OCTOBER 2025

inside zhero

Stay Safe Online

Celebrating Cyber Awareness Month

Win £50 amazon voucher

UK Cyber Action Plan

Growth | Leadership | Places

Quantum's Rising Sun

Tooba Hits Osaka

Message from Izak

Welcome to our October edition of Inside Zhero.

This month, it's all things cyber as we look at Cyber Security Awareness Month and the UK Action Plan for Cyber Growth. There's also a special treat in store from Tooba, who details her trip to Japan to present our paper on quantum cryptography.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Stay Safe Online" examines how SMEs and individuals can benefit and build their cyber resilience by applying the 4 basic action points of Cyber Security Awareness Month.

In 2024, there were 8.6 million cyberattacks on UK businesses.

"It's Cybersecurity Awareness Month, and I've been reflecting on how real the threat of ransomware has become. Every year, there are around 600 million ransomware attacks worldwide, about 20% of all data breaches. Here in the UK, it's especially worrying to see that a third of businesses hit by these attacks lose revenue, and one in five have to close their doors for good. It's a sobering reminder of why staying vigilant and investing in cybersecurity isn't optional for any of us anymore."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

50% discount **cyberzhero542**

STAY SAFE ONLINE

Every October, organisations around the world take part in Cybersecurity Awareness Month (CSAM), a global initiative designed to help individuals, communities, and businesses strengthen their defences against cyber threats and develop safer online habits. For small businesses in the UK, this campaign is more than just a date in the diary; it's a chance to recognise just how real the risk is, address weak spots, and embed practices that protect customers, staff, and sensitive information. In 2025, the theme "Stay Safe Online" emphasises taking concrete steps to build resilience against evolving threats and helping create a more secure digital environment for everyone. The campaign's purpose is straightforward yet vital: to raise awareness, offer resources, and support people at all levels — from newcomers to seasoned business owners — in taking proactive action to manage cybersecurity risk. With around 43% of UK businesses reporting a cyber breach or attack in the past 12 months and estimates that global cybercrime could cost the world US$10.5 trillion annually by 2025, the message is clear: staying safe online is a shared responsibility. As part of this global push, the National Cybersecurity Alliance provides adaptable toolkits, guides, and materials that organisations can use to run internal awareness campaigns, shine a light on issues like AI-driven phishing and human error, and nurture a culture of collective vigilance in our digital world.

In the beginning

Cybersecurity Awareness Month began in 2004, launched by the U.S. Department of Homeland Security and the National Cyber Security Alliance to address the growing need for online safety education. Its roots can be traced back to 1987 with the U.S. "National Computer Security Awareness Day," and over the years, the initiative has evolved from a national campaign into a global effort observed every October to raise awareness about cyber threats and promote best practices for staying safe online. In 2009, the campaign introduced a consistent theme, "Our Shared Responsibility," and by 2011, weekly themes were added to provide a more structured focus throughout the month. Most recently, in 2023, a new overarching theme, "Secure Our World," was announced to guide future campaigns, reflecting the ongoing importance of collective action in building a safer digital environment.

#ThinkB4UClick

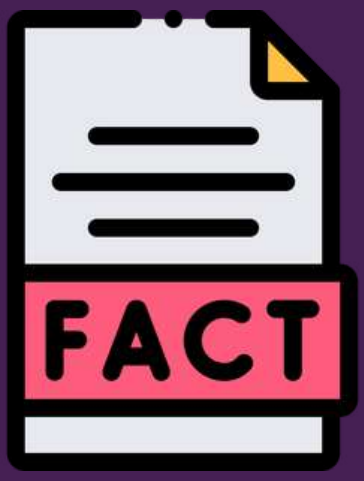
The European Cybersecurity Month (ECSM) is the European Union's annual campaign aimed at promoting cybersecurity among EU citizens and organisations by providing up-to-date online security information, raising awareness, and sharing good practices. Every October, hundreds of activities take place across Europe, including conferences, workshops, trainings, webinars, and presentations, all designed to encourage digital security and cyber hygiene. The campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, with support from EU Member States and hundreds of partners from governments, universities, think tanks, NGOs, professional associations, and the private sector across Europe and beyond. Since its launch in 2012, ECSM has focused on its key priorities under the slogan 'Cybersecurity is a Shared Responsibility,' and in 2020 adopted 'Think Before You Click' as its official motto to further unite participants across Europe against cyber threats.

CSAM in the UK

Launched in the UK in 2012, CSAM is promoted by a range of organisations, including the Department for Science, Innovation and Technology, the NHS, and the cybersecurity training sector. The National Cyber Security Centre (NCSC) is running a campaign focused on phishing and providing resources to help individuals and businesses protect themselves, while the NHS is emphasising back-to-basics approaches to online safety. Several UK universities, including University College London, Royal Holloway, University of London, and the University of Portsmouth, have also organised activities as part of the campaign. The key focus for 2025 is the theme “Stay Safe Online,” which highlights that simple, everyday actions are essential for improving cybersecurity at home, at work, and within the wider community.

"There are only two types of companies: those that have been breached and know it, and those that have been breached and don't know it yet."

John Chambers
Ex-CEO Cisco



- 8.6 million cyberattacks on UK businesses in 2024
- 30% of charities reported at least one cyber breach or attack in the past 12 months
- 85% of affected businesses and charities experienced phishing attacks
- 40% of businesses had 2FA enabled in 2024

Core 4

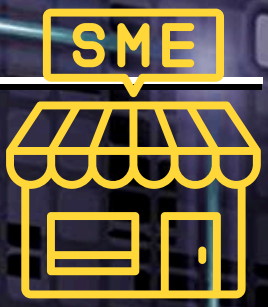
This year, the CSAM campaign focuses on four practical steps or actions, known as the "Core 4," to help everyone stay safer online:

- **Create strong passwords and use a password manager** - Use unique, complex passwords for each account to make it harder for attackers to gain access. A password manager can securely store and generate strong passwords, so you don't have to remember them all.
- **Enable multi-factor authentication (MFA)** - Adding an extra layer of security, such as a code sent to your phone or generated by an app, significantly reduces the risk of unauthorised access even if your password is compromised.
- **Recognise and report scams** - Be alert to phishing emails, suspicious links, and fraudulent messages. Knowing the signs of scams and reporting them promptly helps protect yourself and others from falling victim to cybercrime.
- **Keep your software updated** - Regularly install updates for your operating system, apps, and antivirus software. These updates often contain critical security patches that protect your devices from known vulnerabilities and emerging threats.

By following these steps consistently, businesses and SMEs can create a much safer online environment for their operations and customers. Staying informed and proactive about cybersecurity is one of the best ways to prevent disruptions and protect valuable data.

"Phishing remains unsolvable; there's no patch for human gullibility."

Mike Danseglio
Former Security Manager, Microsoft



CSAM for SMEs

CSAM, and every other month of the year, are especially important for small businesses, which have become increasingly targeted by cyber attackers. SMEs often hold valuable customer data but lack the layered security controls of larger organisations, making them more vulnerable to breaches that can result in regulatory penalties, loss of trust, operational disruption, and reputational damage. By using CSAM as a springboard, small businesses can better understand the importance of security awareness, identify and address risks before they cause harm, equip employees with the knowledge to spot and respond to attacks, and access free resources to support ongoing training and education. While tools like firewalls and antivirus software are essential, people remain the biggest risk in cyber defence—a single careless click on a phishing link can compromise an entire business. Security awareness training is therefore critical, as it teaches staff how to recognise and report scams, builds confidence in spotting unusual requests or suspicious emails, reinforces that cybersecurity is a shared responsibility, and creates a culture where employees feel empowered to protect the business. For SMEs, running awareness training does not have to be costly, as free guides, quizzes, and posters from the National Cybersecurity Alliance and the UK's NCSC can be adapted to keep cybersecurity top-of-mind throughout the year.

"An ounce of prevention is worth a pound of cure."

Benjamin Franklin
Former U.S. President

"Even garbage can become intel —hackers look everywhere."

Kevin Mitnick
Former Hacker

Resources for SMEs

Small businesses don't need to tackle cybersecurity alone. A wide range of trusted organisations provide free guidance, toolkits, and practical support to help SMEs strengthen their defences and stay compliant. Here are some of the most useful resources to explore:

- National Cybersecurity Alliance – toolkits, posters, and the Champion sign-up.
- CISA – U.S. partner with practical how-tos for SMEs.
- UK NCSC – Cyber Aware – plain-English guidance for small businesses.
- ICO – data protection and GDPR compliance support.
- FSB Legal & Business Hub – dedicated advice for small businesses.

CSAM 2025 is more than a campaign; it's a call for small businesses to engage, learn, and strengthen their defences. By aligning with the theme "Stay Safe Online", adopting the Core 4, and making security awareness training a regular part of operations, SMEs can protect against cyber threats, reduce the risk of costly attacks, and contribute to a safer cyber world.

CYBER GROWTH ACTION PLAN

The UK's cybersecurity sector continues to experience strong growth, with jobs up 11%, revenue up 12%, and Gross Value Added (GVA) up 21% over the past year. GVA is a measure of the increase in the value of the economy due to the production of goods and services. In 2024, the cybersecurity sector employed an estimated 67,300 people across more than 2,100 companies, offering a wide range of products and services. The UK Cyber Growth Action Plan, an independent report published in September 2025 by Bristol University and Imperial College London, provides recommendations for the government to further strengthen the nation's cybersecurity sector. The plan aims to boost resilience and growth by stimulating demand, supporting businesses at all stages, making strategic choices about which technologies and sectors to prioritise, and simplifying government roles. It is intended to inform a refreshed National Cyber Strategy and enhance the UK's position as a global leader in cybersecurity. Zhero's amazing Izak Oosthuizen was a proud participant in the research and is recognised as a significant contributor to the report.

Report recommendations

The report sets out nine recommendations, organised around three main pillars: culture, leadership, and places. Measuring growth isn't always straightforward and things like revenue, GVA, jobs, and investment can all tell a story, but they don't always move in step. Some recommendations focus on growing the cybersecurity sector itself, while others aim to support the wider economy by emphasising incident prevention, resilience, and building cyber confidence. Each recommendation may have different effects on job creation and productivity at first. The report also includes practical suggestions for putting the recommendations into action and highlights areas where further research is needed. While it doesn't cover everything, it provides useful insights and options for next steps. Given how quickly this review was carried out, more detailed work will be needed in the future to target specific products or services, or to focus on particular locations.

A culture for growth

Growing cyber businesses depend on the connection between the vendors who create products and services and the CISOs and managers who use them. This supply-and-demand relationship is shaped by the UK's cyber culture and mindset, and strengthening it means supporting the growth journeys of cyber businesses, setting clearer expectations for how cyber risk is managed and reported, and engaging the public on the role cyber growth plays in the nation's safety and prosperity. Places also matter, as they help drive innovation and growth by attracting investors, shaping research and development, and fostering the relationships cyber businesses need to start and thrive.

Changing the culture

To support a culture for growth, three key recommendations stand out: first, government and industry should review the incentives and validation routes for cyber businesses to make it easier to navigate demand and create a culture that helps promising companies grow; second, regulations and guidance should stimulate informed demand by encouraging high-quality reporting of cyber risks, mandating Cyber Essentials where appropriate, and promoting cyber insurance and assurance, which helps organisations prioritise security, reduce incidents, and drive growth for UK cyber services; and third, cyber professionals should engage with civil society to highlight the sector's role in national resilience and prosperity, emphasising skills initiatives from schools to professional development to attract and retain talent and build wider support for the importance of cyber across the UK.

Cyber Essentials

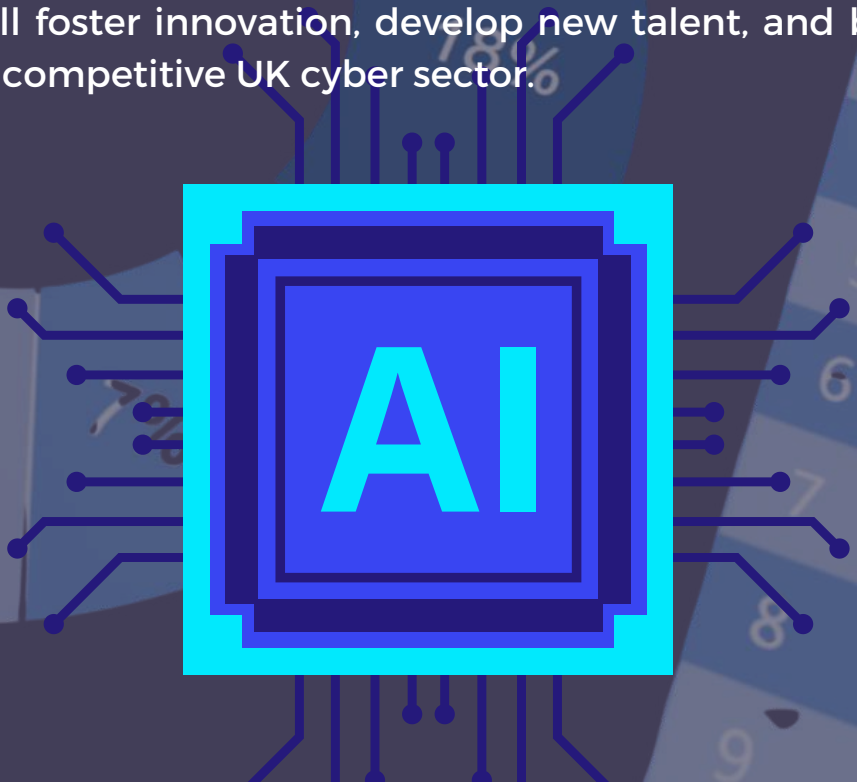
The Cyber Essentials (CE) scheme has been in operation for over a decade, with a steady increase in uptake and emerging evidence on its effectiveness. According to a NCSC report, 89% of CE-certified organisations would recommend the scheme, and 69% believe it made them more competitive. The uptake of the scheme has seen an upward trajectory over the past several years, with over 33,000 certificates awarded in the past year, representing a 20% increase from the previous year. However, this still represents a fraction of businesses, as the UK is home to 5.5 million private businesses. Currently, only 11% of organisations review cybersecurity risk in their supply chains.

The need for leadership

While the UK cyber community has many strong leaders, few focus on connecting supply and demand to drive sector growth. To address this, the report recommends creating and elevating cyber leadership roles in government and in regions with research, development, and commercial strength. First, a UK cyber growth leader should be appointed to provide expertise and coordinate action across the industry and within Whitehall, taking on responsibilities such as advancing exports, supporting national security objectives, and driving this growth plan forward to ensure cyber growth is integrated across policy areas. Second, place-based growth leaders should be appointed to convene and drive local cyber initiatives, using their industry experience to support the national leader while remaining independent from central and regional government, ensuring regions leverage their strengths to create, grow, and attract more cyber businesses. Third, the National Cyber Security Centre (NCSC) should have its role expanded and properly resourced to support growth initiatives alongside its core mission of cyber resilience, using its expertise to guide and validate cyber businesses, research, emerging technologies, and future developments without diverting focus from existing priorities.

The role of places

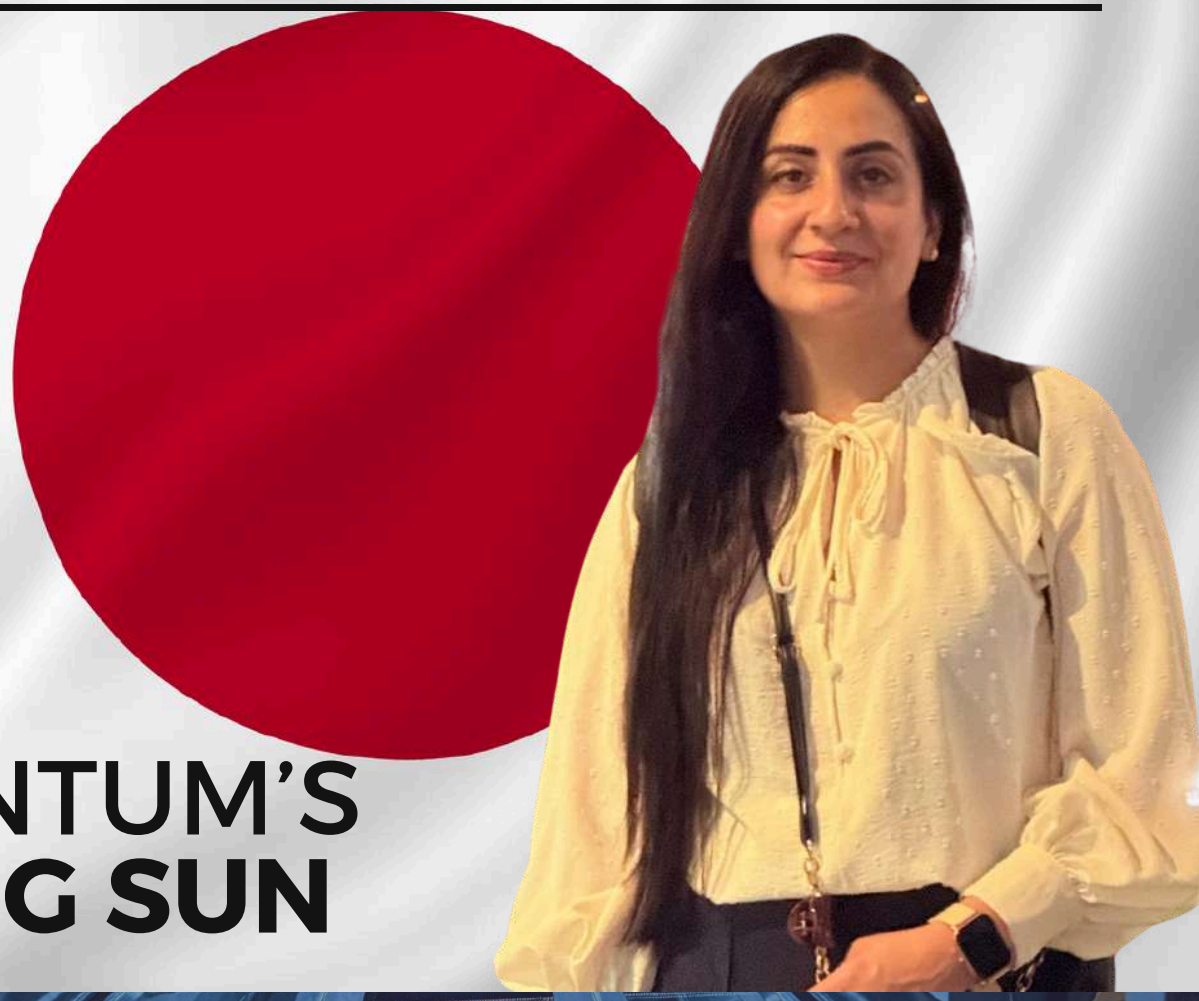
Places play a vital role in driving innovation and growth, attracting investors, shaping research and development, and fostering the relationships cyber businesses need to start and thrive. The UK's cyber sector now employs over 58,000 people across more than 1,800 firms, contributing over £10 billion a year to the economy—highlighting the value of strong regional ecosystems. To build on this success, the report recommends developing future-oriented communities, where place-based leaders bring together CISOs, academia, industry, government, and other stakeholders to share perspectives and tackle emerging cyber challenges. This collaborative approach encourages the co-creation of innovative projects and builds a forward-looking culture that strengthens local and national resilience. The report also suggests that places should nurture distinct technology areas, focusing on local cyber strengths aligned with the Industrial Strategy and the UK Government Resilience Action Plan. Priority areas include AI, cyber-physical systems, and fundamental cyber tooling, creating place-based specialisations that enhance the UK's overall cyber capability. Finally, places should provide secure environments and accessible infrastructure where multiple stakeholders—not only those with security clearances—can safely explore, test, and refine solutions. This approach will foster innovation, develop new talent, and build a more resilient and competitive UK cyber sector.



Izak's cyber MOT

A Cyber MOT is essentially a cyber "check-up" or assurance process for organisations of all sizes, ensuring that essential, real-time controls are in place to minimise cyber risk. It focuses on implementing fundamental cybersecurity practices properly — maintaining digital hygiene such as access controls, multi-factor authentication, password management, regular backups, and timely updates. The aim is to address the most common vulnerabilities that account for the majority of cyber incidents, potentially reducing risk by up to 95%. This concept reflects Izak's emphasis, in both You Don't Need a £1 Million Cyber Security Budget and his contributions to the UK Cyber Growth Action Plan, on practical and cost-effective cyber resilience rather than costly or over-engineered defences.

For many UK SMEs, the Cyber MOT provides a structured, affordable approach to cybersecurity. Smaller businesses are often exposed to risks such as data breaches, operational disruption, and reputational damage, yet lack the financial resources or expertise of larger firms. Oosthuizen's model encourages SMEs to take manageable steps that not only strengthen protection but also demonstrate reliability within supply chains. As supply chain partners and clients increasingly demand proof of good cyber hygiene, completing a Cyber MOT helps businesses build trust, meet compliance expectations, and avoid becoming the weakest link in interconnected networks....



QUANTUM'S RISING SUN

Tooba Qasim,a Ph.D student at City St. George's University of London, tells us about her amazing quantum adventure in her recent visit to the Land of the Rising Sun.

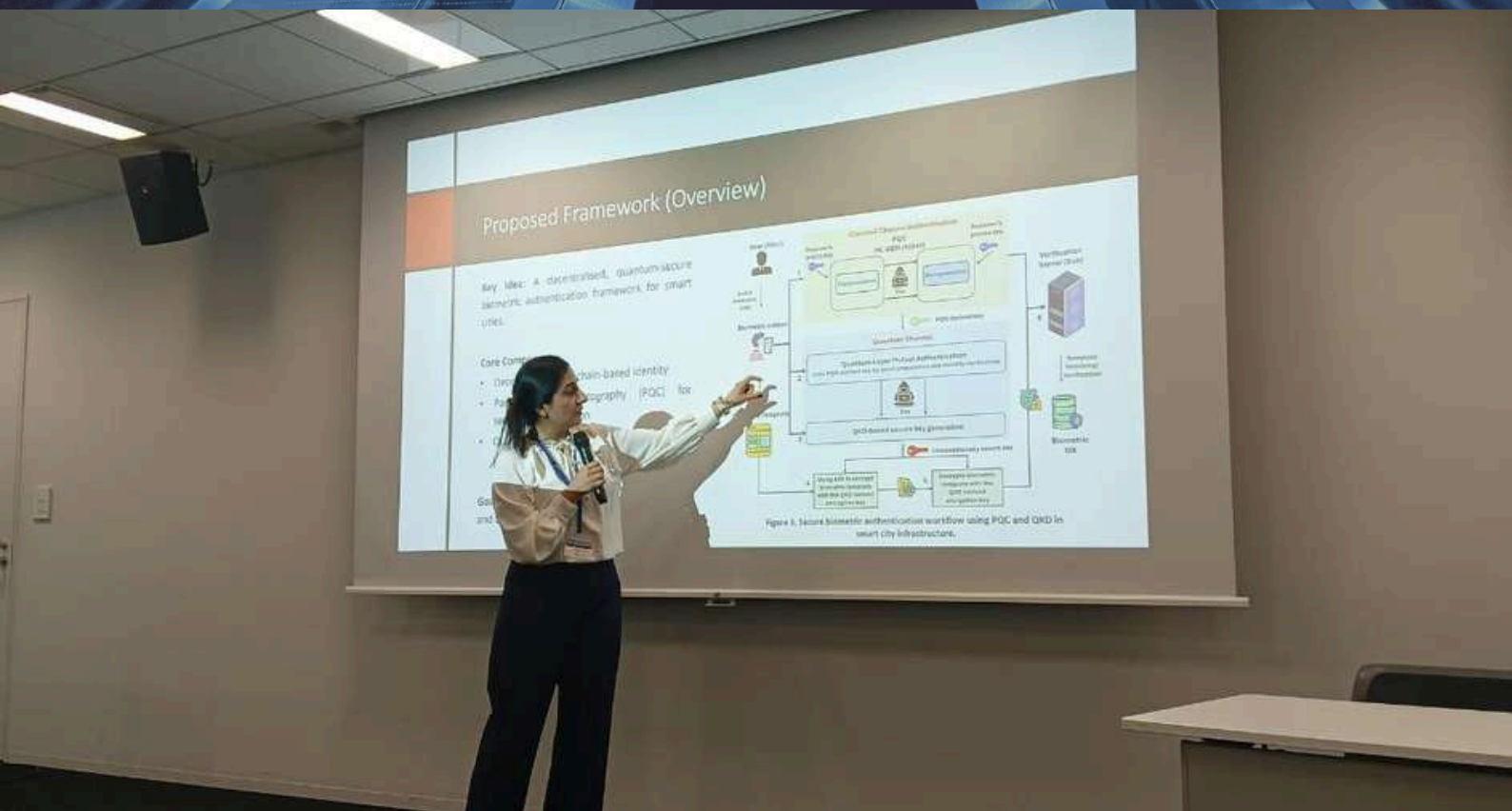
Anyone doing a PhD will tell you, it's not for the faint-hearted. There are endless months of hard work, long nights of writing, revising, rewriting, and then waiting... and waiting some more for that one email that says "your research paper has been accepted." It's a mix of exhaustion, excitement and relief all at once.

