengthening both trust in online services and the resilience of essential government functions against ever-greater cyber risks.

2026 and BEYOND

Our amazing Head of Operations & Finance, Natasha Botha, gives us her spin on what to expect from Zhero in 2026.

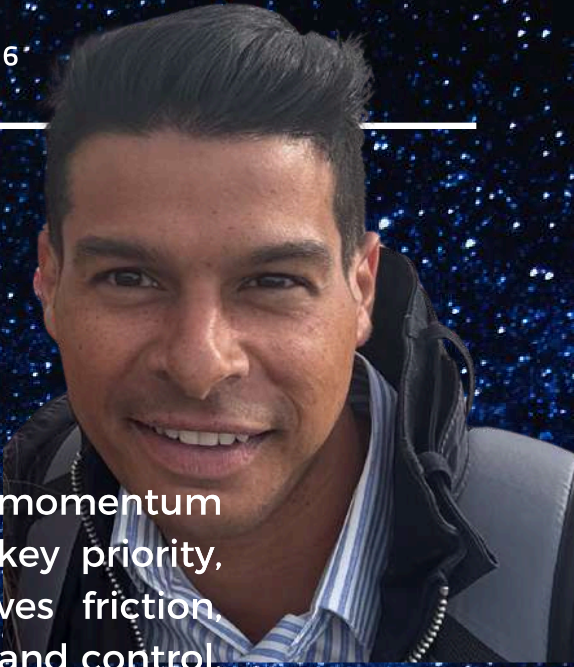
In account management, we will prioritise proactive infrastructure improvements, such as cabinet and cable clean-ups, along with structured renewals and upsell initiatives for CES/CES+, SharePoint, and Azure. We are also finalising updates to client location suppliers, ensuring consistency, compliance, and faster service delivery across all sites.

Operational and financial efficiency is another key pillar for the year ahead. We are aligning supplier contracts within Zhero Wait, completing asset reconciliations across Zhero Wait, N-able, and Xero, and improving the flow between ticketing, asset management, and invoicing. These initiatives are aimed at increasing accuracy, reducing manual intervention, and giving both our teams and clients clearer visibility of services and costs.

People and performance will remain at the heart of everything we do. In 2026, we will further invest in recruitment, skills development (particularly in Microsoft and Fortinet certifications), and building a consistently high-performing team. Alongside this, we are revamping our Operations Manual and refining standby and late-shift structures to ensure scalable, reliable support as we continue to grow.

Finally, our marketing strategy will become more targeted and measurable. We aim to host one to two breakfast events per month, generate at least 120 sales-qualified leads, and focus our messaging on business leaders rather than only IT professionals. With a strong emphasis on metrics, traceability, and brand presence, we will strengthen Zhero’s position as a trusted business technology partner.

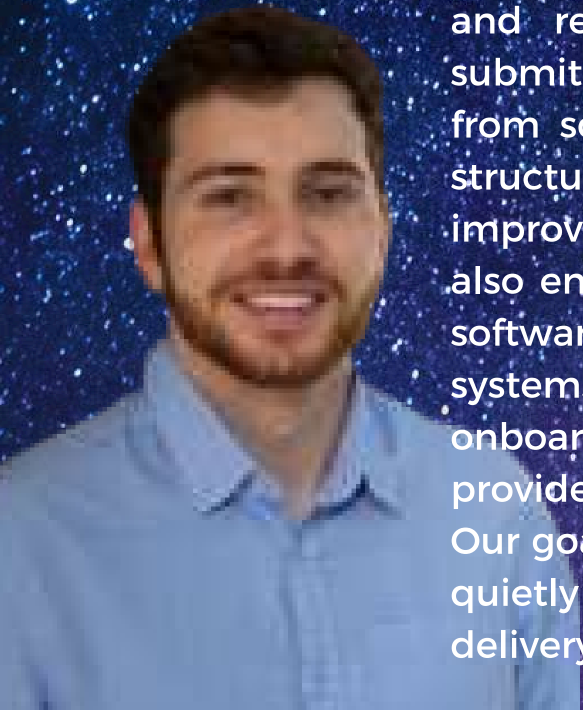
zhero



Zaheer Raman, our incredible Head of Engineering, provides his insight into the upcoming year

My focus for 2026 is building calm, dependable momentum across everything we deliver. Zhero Wait is a key priority, designed as a workflow platform that removes friction, reduces delays, and gives teams clearer visibility and control. . Alongside this, we are expanding structured knowledge bases for assets and services to improve consistency and speed of support. We are also investing in third-party vendor certification partnerships, ensuring every supplier and integration meets the same high engineering and security standards our customers expect as we scale into 2026.

Last, but not least, we hear from the talented Wesley Harris, our Head of Development since 2019.



