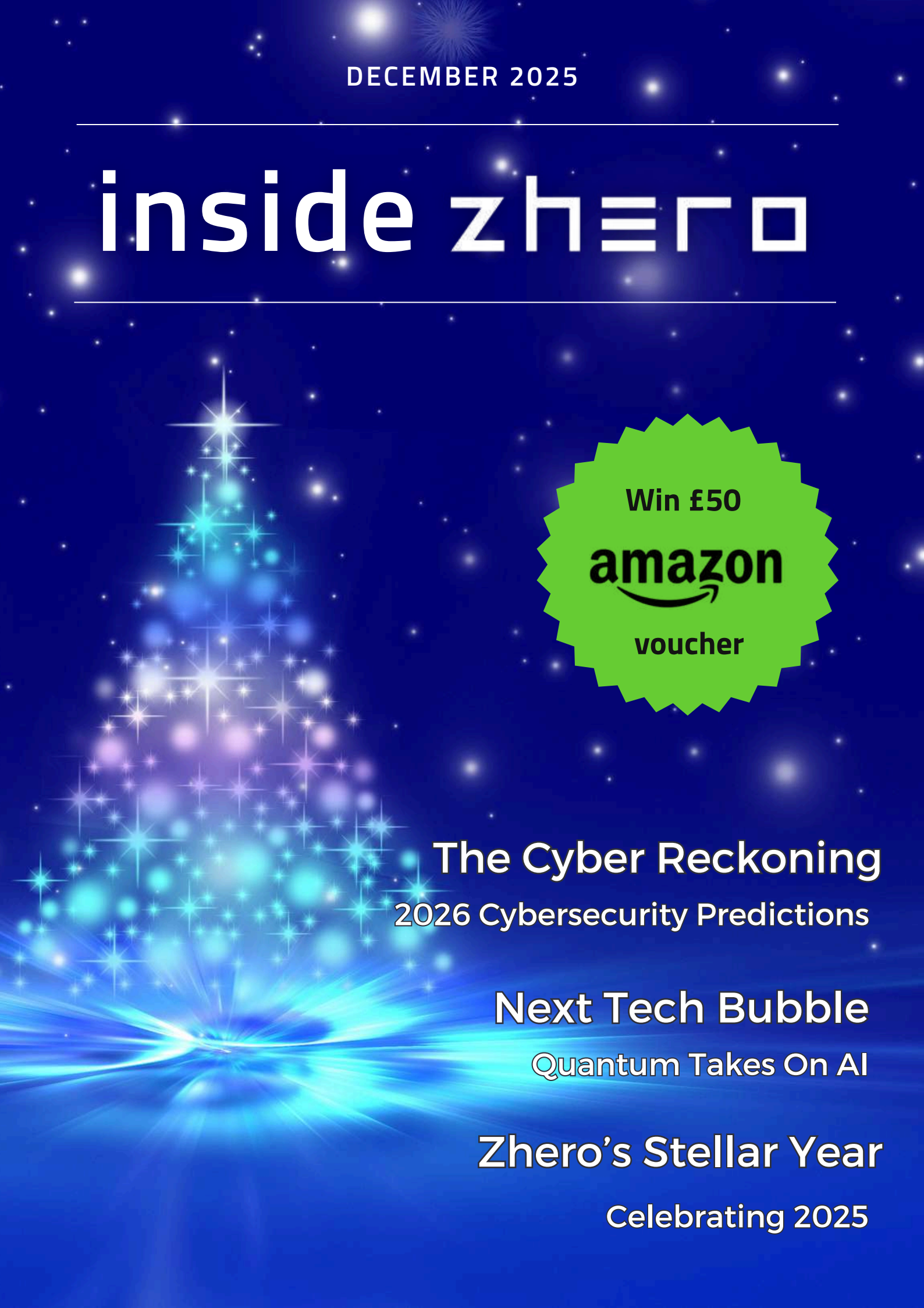
DECEMBER 2025

inside zhero



The Cyber Reckoning

2026 Cybersecurity Predictions

Next Tech Bubble

Quantum Takes On AI

Zhero's Stellar Year

Celebrating 2025

Message from Izak

Welcome to our December edition of Inside Zhero.

As the year draws to a close, we examine some of the cyber predictions for 2026 and consider the impact of quantum computing in the next decade. That said, I wish you all a Merry Christmas and a very Happy New Year. Exciting times ahead.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature “The Cyber Reckoning” looks at the impact of AI, RaaS, Zero Trust, social engineering and much more, on cybersecurity in the future.

78% of recipients open AI-generated phishing emails.

"I believe that the future of cyber leadership will be all about finding the right balance. For me, it means learning to trust AI and advanced technologies to help us make smarter, faster decisions, while never losing sight of the human judgment that keeps us grounded. Even as we embrace automation and machine intelligence, we need to maintain thoughtful oversight, ethical responsibility, and the ability to make nuanced calls that only humans can make. We'll need to constantly navigate the line between innovation and caution, leveraging AI as a powerful ally while remembering that true leadership always requires a human touch."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

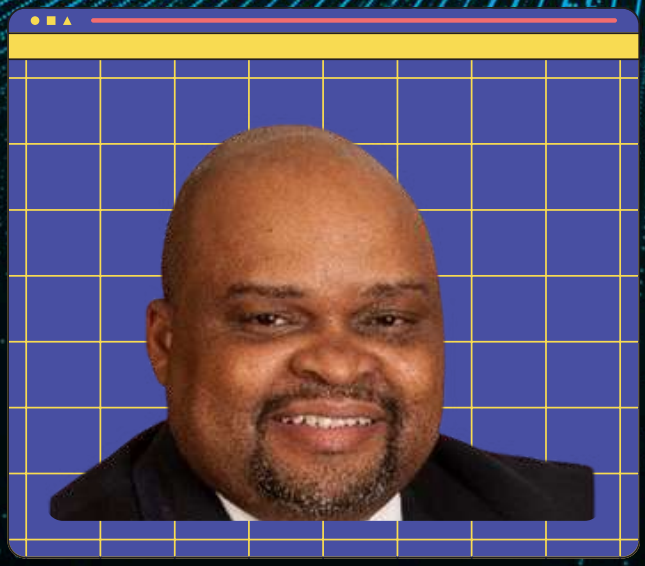
50% discount **cyberzhero542**

CYBER RECKONING

Cybersecurity in 2026 is set to be shaped by the dual use of AI, powering both adaptive cyberattacks and more intelligent defence, alongside the continued spread of Ransomware-as-a-Service and wider adoption of zero-trust strategies. Attack surfaces will keep expanding through vulnerable supply chains, multi-cloud complexity, and vast numbers of insecure IoT devices on 5G networks, while human error, responsible for roughly 90% of breaches, remains a critical weakness. By 2026, AI-driven social-engineering attacks are expected to grow by over 30%, increasing pressure on organisations already grappling with looming quantum-era encryption risks, tightening global regulations, and a persistent cybersecurity talent shortage. Organisations are also expected to invest more heavily in automated threat-response systems to keep pace with the speed of modern attacks. Increased board-level scrutiny will push cybersecurity spending higher as resilience becomes a core business priority. Additionally, the industry is likely to see faster adoption of privacy-enhancing technologies to help organisations balance security, compliance, and data-driven innovation.

Double-edged sword

AI and Machine Learning (ML) now play a dual role in cybersecurity, used both by defenders to spot and respond to threats, and by attackers to scale up sophisticated attacks. Around 67% of organisations now use AI-based tools in their cybersecurity operations, largely for advanced threat detection and automated response. Meanwhile, attackers are harnessing generative AI to produce highly convincing phishing emails at a fraction of the cost; some reports suggest phishing campaign costs drop by as much as 95% when using large language models. Deepfake techniques are also surging, with over 105,000 deepfake attacks reported in 2024 alone, with fraudsters impersonating people via voice or video in real-time. Alarmingly, AI-generated phishing emails can convert at very high rates. In some studies, 78% of recipients open them, and 21% click on malicious links. On the defence side, AI systems are helping organisations reduce detection time dramatically, with some tools improving threat detection accuracy by up to 60%. This evolving arms race illustrates how AI is transforming cybersecurity. It's as much of a shield as it is a weapon.



"The future of cyber leadership will be about striking the right balance — trusting AI while maintaining human oversight."

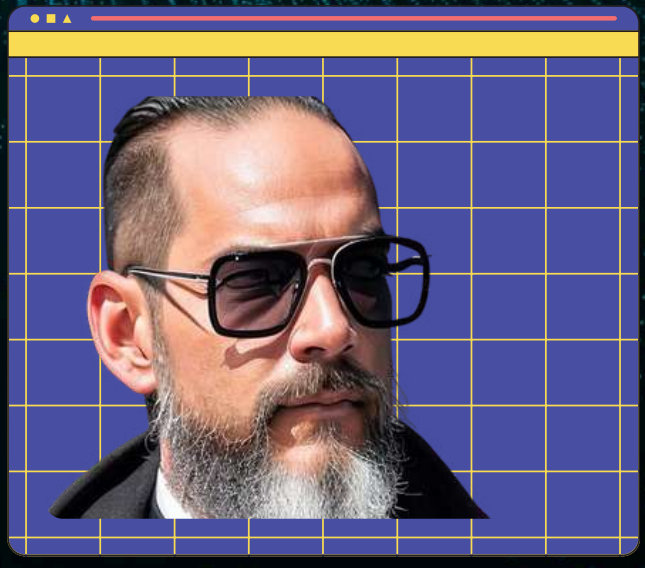
Timothy Youngblood,
University of Oklahoma

RaaS

Ransomware-as-a-Service (RaaS) has become a major force in cybercrime, making it far easier for criminals, even those without deep technical skills, to launch sophisticated attacks. According to the 2024 DigitalXRAID report, double-extortion tactics, where attackers both encrypt systems and steal data, were used in over 80% of ransomware incidents. These RaaS platforms operate much like legitimate businesses, complete with affiliate programmes, customer dashboards, and profit-sharing models, which dramatically lowers the barrier to entry for would-be attackers, as highlighted by TechForce UK. Two recent examples illustrate the impact of these attacks. The SafePay ransomware group attacked Ingram Micro in 2025, exfiltrating 3.5 terabytes of sensitive data and threatening to leak it, disrupting operations across parts of the company, according to TechRadar. Similarly, the Qilin gang, a well-known RaaS operator, carried out a cyberattack on Asahi Group Holdings in 2025, claiming to have stolen more than 9,300 files, approximately 27 gigabytes, and causing production outages, as reported by Reuters. The consequences of these attacks are severe. The average cost of a ransomware incident rose by 17% in the first half of 2025, largely driven by data theft and double-extortion tactics. This escalation demonstrates how damaging RaaS operations can be, both financially and operationally, reinforcing why they remain a top concern in cybersecurity.

"Ransomware has been industrialized."

Mick Baccio,
Splunk



Trust nobody

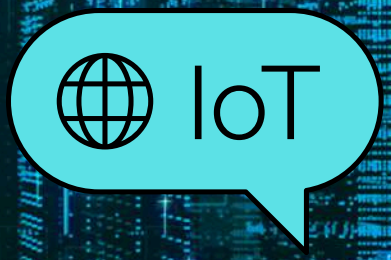
Zero Trust Architecture represents a major strategic shift in cybersecurity, embracing a “never trust, always verify” philosophy that assumes no user or device is inherently trustworthy. This model enforces strict access controls and continuous authentication, helping to contain breaches and prevent malicious actors from moving laterally across networks, as explained by leading tech analysts at Gartner. Recent industry data from Forrester shows that organisations which have adopted Zero Trust frameworks report up to a 50% reduction in their risk exposure, particularly when isolating sensitive resources. By enforcing micro-segmentation and least-privilege access policies, Zero Trust limits the “blast radius” of a breach and makes it far harder for attackers to escalate privileges across systems.

Outsider risk

Supply-chain and third-party cyber risk is now one of the most pressing concerns for organisations, as attackers increasingly exploit vulnerabilities in vendors and software suppliers. According to SecurityScorecard, 88% of cybersecurity leaders are worried about immature supply-chain security, and a report from BlueVoyant shows that 81% of organisations have experienced a supply-chain breach in the past year. These third-party incidents are not just common; they’re also costly: Gitnux data indicates that the average cost of a breach caused by a third-party vendor is around US$4.3 million. SecurityScorecard also found that 75% of third-party breaches target the software supply chain, enabling threat actors to scale their attacks efficiently. One very concrete example is the 2025 cyberattack on Jaguar Land Rover, which disrupted its entire manufacturing operations and reverberated through its supply chain — the knock-on effects are expected to cost the UK economy billions. The interconnected nature of modern business means that a weak link in one vendor can have systemic consequences, so managing and continuously monitoring these risks is now a top priority for security leaders.

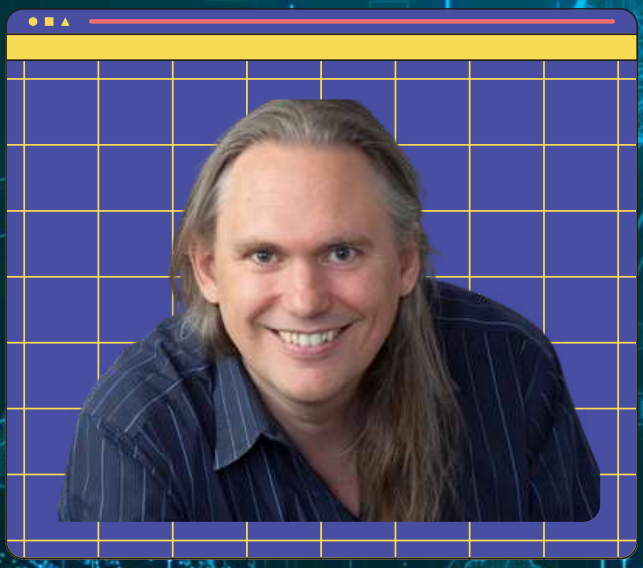
Cloud security

Cloud security is becoming increasingly challenging as organisations move into multi-cloud environments, where misconfigurations and weak access controls pose serious risks. According to recent data, around 60% of cloud security breaches stem from misconfigured storage, and half of breaches involve insufficient access controls. The Cloud Security Alliance also points out that identity issues are now the top risk, with excessive permissions, inconsistent access controls, and weak credential hygiene all driving incidents. Human error is a huge factor too; up to 88% of cloud data breaches are blamed on it. With the average cost of a cloud-related data breach rising to more than US$5 million, these vulnerabilities are both technically and financially significant.



39 billion

The rapid expansion of IoT devices alongside the rollout of 5G networks is dramatically increasing the overall attack surface for cyber threats. CompareCheapSSL reports that 61% of IoT devices have unpatched firmware vulnerabilities, and many still rely on weak or default passwords, making them easy targets for brute-force or credential-stuffing attacks. According to CWC Business, IoT devices often transmit data without proper encryption, exposing them to man-in-the-middle attacks. 5G introduces new risks via network slicing and edge computing, where a breach in one slice could potentially compromise others. Research aligned with NIST standards notes that limited processing power and memory in many IoT devices make it difficult to run strong security protocols, and Lancaster University highlights that poor lifecycle management means many devices never receive critical security updates, leaving them exposed for years. Looking ahead, analysts at IoT Analytics forecast that the number of connected IoT devices will grow to 39 billion by 2030, putting even greater strain on security teams to manage and segment these devices properly.



"The cloud doesn't eliminate risk—it changes who owns it."

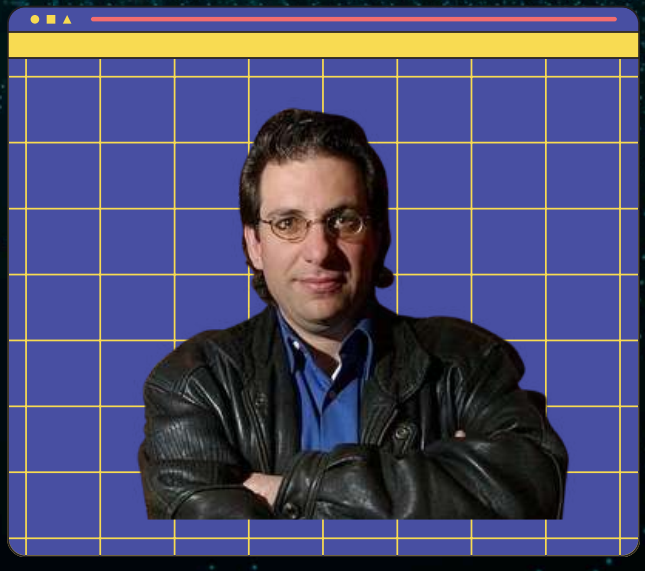
Mike Lloyd,
Red Seal

Weakest link

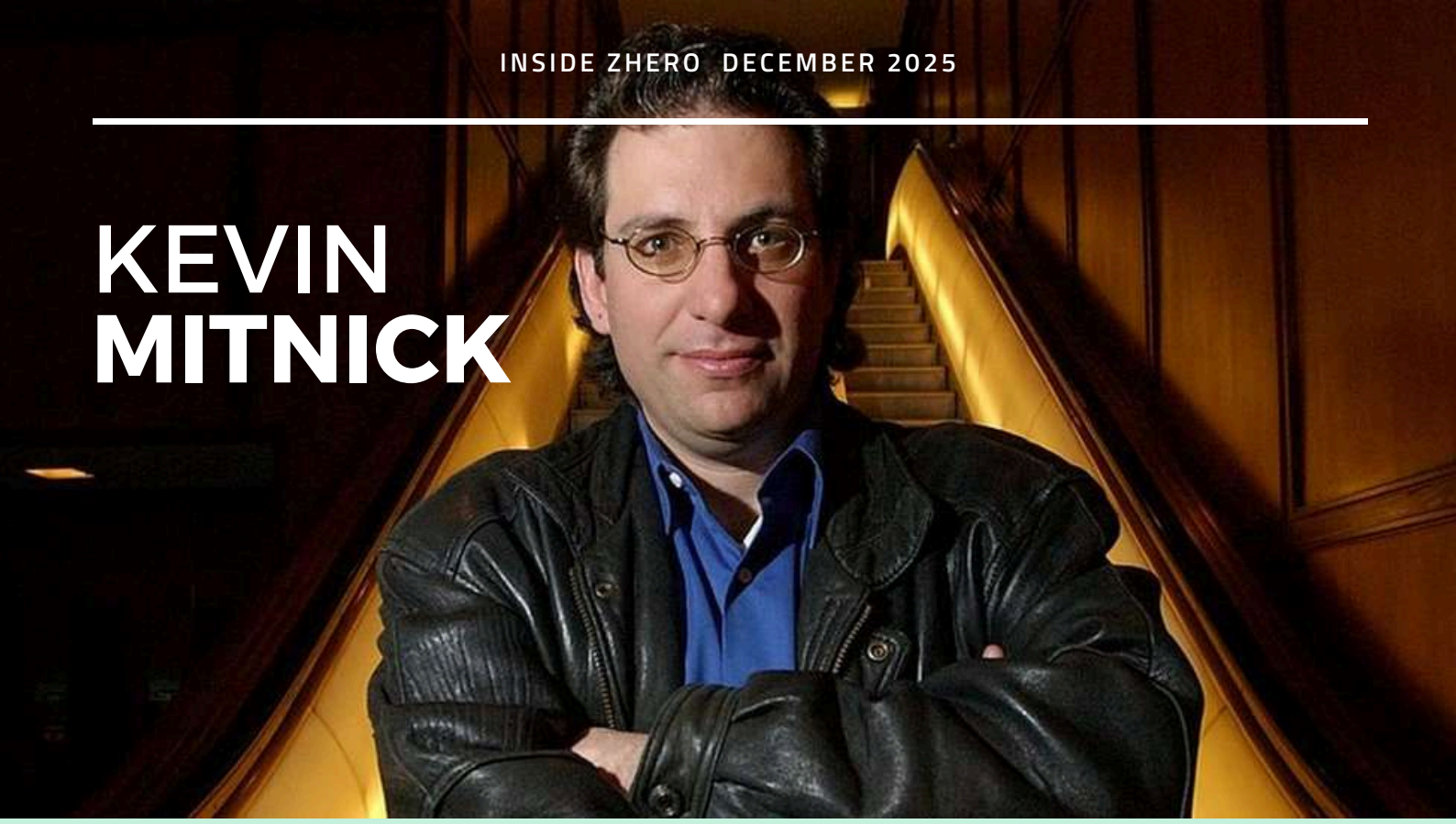
Human error continues to be a leading cause of cyber breaches. Phishing, spear-phishing, and vishing attacks are becoming increasingly convincing, with the help of AI, which allows attackers to craft highly personalised and believable messages. According to Verizon's 2024 Data Breach Investigations Report, around 82% of breaches involve human factors, while a recent report from IBM Security found that human error contributes to 95% of all security incidents, including misdelivery of sensitive information and accidental configuration mistakes. Organisations that fail to maintain continuous security awareness training see far higher rates of employee-driven incidents. Industry analysts predict that by 2026, AI-enhanced social engineering attacks could increase breaches caused by human error by more than 30%, as attackers exploit increasingly sophisticated techniques to manipulate employees. This underscores the urgent need for regular training, simulated phishing exercises, and cultivating a security-conscious culture.

"Companies spend millions of dollars on firewalls and it's money wasted because none of these measures address the weakest link in the security chain."

Kevin Mitnick



KEVIN MITNICK



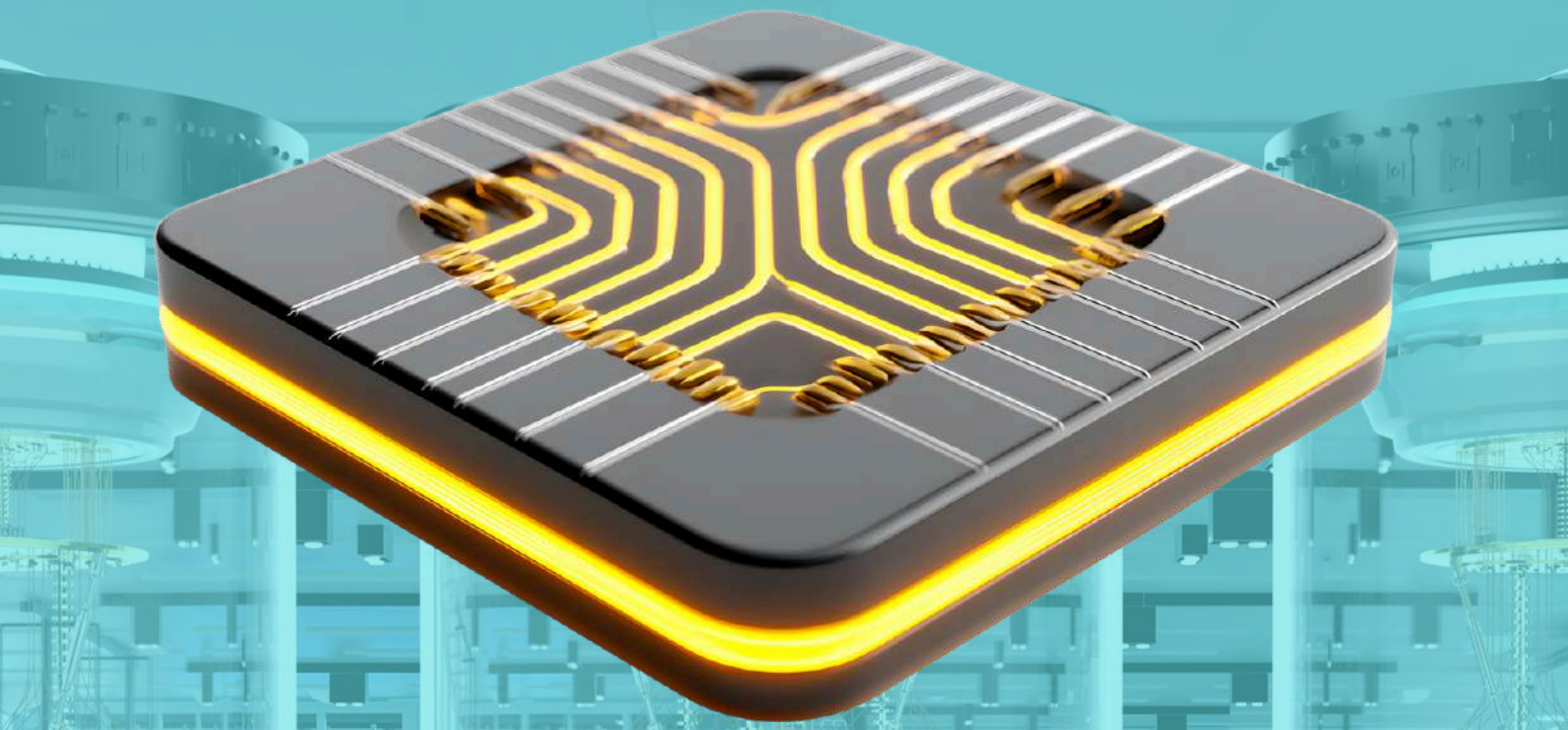
Kevin Mitnick (1963–2023) was essentially the rock star of hacking long before the field went mainstream. Growing up in Los Angeles, he displayed an early talent for clever mischief. At just 12, he figured out how to ride city buses for free by persuading drivers and digging unused transfer slips out of trash bins. That blend of curiosity, rule-bending, and social engineering set the tone for everything that followed. By his teenage years, Mitnick had progressed from manipulating transit systems to exploring telephone networks and early computer systems. He slipped into networks belonging to major companies such as Digital Equipment Corporation and Pacific Bell, not for financial gain but to test boundaries and understand complex systems. Using the alias “The Condor,” inspired by Three Days of the Condor, he became known as an elusive and highly skilled hacker who constantly stayed one step ahead of authorities. Throughout the late ’80s and early ’90s, Mitnick’s activities evolved into a dramatic pursuit involving the FBI, turning him into both a media sensation and a symbol of digital-age rebellion. After his arrest in 1995, he served five years in prison, including time in solitary confinement due to exaggerated fears about his abilities. Once released, Mitnick transformed himself into a respected cybersecurity consultant, author, and speaker. He founded Mitnick Security Consulting and became a leading expert on social engineering. When he passed away in 2023 from pancreatic cancer, he left behind a legacy that reshaped public understanding of hacking and cybersecurity.

Quantum computing

While quantum computing is not yet an immediate threat, it poses a growing risk to current encryption methods. ISACA reports that 62% of technology and cybersecurity professionals are concerned that quantum computers could eventually break today's internet encryption, yet only 5% cent of organisations currently have a defined quantum-computing strategy. Capgemini research adds that nearly two-thirds of organisations view quantum as the most critical cybersecurity risk within the next three to five years, particularly due to "harvest-now, decrypt-later" attacks, where sensitive data is collected now to be decrypted once quantum capabilities become available. Digicert highlights that about 60% of firms are already evaluating quantum-resistant encryption, though only 5% have implemented quantum-safe encryption so far. ISACA further notes that just 4% of organisations have a fully defined quantum-computing roadmap. As a result, many organisations are beginning to explore post-quantum cryptography and build "crypto-agile" strategies, but full adoption of quantum-resistant standards remains a complex technical and operational challenge.

Regulatory compliance

Regulatory compliance is becoming a major challenge as governments tighten data protection and breach-reporting laws. In the EU, the GDPR still sets the tone: organisations must report certain breaches within 72 hours and can face fines of up to €20 million or 4% of global turnover (or £17.5 million under UK GDPR). In the US, the Securities and Exchange Commission now requires publicly listed companies to disclose material cybersecurity incidents within four business days. New rules such as the EU's NIS2 Directive and Cyber Resilience Act further push companies to conduct regular risk assessments, report incidents, and strengthen resilience. With regulations multiplying and diverging, organisations must invest heavily in compliance, auditing, and cross-border cyber-risk strategies.



NEXT TECH BUBBLE

There's a long-standing joke among tech journalists: you can either explain quantum mechanics in a way that's completely accurate or in a way people actually understand—but never both. The field is notoriously strange, filled with particles that can exist in multiple states simultaneously and behave in ways that defy everyday intuition. Yet it's precisely these bizarre behaviours that open the door to entirely new forms of computational power. As Brian Hopkins of Forrester remarked, "I used to believe that quantum computing was the most-hyped technology until the AI craze emerged," a reminder that even amid today's shifting tech hype cycles, quantum's promise remains substantial. The market supports that: one estimate puts the global quantum computing market size at about USD 1.44 billion in 2025, with a projected rise to USD 16.44 billion by 2034 and another forecast seeing the global market reaching USD 27.6 billion by 2035 with significant annual growth. With such figures and a potential market size of up to USD 97 billion by 2035 cited by McKinsey, it's clear that quantum computing is far more than a theoretical curiosity.

Hardware heroes software sidekicks

While artificial intelligence dominates headlines, quantum quietly builds its empire through hardware such as sensors, computers, and communication systems. McKinsey's research highlights that quantum computing alone could rise from around three billion pounds today to more than USD 70 billion by 2035, making it a major economic and technological force. Unlike AI, which primarily relies on software but still needs hardware to run, quantum's value lies in manipulating the physical world at an atomic and subatomic level, opening up possibilities for industries ranging from pharmaceuticals to finance.

Hype, fear and errors

Despite the excitement, quantum remains a risky investment. Analysts recently warned that some key quantum-related stocks could fall by as much as 62%, echoing similar concerns about a potential AI bubble. Quantum computers are also plagued by their own type of errors: qubits are extremely fragile, and even the slightest disturbance from temperature changes, light, or electromagnetic noise can disrupt calculations. This fragility underscores how challenging it is to harness the full power of quantum machines in a practical, reliable way.

Not your traditional computer

Quantum computers bear little resemblance to the PCs or laptops we use every day. They are large, lab-based devices often kept at temperatures close to absolute zero, and some experimental designs even resemble jellyfish or other organic forms. Elon Musk has jokingly suggested that quantum computers might work best in the permanently shadowed craters of the moon, highlighting just how sensitive these machines are to their environment. Researchers are also experimenting with synthetic diamonds to make qubits more stable, a technique pioneered by De Beers' Element Six in collaboration with Amazon Web Services.

Small machines mind-bending potential

"The area of quantum computing is, in my mind, when you look at the applications, as big, if not bigger than AI chain."