When my first paper was finally accepted for presentation at the IEEE International Joint Conference on Biometrics (IJCB 2025), it felt like a huge step forward, not just as a researcher but as a learner. After months of experiments, simulations, readings and endless drafts, that moment of acceptance was a quiet victory, a reminder that persistence really does pay off.

In September, I travelled to Osaka, Japan, to present my research on quantum-secure biometric authentication. Standing in front of an international audience of scientists and professionals, sharing my work and hearing their thoughts, was both exciting and eye-opening. My research focuses on how quantum cryptography can make digital identities more secure, protecting data in a world that's becoming increasingly connected.

But what made this experience truly special wasn't just presenting my work, it was the people I met and the conversations that followed. I connected with researchers from all over the world, each bringing unique ideas, challenges and insights. One of my favourite sessions was Women in Biometrics, where inspiring women shared their experiences of working in technology and research. Listening to their stories was deeply motivating, a reminder that progress in science is also about collaboration, inclusion, and shared growth.

Beyond the conference halls, I fell in love with Osaka, a city that perfectly blends tradition and technology. From peaceful temples to the buzz of neon-lit districts, every corner had a story. Exploring the culture, food, and warmth of the people made the trip even more memorable. It was the perfect balance between learning and reflection, a chance to see the world through a wider lens.



I am incredibly grateful to City University of London and Zhero IT Support for their support in making this journey possible. Zhero's mission of empowering businesses through secure and intelligent technology aligns beautifully with my own research on building safer digital systems for the future. Their encouragement and collaboration have been instrumental in helping me transform ideas into tangible research outcomes.

This publication marks just the first step in my PhD journey and I am looking forward to continuing the process, aiming for more meaningful and impactful research that contributes to the evolving world of cybersecurity and quantum technologies. I am excited to explore new partnerships and delve deeper into how emerging technologies can shape a more resilient digital future.

Looking back, my trip to Japan wasn't just about presenting a paper. It was about learning from others, sharing ideas, and growing as a researcher and individual. Every new experience adds something to who we are and this one reminded me that curiosity and collaboration will always be at the heart of discovery. The insights and connections I gained there continue to inspire my work and strengthen my commitment to advancing global cybersecurity.

METROPOLITAN POLICE

CYBER. LONDON

HIGH-ENERGY ESCAPE

Cyber London, City St George's, University of London, and the Metropolitan Police hosted a hands-on Cyber Escape Room on 22 September, offering an exciting and immersive experience. Teams engaged in real-world social engineering scenarios, learning to spot scams quickly, build cyber-smart habits, and respond to threats with confidence. Participants left with practical skills, sharper instincts, and a stronger "human firewall," making the event a powerful blend of energy, interaction, and learning.

zhero
crush the chaos

×

CYBER.
LONDON

AI & CYBERSECURITY

Professor Raj, Zhero's Head of R&D, and Izak Oosthuizen, both directors of Cyber London, hosted an outstanding AI and Cybersecurity event on 2 October. Alongside networking and a wholesome breakfast, Izak and Raj shared invaluable insights into the role of artificial intelligence in cybersecurity and addressed key questions on the current state of IT security for SMEs. Attendees also received a signed copy of Izak's latest Amazon bestseller, The AI Advantage: Thriving Within Civilisation's Next Big Disruption. The morning featured Raj introducing Cyber London's AI initiatives with a focus on the EU AI Act and its implications for SMEs in London, followed by Izak outlining best practices for achieving robust and affordable cybersecurity. Together, they explored AI's dual role in cybersecurity, as both a transformative tool and an emerging threat.