My priority is delivering tools that reduce friction for both our teams and our clients. Our key initiative is the Projects Portal, improving project visibility and collaboration, while giving clients a clear, structured way to define requirements with minimal ambiguity.We'll also streamline internal workflows by pre-drafting quotations and related assets directly from client requirements submitted through the Projects Portal. Instead of starting from scratch each time, teams will review and refine a structured draft, reducing manual administration, improving consistency, and speeding up turnaround. This also ensures a complete sync between our in-house PSA software and N-able so information moves reliably across systems without manual effort. Finally, we're accelerating onboarding clients to Operations Insight and Risk portal to provide better visibility, reporting, and actionable insights. Our goal for 2026 is to integrate scalable systems that run quietly in the background, freeing people to focus on delivery, not administration.

FUTURE QUANTUM

QUANTUM THINK TANK

Last December, Cyber London launched its innovative Quantum Security Think Tank. The Think Tank promises to be a global hub where top minds from academia, industry, government, and non-profits unite to shape the future of quantum technology. By addressing security risks, ethical challenges, and regulations, it ensures that quantum advances aren’t just smart but safe, fair, and valuable to society. Through collaboration and insight, the Think Tank is turning quantum potential into real-world progress that benefits everyone.

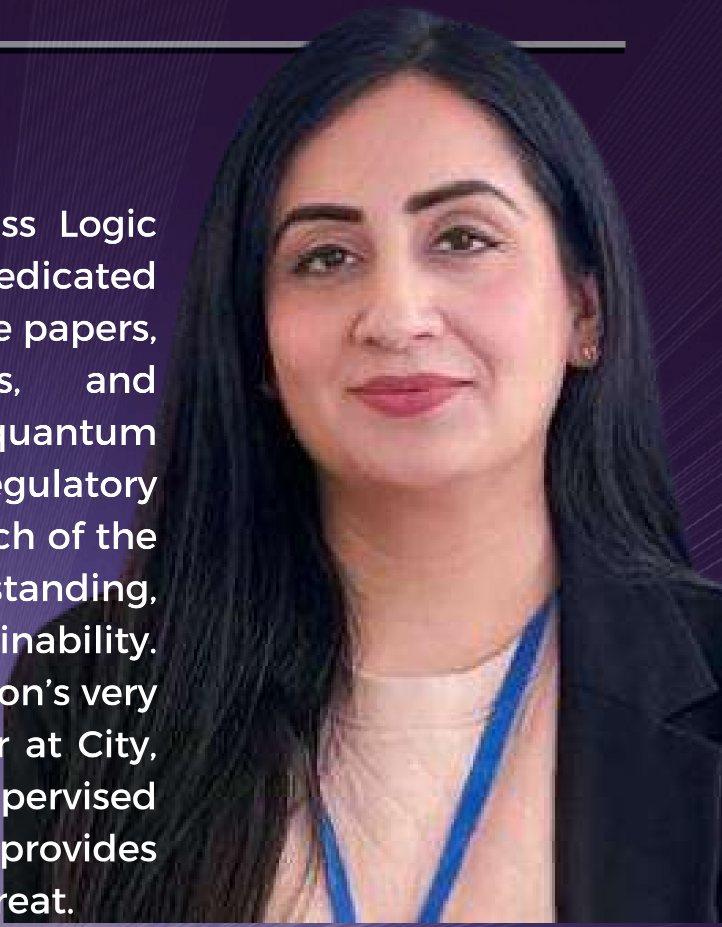
QUANTUM SAFE READINESS LOGIC TRAIN

Now, Cyber London is super excited to release its Quantum Safe Readiness Logic Train, a practical framework that helps organisations prepare for a post-quantum world with a practical roadmap across five key phases.

- **Awareness** - Recognise the quantum threat, understand risks, and see why immediate action is essential.
- **Understanding** - Build a foundation with PQC knowledge, quantum-safe principles, and regulatory insight.
- **Preparation** - Plan your migration, adapt systems, implement governance, and ready your workforce.
- **Implementation** - Deploy, test, validate, and refine quantum-safe solutions through pilots and real-world applications.
- **Sustainability** - Maintain long-term resilience with monitoring, innovation, collaboration, and strategic planning.