Rajeeb Hazra, Quantinuum

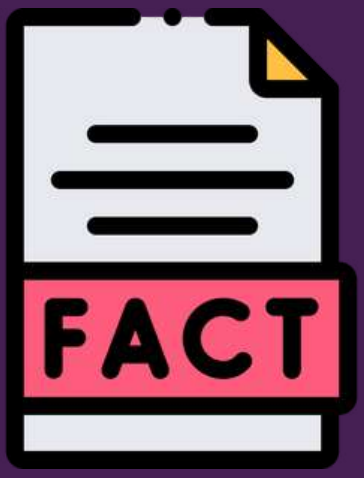
While There are only around 200 quantum computers globally, but their potential is enormous. Professor Sir Peter Knight, one of the UK's leading quantum scientists, told Dr Jim Al-Khalili on BBC Radio 4's The Life Scientific that quantum machines could perform calculations "that could take the age of the universe on a supercomputer in seconds." Google has unveiled a new quantum chip called Willow, which it claimed could take five minutes to solve a problem that would currently take the world's fastest supercomputers 10 septillion years, or 10,000,000,000,000,000,000,000,000, to complete. Applications include drug discovery, where machines could test trillions of molecular combinations, and personalised medicine, which could deliver tailored treatments based on an individual's unique biology.

Quantum sensors and navigation

Quantum technology is already producing practical innovations beyond computing. Nottingham University researchers developed helmet-sized quantum sensors capable of non-intrusive brain scans in children, overcoming limitations of conventional MRI machines. Imperial College London trialled a "quantum compass" on the London Underground to accurately navigate underground, where GPS fails. Dr Michael Cuthbert of the UK's National Quantum Computing Centre explained that precise timing and positioning are essential not only for navigation but also for financial transactions, making quantum sensors highly valuable.

Harvest now decrypt later

Quantum technology doesn't just promise progress; it poses threats. Professor Alan Woodward of Surrey University warns that once quantum computers reach sufficient power, they could break today's encryption through "harvest now, decrypt later" attacks. Nations are reportedly already collecting encrypted data in preparation for future decryption. Experts argue that quantum-resistant encryption must be implemented immediately, as the theoretical ability to break current public-key encryption exists even if fully operational quantum machines are not yet widespread.



- 🌐 Quantum computing market expected to reach 2.2 billion USD by 2026
- 💰 Venture capital investment in quantum startups hit 1.7 billion USD in 2021
- 🌍 China, the US, and Japan lead in quantum computing research and patents
- 💻 IBM's Eagle processor has 127 qubits, aiming for 1,121

Prepare for Q-day

When will Q-day, the arrival of quantum computers powerful enough to break real-world encryption, occur? Estimates vary, but Forrester analyst Brian Hopkins predicts around 2030. McKinsey's 2025 Quantum Technology Monitor forecasts that by then, there could be between 2,000 and 5,000 quantum machines worldwide. Some companies, including Apple and Signal, have already begun rolling out post-quantum encryption keys, although existing data encrypted under traditional systems remains vulnerable. Daniel Shiu, former head of cryptographic design at GCHQ, told the Sunday Times that it is credible that almost all UK citizens will have had their data compromised by state-sponsored attacks, stockpiled for decryption once quantum machines are operational.

QUANTUM SECURITY THINK TANK

CYBER LONDON

Cyber London's Quantum Security Think Tank provides a global platform for academics, policymakers, industry leaders, and not-for-profit organisations to shape a responsible future for quantum security technologies. It aims to catalyse international collaboration, advance ethical standards, and ensure quantum technologies deliver secure and inclusive societal and economic benefits. The Think Tank guides organisations through the Quantum Safe Readiness Logic Train, a five-stage framework for adopting quantum security standards, encompassing awareness of quantum threats, understanding the impacts on cryptography, preparation and planning, implementation of post-quantum solutions, and continuous improvement. This practical pathway helps organisations manage risks, plan transitions, and align with best practices.

The Think Tank offers a range of resources, including blog and insight articles, brief reports, case spotlights, advisory board commentary, and a curated resource library. Topics cover the quantum threat to cybersecurity, post-quantum cryptography, workforce skills, international approaches, and real-world adoption examples. Webinars, workshops, SME roundtables, and collaborative events further support engagement across the global ecosystem. By providing thought leadership, regulatory guidance, and actionable insights, the Quantum Security Think Tank empowers stakeholders to prepare for the quantum security transformation, mitigate emerging risks, and ensure long-term value from quantum innovation. It is designed as a collaborative, evolving marketplace that brings together expertise, innovation, and practical guidance to secure the quantum future. The Think Tank was launched on 9 December this year.

Here's the Think Tank: Cyber London Quantum Security

zhero

A Journey into Cybersecurity

This month we hear from our amazing Service Desk Engineer, Marc van Romburg, who tells us what led him into the world of technology, cybersecurity and IT support.

From a young age, I fell in love with games, and that passion naturally led me into the tech space. I still remember my dad salvaging old, end-of-life computers — machines running Windows 98 in 2004 — and giving them a second life. Together, my dad and I built my first real gaming device with what, at the time, felt like incredible specs, including a Pentium 4 processor, 1 GB RAM, a Voodoo Graphics card and a 20 GB IDE hard drive.

From that moment on, throughout my school career, I was always at my happiest in Computer Science class. I loved learning how programs worked, understanding systems, and figuring out how to make things run better and faster. Technology quickly became more than a hobby — it became something I wanted to build a future in.