Windows 10 EOL

On 14 October 2025, Windows 10 Home and Pro reached end of support or end of life (EOL). End of Life (EOL) is when a software application is taken off the market or not renewed. The manufacturer may still provide some support, such as security patches and updates. End of Support (EOS) is the complete discontinuation of all support services for the software.

WHAT THIS MEANS

- No more free updates - After October 14, 2025, Windows 10 users will not receive any further free security updates, feature updates, or technical support from Microsoft.
- Security risks - Running Windows 10 without security updates will expose your device to potential security threats, malware, and vulnerabilities.
- Upgrade or replace - Microsoft advises users to either upgrade to Windows 11 (if their hardware is compatible) or replace their devices with new ones that support Windows 11.
- Extended Security Updates (ESU) - Microsoft offers an ESU program for Windows 10, which provides paid security updates for a limited time after the EOL date, but it's not a long-term solution and doesn't include new features.
- Windows 11 advantages - Windows 11 offers a modern and efficient experience with enhanced security features, designed to meet current demands.
- Free upgrade - Upgrading from Windows 10 to Windows 11 is free for eligible devices.
- PC Health Check - If you're unsure whether your PC is compatible with Windows 11, you can use the PC Health Check app to check its eligibility.

Windows 10 EOL

WHAT WILL HAPPEN

Your PC will continue to work, but all support for Windows 10 is discontinued.

WHAT YOU CAN DO

- You could ignore the EOL deadline completely. This is NOT recommended as your PC is no longer receiving updates and security patches from Microsoft. This means your PC is vulnerable to malware infections and other cyber threats. You will also experience performance and compatibility issues.
- You can pay Microsoft for security updates for Windows 10. With the Extended Security Updates package you can keep your current Windows 10 device fully protected for up to 3 years. According to Microsoft, the first year of protection will cost £50. This increases to £100 in the second year and £150 in the final year of cover.
- You can upgrade your existing PC to Windows 11 or buy a new laptop with this latest OS already installed.

WHAT WE WILL DO

Zhero recommends switching to Windows 11. We will assess whether your existing PC can be upgraded and is capable of running Windows 11 or if you will need a new workstation. While making the change to a new OS may seem daunting, we are here to support and assist you in every way we can.

Digital Defender Giveaway

Win £50 amazon voucher

- *I'm portable and removable*
- *I'm made up of three, and my first is in "you"*
- *My whole is in "husband"*

What am I?

Enter our monthly draw and stand a chance of winning a £50 Amazon voucher. The winner will be announced in the next edition of Inside Zhero.
Competition ends 17 November.
Good Luck!

Winner!

Congrats to Keith Carvalho, Parts Manager at Citygate, for winning last month's draw and a £50 Amazon voucher.

Citygate

Enter Now

Meet the team

Saad Arshad

ONSITE ENGINEER

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

Hi! I've always enjoyed problem-solving and working with technology, so the IT industry felt like the perfect fit for my interests and skills.

What's your most-used productivity tool?

My most-used productivity tool is Jupyter Notebook — it's great for writing and testing code, documenting my work, and visualising data all in one place.

How would you describe yourself?

I'd describe myself as a curious and motivated learner who enjoys solving problems, working with technology, and continuously improving my skills.

What do you enjoy the most about your role?

What I enjoy most about my role is the opportunity to learn new technologies and solve real-world problems through troubleshooting and collaboration.

Do you have any hidden talents or hobbies?

One of my hidden talents is playing padel — it's a fun way to stay active and competitive, and I really enjoy the fast-paced nature of the game.

What is your favourite movie or TV show?

My favourite TV show is Breaking Bad — I really enjoyed the intense storyline and how the characters evolved throughout the series.

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