Here’s the Think Tank: Cyber London Quantum Security

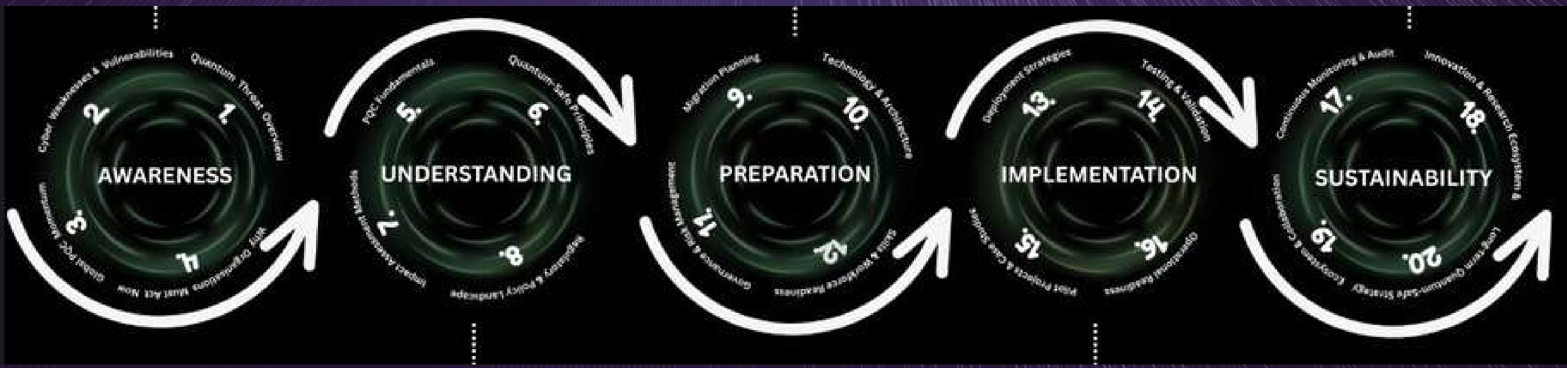
QUANTUM RESOURCES HUB



As part of the Quantum Safe Readiness Logic Train, Cyber London has developed a dedicated resource hub, a curated selection of white papers, policy briefings, technical reports, and collaborative insights focused on quantum security, risk and audit, and regulatory preparedness. The resources focus on each of the 5 phases – awareness, understanding, preparation, implementation, and sustainability. The first resource, penned by Cyber London's very own Tooba Qasim, a doctoral researcher at City, St George's, University of London and supervised by Cyber London Director, Raj Rajarajan, provides an insightful overview of the quantum threat.

QUANTUM THREAT OVERVIEW

Quantum computing is advancing rapidly, creating long-term risks for today's cryptography, especially for data that must remain confidential for decades. AI accelerates cyber threats, enabling attackers to "harvest now, decrypt later." The UK NCSC, along with global bodies like NIST and ETSI, has issued post-quantum cryptography timelines, highlighting that migration is a complex, multi-year process requiring awareness, planning, testing, and vendor coordination. Organisations must understand where cryptography is used, which algorithms protect critical data, and how long it must stay secure. Quantum security is no longer a distant specialist topic—it is a practical, urgent concern. Early awareness is essential. CLICK FOR MORE


AWARENESS
1. Quantum Threat Overview
2. Cyber Weaknesses & Vulnerabilities
3. Global PQC Momentum
4. Why Organisations Must Act Now
UNDERSTANDING
5. PQC Fundamentals
6. Quantum-Safe Principles
7. Impact Assessment Methods
8. Regulatory & Policy Landscape
PREPARATION
9. Migration Planning
10. Technology & Architecture
11. Governance & Risk Management
12. Skills & Workforce Readiness
IMPLEMENTATION
13. Deployment Strategies
14. Testing & Validation
15. Pilot Projects & Case Studies
16. Operational Readiness
SUSTAINABILITY
17. Continuous Monitoring & Audit
18. Innovation & Research Ecosystem &
19. Ecosystems & Collaboration
20. Long-Term Quantum-Safe Strategy

Here's the Resoruces Hub: Cyber London Quantum Resources

Meet the team

Elizabeth-Ann Mentor

HR MANAGER

Hi Liz! What made you realise you want to go into the IT industry?

Hi! My path into IT naturally grew from my work in Fraud Examination, Education, and Training in the Financial and Business Services sector, focusing on IT as a key part of delivering effective processes.

What's your most-used productivity tool?

I leverage Microsoft tools, creative platforms, and project management software to boost efficiency and effectiveness in HR, continuously evolving my toolkit to deliver the best results.

How would you describe yourself?

I'm serious about learning, committed to delivering high-quality work, and motivated by being part of positive, collaborative environments.

What do you enjoy the most about your role?

I enjoy planning and anticipating possibilities, designing ways to achieve them, and helping people learn and grow, empowering them to reach their goals.

Do you have any hidden talents or hobbies?

I enjoy exploring creative and technical hobbies, including photography, graphic design, 3D animation, web design, and even dabbling in AI automation.

What is your favourite movie or TV show?

I enjoy fantasy and action genres. Films like Underworld or Resident Evil are the kind I can easily get drawn into.

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos