JUNE 2025

inside zhero

AI at Work

A Workplace Roadmap

Cover Your Risk

Cyber Insurance for SMEs

Cyber Celebrations

Cyber London has a Birthday

Message from Izak

Welcome to our June edition of Inside Zhero.

This time, we're seeing how AI will transform the way we work. There are also some amazing insights from our driven onsite engineer, Wajahat Khan. We also have a birthday to celebrate - Cyber London turns one!

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "AI at Work" shows the potential of artificial intelligence as a tool to transform the way we work.

72% of business leaders report a significant productivity boost as a result of comprehensive AI adoption in their organisations.

"I've seen firsthand how AI is transforming the workplace. It's changing the way we operate, opening up new opportunities for greater efficiency, creativity, and productivity. It's incredible how AI can take over repetitive tasks, help us connect with customers more effectively, and make sense of complex data in ways we couldn't before. But with all these benefits, I also know it brings important legal and ethical questions we need to think about carefully. "

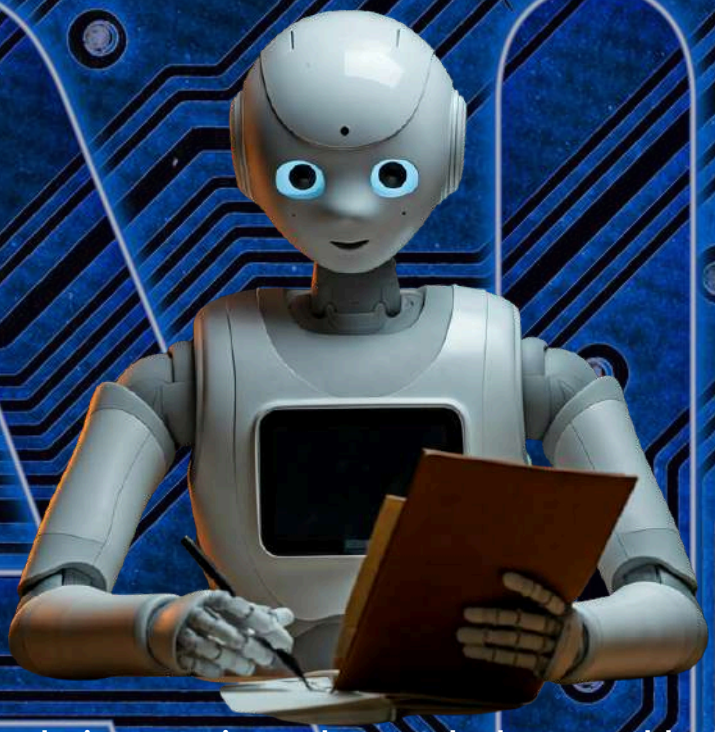
Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

30% discount **cyberzhero542**



AI AT WORK

Artificial intelligence has made its way into the workplace and holds the potential to be as transformative as the steam engine was during the Industrial Revolution. With the development of advanced large language models by major technology firms such as Anthropic, Cohere, Google, Meta, Mistral, and OpenAI, we are entering a new era of information technology. The long-term promise of AI is substantial, with potential productivity gains from corporate use cases estimated at $4.4 trillion. However, the short-term benefits remain less clear. Over the next three years, 92% of companies plan to increase their investment in AI. Despite this, only 1% of business leaders consider their organisations to be truly mature in their AI deployment, where the technology is fully integrated into workflows and delivers significant business outcomes. The key challenge for leaders is how to allocate resources effectively and steer their organisations towards greater AI maturity, to the point where the technology becomes the foundation of any successful business.

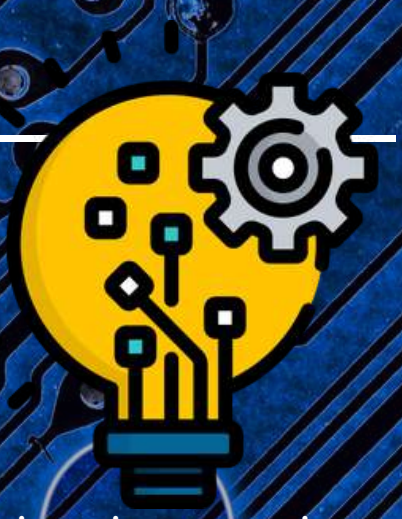
Benefits of AI in the workplace

- **Increased efficiency and productivity** - AI can automate repetitive tasks, enabling employees to concentrate on more strategic and creative activities.
- Improved decision-making - AI-driven analytics can identify trends, predict outcomes, and support more informed decision-making.
- **Reduced costs** - Automation minimises human error, streamlines manual processes, and boosts overall efficiency, resulting in cost savings.
- Enhanced risk management - AI can analyse data to detect potential risks and anomalies, helping to prevent fraud and other issues.
- **Personalised learning and development** - AI can customise training programmes to address individual skill gaps and development needs, promoting growth and engagement.
- Improved employee satisfaction - AI can assist employees in managing workloads, accessing information quickly, and receiving real-time feedback, contributing to a more positive work environment.
- **Streamlined collaboration** - AI-powered tools can improve communication, coordination, and teamwork, supporting a more collaborative and productive workplace.

"People are using AI to create amazing things. If we could see what each of us can do 10 or 20 years in the future, it would astonish us today."

Sam Altman, cofounder and CEO of OpenAI

Hardware innovation



Ongoing hardware innovation and the resulting increase in computing power continue to improve AI performance, with specialised chips now supporting faster, larger, and more adaptable models, making it easier than ever for businesses to adopt AI solutions that demand high processing capacity, enabling real-time applications and greater scalability. For instance, an e-commerce company could enhance its customer service by deploying AI-driven chatbots powered by advanced graphics processing units (GPUs) and tensor processing units (TPUs), ensuring quick and intelligent responses. By leveraging distributed cloud computing, the company can maintain optimal performance even during periods of high traffic, while the integration of edge hardware allows it to run models that analyse images of damaged products—streamlining insurance claims with greater accuracy and speed. Fun fact: The world's fastest supercomputer, Frontier, can perform over a quintillion (that's a billion billion!) calculations per second, many of which are used to support cutting-edge AI research.

“Scientific discoveries and technological innovations are stones in the cathedral of human progress.”

Reid Hoffman, the cofounder of LinkedIn and Inflection AI

Increasing transparency

AI is gradually becoming less risky, but it still lacks sufficient transparency and explainability. These elements are essential for enhancing AI safety and reducing the potential for bias, both of which are critical for widespread adoption in enterprise settings. While there remains a long way to go, new models and updates are driving rapid progress. According to Stanford University's Centre for Research on Foundation Models (CRFM), significant improvements are being made in model transparency. The CRFM's Transparency Index, which rates openness on a scale from 1 to 100, showed that between October 2023 and May 2024, Anthropic's score rose by 15 points to 51, while Amazon's more than tripled to 41. These gains indicate a growing focus on openness among AI developers, though many models still fall short of ideal standards.

Improved explainability

Other forms of AI and machine learning are also improving in explainability. These advancements allow the outcomes in critical decisions, such as credit risk assessments, to be traced back to the underlying data. This enables organisations to continuously monitor such systems for bias, inaccuracies, and other issues that may arise from model drift or changes in input data, even in systems that were initially well-calibrated. These capabilities are vital for detecting errors and ensuring adherence to regulatory requirements and internal policies. Many organisations have begun implementing stronger explainability practices and introducing essential checks and balances. Ultimately, achieving AI superagency in the workplace is not just about technical proficiency. It is also about empowering people, designing effective processes, and upholding robust governance.

Challenges and risks

- **Job displacement** - Some roles may be automated by AI, potentially resulting in job losses or the need for reskilling and upskilling.
- **Data privacy concerns** - AI systems often require large volumes of data, including sensitive personal information, raising concerns about data breaches and unauthorised access.
- **Ethical considerations** - AI can produce biased or discriminatory outcomes if trained on biased data, leading to unfair or unjust decisions.
- **Lack of transparency** - Some AI systems operate as "black boxes," making it difficult to understand how decisions are made, which raises issues around accountability and fairness.
- **Dependence on technology** - Over-reliance on AI may reduce human oversight and weaken decision-making skills.
- **Need for continuous learning** - As AI continues to evolve, employees will need to adapt to new roles and technologies, requiring ongoing learning and development.

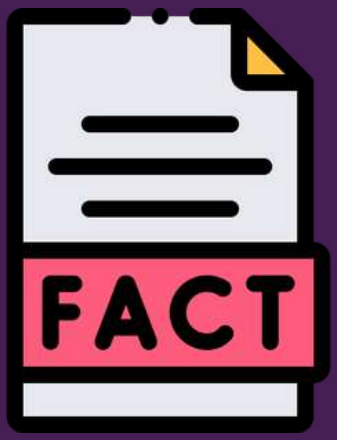
The thing is, if we know how to manage and control challenges and risks, we can potentially turn them to our advantage.

"Soon after the first automobiles were on the road, there was the first car crash. But we didn't ban cars, we adopted speed limits, safety standards, licensing requirements, drunk-driving laws, and other rules of the road."

Bill Gates, founder of Microsoft

Workplace roadmap

Business leaders are responding to the need for speed by increasing their investment in AI. Among surveyed executives in a McKinsey report, 92% expect to raise AI spending over the next three years, with 55% anticipating an increase of at least 10% from current levels. However, simply investing in AI is no longer enough; there is growing pressure to demonstrate a clear return on investment as organisations move beyond the initial excitement surrounding generative AI. We have reached a pivotal moment. While early enthusiasm for AI may be tapering off, the pace of technological advancement is only accelerating. This calls for bold, purposeful strategies to lay the groundwork for long-term success. Many leaders are already taking action: one in four executives surveyed has established a generative AI road map, and just over half are refining a draft plan. Given how rapidly the technology is evolving, these plans must remain flexible and responsive. The key for business leaders is to make clear decisions about which opportunities to prioritise, and to collaborate closely with peers, teams, and partners to realise that value effectively.



- Around 75% are using AI at work, with a substantial increase in usage over the past six months.
- The AI market is expected to continue expanding, with a projected value increase of around 5x over the next five years.
- The number of UK AI companies has increased by over 600% over the last 10 years.

Ethical concerns

AI in the workplace raises several ethical issues, including privacy, bias, accountability, and the risk of job displacement, all of which require careful attention to ensure responsible use. Privacy concerns arise from data collection and surveillance, demanding transparency and regulatory compliance. Bias in AI algorithms can lead to discrimination, necessitating careful data management and monitoring. Clear accountability is essential when AI impacts individuals, along with transparency about how decisions are made. The automation of tasks may cause job losses, highlighting the need for retraining and support. Maintaining human agency is important to avoid over-reliance on AI that could undermine skills and creativity. Moral responsibility for AI actions is complex, involving developers and employers. The broader social impact includes effects on values, norms, and economic inequality, while environmental concerns relate to AI's energy use. Additionally, generative AI raises copyright and plagiarism issues that must be addressed. Overall, these challenges call for thoughtful, proactive measures to manage AI's ethical implications in the workplace.

"We need to be sure that in a world that's driven by algorithms, the algorithms are actually doing the right things. They're doing the legal things. And they're doing the ethical things."

Marco Iansiti, Harvard Business School

Google DeepMind

“It is in the collaboration between people and algorithms that incredible scientific progress lies over the next few decades.”

Demis Hassabis, cofounder and CEO of Google DeepMind

Many groundbreaking technologies, such as the internet, smartphones, and cloud computing, have reshaped the way we live and work. However, AI stands apart from these innovations by offering more than just access to information. It can summarise, write code, reason, engage in conversation, and make decisions. AI can lower skill barriers, allowing more people to gain expertise across various fields, in any language and at any time. It holds the potential to transform how individuals access and apply knowledge, leading to more efficient and effective problem-solving and enabling innovation that benefits all.

zhero

A Journey into Cybersecurity

This month, one of our amazing onsite London-based engineers, Wajahat Khan, reveals his amazing journey into cybersecurity, aptly titled “From Pixels to Protectors.” Wajahat is married to Tooba Qasim, a PhD student at City St George’s University, who is partly sponsored by Zhero. More about Tooba later so now on with Wajahat’s story.

It all began with a simple game—Super Mario, the bright, pixelated plumber bouncing through colourful worlds, and Duck Hunt, where I’d sit for hours aiming and shooting, enthralled by the challenge. As a young kid, I was captivated by the magic of gaming, not just for entertainment but for the wonder of how these digital worlds came alive. From those early days, my fascination with technology grew like a seed planted deep within my soul, yearning to explore the endless possibilities of the digital universe. From Nintendo, Atari & Sega to Playstation, Xbox and Gaming Laptops, you name it and I’ve been there, done that.

zhero

A Journey into Cybersecurity

Growing up in a world where technology was evolving rapidly but equipped with limited resources, I was eager to keep pace. I pursued a degree in Computer Software Engineering—a step that felt natural, almost destined. During study, I channelled my passion into real projects. My first was creating a virtual tour for my university, transforming a simple campus map into an interactive digital experience. It was my first taste of turning imagination into reality through code. As I delved deeper, I developed educational games with student and teacher portals as part of a project funded by DFID, aiming to make learning fun for children. These projects weren't just assignments; they were milestones, each teaching me something new about the power of technology to influence lives.

But life is rarely a straight path. I wore many hats—software engineer, game developer, lecturer, IT support engineer—each role adding a new layer to my understanding of technology and its impact. The thrill of developing games, the satisfaction of teaching others, and the technical mastery of managing complex systems kept my passion alive. Yet, as I stepped into the world of work, I also embraced responsibilities beyond coding—marriage, family, and the realities of adult life.

In Pakistan, I took on a government role at a tax-collecting authority. Here, I thought I'd find my calling, but something was missing. The more I immersed myself in managerial duties and bureaucratic processes, the more I felt a distant echo of my earlier dreams. My passion for IT began to fade—not because of the work itself, but because life had shifted my focus. The carefree days of youth, filled with endless curiosity and dreams of innovation, seemed like a distant memory. I was now a father, navigating a new paradigm where responsibilities overshadowed passion. The transition was profound, almost untellable—an internal journey from freedom to responsibility, from dreamer to provider.

zhero

A Journey into Cybersecurity

Then, life threw a curveball: after six years in government service, my wife was awarded a scholarship for her PhD at City University of London. Respecting her dedication and dreams, I made a tough decision—to leave the familiar and accompany her across the world. Moving to London was a whirlwind of challenges. Coming from a third-world country, I found myself in a bustling, fast-paced city, trying to hold onto my identity while adapting to a new culture. Juggling odd jobs, battling feelings of regret, and worrying about the future, I often wondered if I had taken the right path. I questioned whether I should have pushed further into game development, where my heart truly lay.

Yet, amidst the chaos, I began to notice something. My wife, immersed in her studies on cybersecurity and quantum cryptography, was inspiring me. Her dedication rekindled a spark within me. I started reading about recent cyberattacks, data breaches, and online fraud—stories that painted a stark picture of a world needing protection. The blackouts in cities, the rise of phishing scams, the theft of personal data—these weren't just headlines; they were signs that our digital world was vulnerable. I realized that cybersecurity wasn't just a technical field; it was a vital shield safeguarding our lives, our identities, our futures.

zhero

A Journey into Cybersecurity

My curiosity grew into a passion. Every new concept was a piece in a puzzle—one I desperately wanted to solve. Then, an opportunity arose. I went through assessments and landed a role at Zhero as an Onsite Engineer. It was a turning point. Suddenly, I was back in the thick of IT—fighting chaos, securing systems, and defending digital assets. My past skills came rushing back, but this time, I was armed with new knowledge, new trends, and a fresh purpose.

Joining Zhero wasn't just a job; it was a rebirth. Even within a few months, I could see my growth—understanding the latest cybersecurity methodologies, implementing protective measures, and learning how to stay ahead of cyber threats. The thrill of unravelling complex problems, of securing systems from unseen enemies, reignited my passion. I realized that my journey wasn't just about personal fulfilment—it was about making a difference, protecting society from the unseen dangers lurking online.

Looking ahead, I see a future where I can deepen my expertise, contribute to creating safer digital environments, and perhaps, inspire others to pursue their passions regardless of the setbacks. My story isn't just about coding or cybersecurity; it's about resilience, rediscovery, and the relentless pursuit of dreams. From a young gamer captivated by pixels to a cybersecurity enthusiast safeguarding the digital world, my journey continues—with every challenge, a new opportunity to grow and serve.

COVER YOUR **RISK**

The UK government's Cyber Security Breaches Survey 2025 paints a clear picture of how serious the cyber threat landscape has become. According to the survey, 43% of businesses reported experiencing a cyberattack or security breach in the past 12 months. These incidents don't just cause disruption — they can be expensive too. The average cost of the most disruptive breach was £1,600, and for those that did incur a cost, that figure rose to £3,550. That's a significant financial hit, especially for smaller businesses that may not have the resources to bounce back easily. Despite the growing risks, many small and medium-sized enterprises (SMEs) still don't have adequate protection in place. A separate 2025 survey found that just 40.2% of SMEs currently hold a cyber insurance policy. This means that nearly 60% of the sector remains exposed to the financial and operational fallout that can follow a cyber incident. Whether it's a ransomware attack, data theft, or prolonged system downtime, the consequences can be severe, and yet, the uptake of cyber insurance remains low.

The threat from AI

AI is increasingly being used by cybercriminals to create more sophisticated attacks. More than a third of SMEs now list AI-driven threats as their number one cybersecurity concern. These types of attacks are particularly dangerous because they can scale quickly and are often harder to detect. For example, AI can be used to automate phishing campaigns, craft convincing fake emails or messages, and even identify and exploit weaknesses in a company's defences. Traditional security tools often struggle to keep up with this new wave of intelligent, adaptive threats. Businesses of all sizes — but especially SMEs — need to start thinking more seriously about both prevention and protection. That means not only improving their cybersecurity measures but also considering the safety net that insurance can provide when things go wrong.

Enter cyber insurance

Cyber insurance covers costs like investigation, remediation, legal fees, and compensation to affected parties. In the UK, policies are available for businesses of all sizes, with limits ranging from £100k to £5 million, and higher for firms with more complex risks. Cyber insurance can cover a wide range of costs associated with a cyberattack, including

- **Incident response** - costs to contain and recover from a cyberattack.
- **Data restoration** - Costs to recover lost or corrupted data.
- **Legal fees** - Costs associated with defending against lawsuits or regulatory investigations.
- **Business interruption** - Lost income due to a cyberattack that disrupts business operations.
- **Third-party liability** - Legal costs and damages related to claims from third parties affected by a data breach.

Financial safety net

Cyber insurance offers many benefits to SMEs:

- **Financial Protection** - Cyber insurance helps cover the costs associated with a cyberattack or data breach, including incident response, legal fees, data restoration, and business interruption.
- **Reduced Risk** - By mitigating the financial impact of a cyber incident, cyber insurance can help businesses focus on recovery and rebuilding trust, rather than struggling with high costs.
- **Legal Support** - Cyber insurance policies often include coverage for legal fees and expert advice related to the incident, providing crucial support during a crisis.
- **Reputation Management** - Cyber insurance can cover the costs of PR and communication efforts to manage the fallout from a cyber incident and protect the business's reputation.
- **Compliance** - Many cyber insurance policies include coverage for regulatory fines and penalties that may arise from a data breach.
- **Peace of Mind** - Knowing that the business is financially protected from the risks of cybercrime can provide valuable peace of mind and allow for a more proactive approach to security.
- **Commitment to Security** - Obtaining cyber insurance can demonstrate a commitment to security and can help attract customers and partners who value data protection.
- **Expert Support** - Insurers may offer access to cybersecurity expertise and threat intelligence services, assisting with vulnerability assessments, staff training, and password management.
- **Business Continuity** - Cyber insurance can help cover the costs of business interruption, including lost income and increased operational expenses, allowing businesses to maintain operations during a cyber incident.

