JANUARY 2025

inside zhero

Tech Out the Future

Tech Transformation in 2025

The Top 5

Reflections on Cybercrime

Cybersecurity in 2025

Cyber Insights from Zaheer

Message from Izak

Hello everyone! Wishing each and every one of you a bright and prosperous New Year ahead.

To kick off this issue of Inside Zhero, we'll look at some of the trending technologies of 2025. Our Technical Lead, Zaheer, also gives us his views and predictions on IT support and cybersecurity in the future.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Tech Out the Future" focuses on some of the main technologies, including AI, that will shape the way we work, live and play.

£200 million in investment is funnelled into the country's AI sector every day.

"Today's technologies aren't the destination but the tools we use to move forward. As we look ahead, we need to focus on building a future driven by abundance, where resources are plentiful, abstraction simplifies complexity, and autonomy empowers systems, individuals and security. It's up to us to prepare and strategise for an evolving technological landscape."

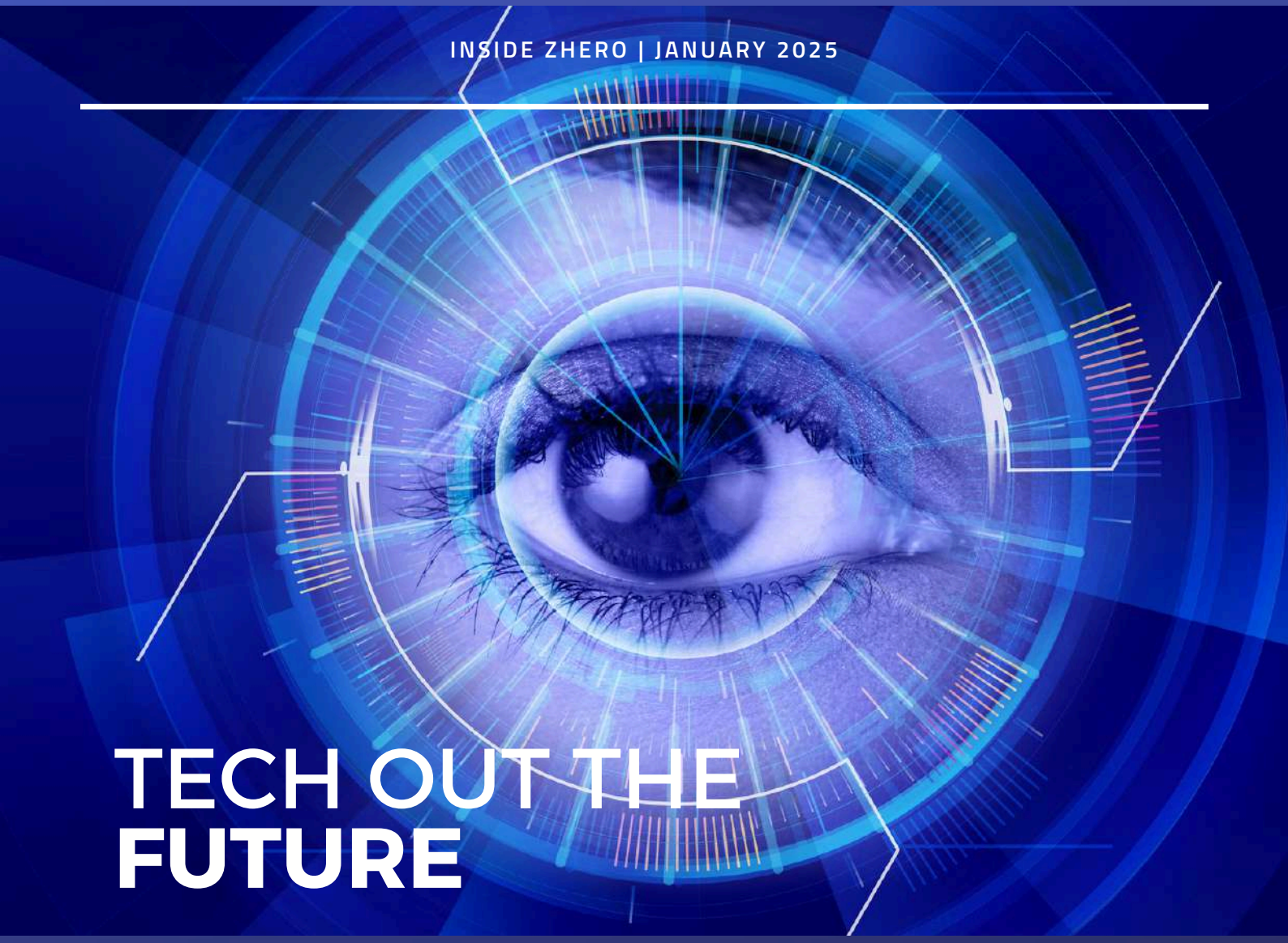
Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consulation