In 2022, I discovered Zhero and joined as an intern. I immediately knew it was a place where I could grow, establish myself, and find my purpose in serving people through technology. Fast forward nearly four years, and I can truly say the experience has been phenomenal. I've had the privilege of working with some of the best in the industry — people who are breaking barriers and delivering affordable, world-class IT solutions, as our CEO would say "We have the Secret Sauce!". My journey from salvaged PCs to professional IT has shaped not only my career, but the person I am to.

zhero
crush the chaos

London

On 14 November, Izak, Natasha and Zaheer joined other Zhero staff members and our invaluable clients to celebrate a remarkable year at Drake & Morgan The Otherist in London. An incredible time of fun, feast and networking by all, and we're already raising a toast for our celebrations next year.

zhero
crush the chaos

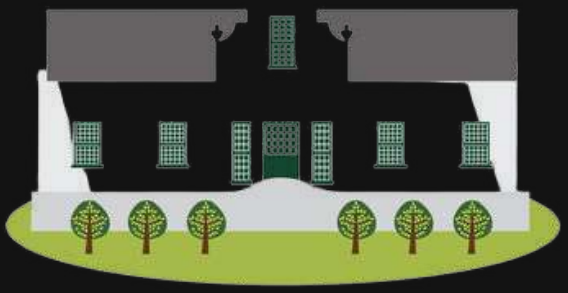
Edinburgh

On 7 November, Zhero headed up to meet with our valued parters, N-able, in Edinburgh. The team meet with Sylvia Roger, our account manager, Jamie Barnes (EMEA director), Ewan Cameron, Chris Dunsmore , Ingrid Nylander, Garry Chaplin, Sally-Anne Jones and Barry Seston. Before an amazing lunch, our star developer, Louis, showcased some of the software we have built and also development work in progress.

zhero
crush the chaos

Franschhoek

Team Zhero and Simon Poole, COO of Citygate Automotive, with some colleagues, had an exceptional time celebrating a stellar and successful 2025 at Haute Cabrière in Franschhoek. A well-deserved day of relaxation and recreation, and good food and wine was shared by all.



zhero
crush the chaos

Annual Awards

Congratulations to the winners of our 2025 annual staff awards, presented by our very own Natasha Botha at Haute Cabrière in Franschhoek.

- Ryan Leech for Living Zhero's Core Values
- Kian Botha Kian Botha for Living Zhero's Purpose
- Louis Oosthuizen for Living Zhero's Vision
- Ryan Leech for Living up to Zhero's Brand Promises
- Macwhill Hanse for Reliability
- Yola Nkepu for Leadership
- Louise Niemand (De Bruin) for Teaching and Coaching
- Ryan Leech for Role Acceleration
- Ryan Leech for Determination
- The Twané Trophy 🏆 went to Ryan Leech for continually going 'Above and Beyond'

zhero
crush the chaos

Our Achievements & Goals

“I was proud to be recognised as a research participant in the UK government’s Cyber Growth Action Plan. We hosted Cyber London – Zhero breakfast events, grew our LinkedIn following to 5K+, and I co-authored an Amazon bestseller on AI. In 2026, we plan monthly breakfast events targeting business leaders, focus marketing on measurable outcomes, and further grow our LinkedIn presence.”

"In 2025, we completed monthly executive reporting, resolved all Zhero Wait items, began importing Ingram invoicing, and finished our annual financial statements early. In 2026, we plan to streamline supplier contracts, complete asset comparisons across Zhero Wait, N-able, and Xero, and improve invoicing processes."

"This year, we implemented XDR, deployed PRTG, cleaned up the data centre, and introduced the Synology 365 backup solution. In 2026, we foresee cleaning Zhero Wait and N-able, developing a knowledge base for assets, services, and third-party vendors, and pursuing certification partnerships."

“In 2025, we attended and presented at the N-able Berlin Empower event, implemented workstation automation, resolved sync issues between N-able and Zhero Wait, partnered with Automatik to automate N-able patch management, and updated the alerts dashboard. Next year, we’ll launch the Projects Portal, draft quotations and assets, achieve full sync between Zhero Wait and N-able, and onboard more clients to Operations Insight and Risk.”

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 store your memories but have no brain*
- *I can crash in an instant yet feel no pain*
- *I'm built from circuits, both silent and plain*
- *Your digital past runs through my domain*

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 9 January.
Good Luck!

Winner!

Congrats to Kathy Meyer, Appointment Setter at Zhero, for winning last month's draw and a £50 Amazon voucher.

Enter Now

Meet the team

Guy Kuipers

SENIOR DIGITAL TRANSFORMATION CONSULTANT

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

Hi! I fell into it as a budding young sales person and have been on the fringes ever since whether working for a MSP or developing software solutions.

What's your most-used productivity tool?

ChatGPT is great. I look forward to MS Co-Pilot catching up, as this will be key for businesses to protect their IP.

How would you describe yourself?

I'd describe myself as being enthusiastic and interested.

What do you enjoy the most about your role?

What I enjoy most about my role is engaging and helping different businesses and people solve real problems.

Do you have any hidden talents or hobbies?

Hockey - I really enjoy team sports and the after party.

What is your favourite movie or TV show?

My favourite movie is The Shawshank Redemption - it takes you through every emotion.

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