What insurers want

Businesses need to show they take cybersecurity seriously by meeting specific requirements set by insurers. This typically includes having strong security controls, an incident response plan, and clear documentation of your IT infrastructure and practices. Insurers will often start with a cybersecurity risk assessment to understand your current posture and identify vulnerabilities. They'll expect to see robust security measures in place, such as firewalls, intrusion detection systems, and multi-factor authentication, along with policies for data classification and access control to ensure only authorised staff can access sensitive information. . You'll need to provide details on your IT environment, including the security software and hardware you use, your network architecture, and whether you're encrypting data in transit and at rest. Insurers may also look for ongoing employee training programs that raise awareness of threats like phishing and teach proper handling of sensitive data. Other key areas include vulnerability management, assessing the cybersecurity practices of third-party vendors, and having a business continuity plan to minimise downtime and recover operations quickly after an incident.

Getting insurance

You can contact an insurer directly or through a broker specialising in cyber risk insurance. Brokers like the British Insurance Brokers' Association (BIBA) can assist in finding the right policy for your specific needs. You can also explore online platforms like PolicyBee or look into options like Hiscox, which offer cyber insurance and business interruption coverage. Brokers like Sutcliffe & Co. Insurance Brokers who specialise in cyber insurance and may offer specific policies, like the Cyber Essentials policy from IASME.

CYBER LONDON

BIRTHDAY CELEBRATIONS

This month, Cyber London celebrates its 1st birthday, and there's so much and more to celebrate! None of the events, webinars, mentoring and social media achievements would have been possible without these people - clockwise from the top: Cyber London's Directors, Simon, Raj, Mark, Izak and Paresh, Cyber London Community Manager, Lucindi, and volunteers, Tooba and Solmaz. Happy Birthday, Cyber London and many more to come!

BRIDGING WORLDS

Last month, Cyber London hosted the "Bridging Worlds" event at City St George's University for students and staff from Maryville University in St. Louis, Missouri. Prof Raj ran the session, and amazing cyber and career insights were provided by Matthew Eccles from City of London Police, Cyber London co-director, Paresh Deshmukh, and Michal Khol, a senior lecturer in Computer Science. Tooba Qasim, a Doctoral Researcher at City, University of London, closed the session by relating her journey into the world of quantum cryptography. She also thanked Izak and Raj for their support and encouragement:

"Both of them created a door for me and then helped me walk through it."

Windows 10 EOL

On 14 October 2025, Windows 10 Home and Pro will reach 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.

WHAT THIS MEANS

After 14 October 2025, your Windows 10 PC will no longer receive free security updates and Microsoft will no longer be available to provide Windows 10 technical support. 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.

Meet the team

Tomasz Jakubczyk

BUSINESS DEVELOPMENT EXECUTIVE

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

I am naturally curious about how things work and find technology captivating. This curiosity led me to explore its inner workings and applications, eventually sparking an interest in IT as a career path.

What's your most-used productivity tool?

OneNote, I have found Trello useful and GenAI tools that offer assistance with writing, brainstorming, and research. I still believe in post-it notes - they work wonders, believe me !

How would you describe yourself?

I am open and honest and don't believe in misleading people, and try to be fair in everything I do. I value flexibility, authenticity, and a pragmatic approach to addressing problems.

What do you enjoy the most about your role?

I find the greatest fulfilment in identifying and pursuing strategic growth opportunities. Seeing my work directly contribute to the company's overall growth and success is incredibly rewarding.

Do you have any hidden talents or hobbies?

I find cooking and exercising outdoors very relaxing . It allows me to clear my head . I am also kind of a wine buff.

What is your favourite movie or TV show?

I believe that European and Asia movies are far superior to the US however, still prefer to grab a non-fiction or SF book rather than binge watch a tv show on Netflix.

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