30% discount **cyberzhero542**

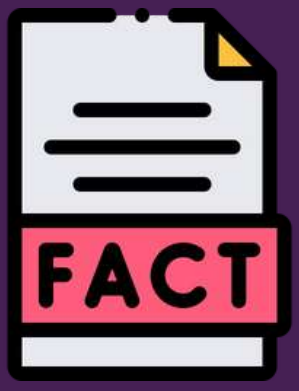


TECH OUT THE FUTURE

2025 promises to be a whirlwind of transformation, brimming with groundbreaking developments poised to reshape our world. With advancements in AI, robotics, biotechnology, and space exploration, we're stepping into a future of constant evolution. Global AI spending is projected to hit $154 billion in 2025, up from $87 billion in 2022, while the robotics market is expected to grow at an annual rate of 10.5%, reaching a staggering $90 billion by 2030. These innovations will open the doors to incredible opportunities such as life-saving medical breakthroughs, smarter automation, and deeper space exploration. They'll also present challenges that demand our attention. As we navigate 2025, it's not just about celebrating progress; it's about ensuring these breakthroughs stay aligned with ethical principles and are used responsibly. With so much at stake and so much potential to unlock, the journey ahead should be thrilling, not daunting.

Meaningful AI

The days of innovation just for the sake of it are behind us. Industries are now zeroing in on AI applications that deliver real value and measurable benefits. Over the past few years, companies have been experimenting with AI to figure out what it can and can't do, as well as its risks and use cases. Now that they've got a better handle on it, the mystery is fading, and AI is becoming more about practical, well-thought-out uses. For example, telecom companies are already seeing noticeable boosts to their profit margins thanks to AI, and they'll keep using it to cut costs. In healthcare, AI is helping improve patient care and outcomes, while retailers are using it to make personalized recommendations and power cool tech like digital mannequins. But as AI becomes more common, so will regulation. Governments and regulators are catching up, and businesses will need to stay on top of the rules as they change quickly over the next year. The EU AI Act and other upcoming regulations will be key in shaping how AI is developed and used moving forward. It's a big moment for AI, and staying informed will be crucial.



AI for customers

- 80% of executives agree that chatbots that all sound the same are creating differentiation challenges.
- 77% agree their organisations will need to proactively build trust between personified AI and their customers.
- 95% report maintaining a consistent personality will be vital to customer-facing AI agents over the next 3 years.

Your face in the future

As businesses bring generative AI into customer interactions, one key question emerges: What's your AI's personality? Generic agents risk creating bland experiences that dilute a brand's identity, but personified AI offers a solution, adding personality and unlocking deeper customer relationships. The challenge is standing out in an increasingly autonomous landscape, where third-party chat platforms dominate. This isn't about rejecting AI - it's about using personified AI to combine the scale of technology with the human touch of a brand. Imagine a future where every interaction feels personal, guided by an AI chatbot that embodies a familiar mascot or influencer. These agents operate across platforms, learning about customers over time, building trust, and taking actions tailored to individual needs. Far from superficial personalization, they manage thousands of conversations while fostering real relationships. The tools are here - AI agents, data frameworks, and advancements in personified AI - but businesses must connect them intentionally. Done poorly, brands risk losing their unique voice. Done right, this marks the beginning of a new era in customer relationships.

Big brand AI

- Amazon uses artificial intelligence to analyze images and videos to improve product listings and recommendations.
- **Netflix uses AI to determine** what shows and movies to show you when you log into your account.
- Tesla's AI system gathers visual data in real-time from eight cameras on the car to produce a 3D image that identifies the road and any obstacles and makes decisions .

Ameca

Ameca is a humanoid robot that uses AI to interact with people. It's designed to look and act like a human and is considered one of the most advanced humanoid robots in the world. Ameca is a place to test AI and machine learning systems. It's designed to help researchers understand how humans and robots can interact in the future. Ameca can be rented out for events and school visits to help people understand robots better. The robot was created by Engineering Arts in Cornwall. The company's founder, Will Jackson, was inspired by his time at London's Science Museum in the 1990s. Amazon Prime Video, National Geographic and Now TV are some of Engineering Arts' clients.

Robotics transformation

Robotics is becoming more common across various industries. Once seen as novelty items, socionic and anthropomorphic robots like Ameca and Digit are now playing essential roles in eldercare, warehousing, and retail. Multitasking robots are quickly becoming the backbone of healthcare and logistics, making everyday tasks more efficient. In households, affordable robotic appliances are replacing traditional devices, offering better convenience, safety, and ease of use. By 2025, there will be growing confusion around what truly involves human effort, sparking deep discussions about work, identity, and the meaning of life.

Fighting back with AI

Cyber threat actors aren't the only ones using AI and this year companies will increasingly turn to AI to beef up their cybersecurity. AI can power predictive defences, allowing cybersecurity teams to sift through massive amounts of data—both historical and attack patterns—to spot threats before they even happen. Even if a business responds effectively to a data breach, it can still suffer serious damage to stock prices, operations, and reputation. Being able to detect and stop attacks before they occur will be a huge advantage, giving companies a clear edge in a competitive landscape. Organisations that move quickly to integrate predictive AI defences and openly share their efforts will enjoy stronger protection and greater trust compared to those who lag behind. Companies that delay could become prime targets as others tighten their security. Over the next few years, AI will become a critical tool in every company's cybersecurity strategy. Threat actors will continue using AI, so it's something businesses of all sizes must adopt to stay ahead.

5G kicks a**

In 2025, internet connectivity is about to get a major shake-up, and traditional broadband providers are going to feel the heat. Fixed wireless access is gaining ground fast, thanks to 5G, which can now replace home broadband with speed and reliability—no cables or expensive infrastructure needed, just lower prices! The UK's 5G services market is expected to soar, growing at a crazy 52.4% compound annual rate from 2024 to 2030. As more people jump on these new, easy-to-use options, broadband companies are going to have to either step up their game or get left in the dust. It's either be innovative or risk getting outpaced so those lagging behind better bring on their A-game!

Giant step for humankind

By 2025, humanity will be deep into experiments in space exploration, taking small but significant steps toward commercializing outer space. Private ventures and government initiatives will begin establishing permanent habitats on the moon—early signs of a sustainable economic presence beyond Earth. Asteroid mining will go from concept to reality, with companies like AstroForge planning to send compact refineries into space to extract minerals and return only precious metals to Earth. Advances in technology will make space tourism more accessible, allowing the ultra-wealthy to experience space travel firsthand. A big part of this progress is driven by rocket reusability advancements from companies like SpaceX and Blue Origin, combined with nations' growing interest in securing space assets for both economic and security reasons. These developments are on track to create trillion-dollar industries. However, with all this activity, there's a clear need for new governance frameworks and conflict resolution in space. By 2025, humanity will face critical decisions as we shift from simply dreaming of space to planning a future where we become a multi-planetary species, no longer confined to life on Earth.

Transformative healthcare

Healthcare companies are already offering a range of telehealth services, but in 2025, these will expand beyond simple patient-doctor interactions to include smart wearable devices that provide real-time medical data. Providers will be able to remotely track at-home medical equipment, like IVs, oxygen machines, glucose monitors, and heart rate monitors, giving them a clearer picture of a patient's condition from afar. Thanks to advancements like improved 5G connectivity, more patients—especially the elderly or critically ill—will be able to receive care from the comfort of their own homes. This will also help providers reach areas that were previously out of reach, reducing the need for in-office visits. Technologies like computer vision could even step in to monitor emergencies, like if a patient falls at home and is unable to call for help. However, healthcare providers will need to be careful about the data they collect and ensure they prioritize strong data security. Keeping medical information safe while staying compliant with regulations will become even more crucial as these technologies grow.

REFLECTIONS ON **CYBERCRIME**

The ransomware epidemic continued its relentless march in 2024, leaving a trail of devastation, including high-profile victims like the UK's NHS, which endured particularly severe attacks. State-backed cyber intrusions from nations such as China and Russia also persisted, fuelled by global geopolitical tensions and exposing numerous long-running cyber espionage campaigns. However, 2024 demonstrated that shedding light on the cyber underworld is making a difference, with the British leading the charge through new attributions from the National Cyber Security Centre (NCSC), takedowns spearheaded by the National Crime Agency (NCA), and proposed legislation targeting ransomware threats to critical sectors. This may well be remembered as the year the defenders fought back decisively against cybercriminals. Here are our top 5 cybercrime stories of 2024.

British Library

The effects of the British Library ransomware attack at the end of 2023 continued to be felt into 2024 as the venerable institution continued to struggle to bring its crippled systems back online. In January 2024, it emerged that the scale of the ransomware attack was so immense and its effects so devastating, it could end up costing the British Library up to £7m, dwarfing the £650,000 ransom demand. Later in the year, in a remarkable display of transparency, the British Library's leadership published a detailed breakdown of their experience at the hands of the Rhysida ransomware crew, to help others learn and understand. The Library has not made any payment to the criminal actors responsible for the attack, nor engaged with them in any way. This is in accordance with the policy of the UK government and the NCSC.

Cozy Bear

In January, Cozy Bear, the Russia-backed hacking group infamous for orchestrating the SolarWinds Sunburst incident, resurfaced. This time, the group targeted Microsoft, using a brute force and password-spraying attack to penetrate the company's systems. Once inside, the hackers managed to access sensitive corporate accounts, including those belonging to leadership and security personnel. Microsoft, like many globally integrated suppliers, is a prime target for such intrusions due to its vast reach, significant market presence, and close partnerships with Western governments. The company has faced mounting scrutiny and tough questions regarding its security practices, with incidents like this one further highlighting the challenges it faces in safeguarding its systems and client data from sophisticated adversaries.

NHS attack

In early June, a devastating cyberattack targeted Synnovis, a key provider of pathology lab services that supports several major healthcare institutions, including Guy's and St Thomas' hospitals, King's College Hospital, and other NHS facilities across London. The attack, carried out by the Qilin ransomware group, severely disrupted operations and had catastrophic consequences for the healthcare system. The intrusion forced the NHS to declare a major incident as critical services ground to a halt. Patient appointments and surgeries were cancelled en masse, creating a backlog that overwhelmed healthcare providers, while blood supplies - a vital resource for surgeries and emergency care - dwindled to dangerously low levels. The aftermath of this cruel and calculated attack has reverberated through the NHS for months, leaving a trail of operational and financial strain, with efforts to restore normalcy continuing six months later. The incident underscores the vulnerability of critical healthcare infrastructure to cybercrime and highlights the dire human impact of such malicious acts.

MoneyGram

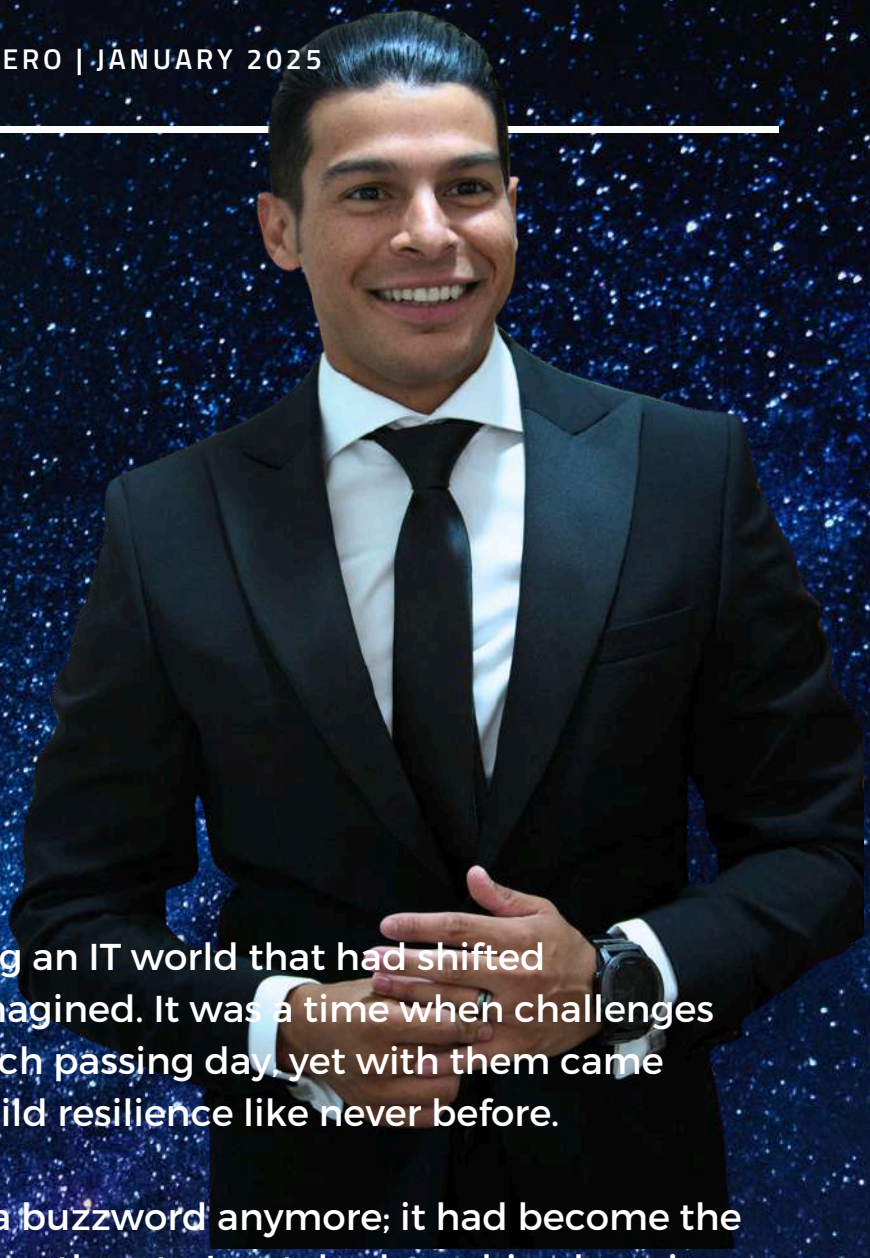
US-based financial services and money transfer outfit MoneyGram was another high-profile cyberattack victim to emerge in 2024, with its systems taken down in an apparent ransomware attack in September 2024. MoneyGram's customers in the UK include the Post Office, which cancelled its contract with the beleaguered supplier shortly thereafter with immediate effect – apologising to its sub-postmasters for giving them barely 24 hours' notice of this. It has since emerged that MoneyGram customer data was stolen in the attack, which most likely began through a social engineering attack on its IT helpdesk.

Scattered Spider arrest

Proving that social engineering, unfortunately, works, a British national now named as 22-year-old Tyler Robert Buchanan was charged in the US in November 2024 with offences relating to the Scattered Spider cyberattacks. A year previously, Scattered Spider hit multiple companies, including high-profile Las Vegas casino operators, and many others, via audacious social engineering attacks that often targeted helpdesks, frequently by exploiting Okta identity services. The Scattered Spider gang was unusual in the current threat environment in that its core members were all US and UK-based, proving once and for all that not all cybercriminals have Russian accents. Buchanan faces over 40 years in prison in the United States.

zhero

Cyber insights



Zaheer Rahman our amazing Technical Lead, belives that 2025 will be a new era of digital defence in cybersecurity. Here's Zaheer's take on the state of IT support and cybersecurity in the year ahead.

In 2024, I found myself navigating an IT world that had shifted dramatically, faster than I ever imagined. It was a time when challenges grew more sophisticated with each passing day, yet with them came opportunities to innovate and build resilience like never before.

Artificial intelligence wasn't just a buzzword anymore; it had become the backbone of our fight against cyber threats. I watched machine learning algorithms do what once seemed impossible—spotting unusual patterns and vulnerabilities in real time. It felt almost surreal to see systems patch themselves before a threat could take hold, like a living, breathing defense mechanism. Yet, it wasn't all victory dances. Cybercriminals had also embraced AI, crafting attacks that were sharper, faster, and harder to predict. The stakes were higher, and my team and I had to adapt constantly, racing to outsmart threats before they reached us.

One of the most transformative shifts was how we thought about trust—or rather, how we stopped trusting anything by default. The "Zero Trust" model became my mantra. Every device, every user, every application had to prove itself, whether it was within our walls or connecting from halfway around the world. It wasn't easy, but the payoff was worth it. Insider threats became less daunting, and unauthorized access felt like a distant memory. For me, it meant living in a world of strict access controls and constant vigilance, where no door was ever left unlocked.

Cloud services became both a blessing and a puzzle. The flexibility was unmatched, but spreading data across multiple providers came with its own set of headaches. I had to dive deep into multi-cloud and hybrid-cloud strategies, ensuring no single point of failure could put us at risk. Encryption tools, identity management systems, and multi-factor authentication became my closest allies. Managing it all wasn't just about tools; it was about ensuring every piece fit seamlessly into our broader security puzzle.

Through all of this, one truth stood out: no matter how advanced the technology became, people remained at the heart of the solution—and sometimes, the problem. Cybersecurity wasn't just about firewalls and algorithms; it was about awareness. Phishing emails and social engineering attacks still haunted me, a stark reminder that even the best systems couldn't replace human vigilance. Training became a cornerstone of our strategy. I poured energy into equipping my team with the skills they needed to stay ahead of the curve, knowing that their expertise could make or break our defenses.

As I reflect on this new era, I can't help but feel a mix of awe and determination. The world of cybersecurity in 2025 is alive with potential and fraught with challenges. Each day demands a careful balance—embracing cutting-edge innovations while holding fast to proven principles. It's a dynamic, unpredictable journey, but I know one thing for sure: staying agile and prepared is the only way forward in this ever-changing digital frontier.

zhero SHOW STOPPERS

Every December, we proudly annouce our superlative team members at the annual Zhero Staff Awards. Here are the winners for 2024!

Louise Niemand, our amazing Finance Controller, is best in Leadership and Zhero's Core Values. Congratulations on two awards!

Our ace developer, the one and only Louis Oosthuizen, was the best ambassador of Zhero's Vision.

Kian Botha, an exemplary member of the Service Desk took home the Reliability and Brand Promises awards. Congrats on the double win!

zhero SHOW STOPPERS

Ryan Leech, a formidable Remote Engineer, was the recipient of the Determination award.

Mikello Terblanche, our incredible Internal Sales guy, received the well-deserved Zhero's Purpose accolade.

Showing awesome perseverance, Tier 0 Engineer Macwhill Hanse was the proud receiver of the Role Acceleration award.

Best-of-breed Service Desk Engineer, Marc Van Romburgh, nabbed the coveted Teaching & Coaching gong.

Meet the team

Jacolene Haasbroek

ASSISTANT

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

It's a very interesting industry. Heading into the future the IT industry is just going beyond anyone's imagination.

What's your most-used productivity tool?

Microsoft 365 is my go-to. And also, I would find it difficult to work without Xero.

How would you describe yourself?

I love being outdoors, whether it's hiking, exploring, or just enjoying nature. I have a great sense of humour and enjoy bringing laughter and fun to every moment.

What do you enjoy the most about your role?

The opportunity to learn new things every day. It keeps me curious, challenged, and constantly growing both personally and professionally.

Do you have any hidden talents or hobbies?

I enjoy camping and fishing. Being out in nature is one of my favourite ways to relax and have fun.

What is your favourite movie or TV show?

Sports are on top. We watched the dart world championship that was held in December '24/January '25 in the UK at the Alexandra Palace. That was just brilliant!!!

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