DECEMBER 2024

inside zhero

Countering Cyber Threat

State-of-Play UK Cybersecurity

Paying the Price

Cybersecurity is a Business Investment

Safe and Ethical AI

Regulatory Insights from Alan

Message from Izak

Merry Christmas and welcome to our super cyber festive edition of Inside Zhero.

Our focus this month is on the cyber threats facing the UK and the cybersecurity practices we can put in place to deter these. You'll also get an exclusive sneak peek at the fun we've been up at Zhero!

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Countering Cyber Threat" examines the cybersecurity landscape in the UK based on the findings of the National Cyber Security Centre.

The cost of cybercrime in the UK is £27 billion every year.

"Cybersecurity is a responsibility we all share, and everyone has a role to play. Whether you are working to maintain the UK's critical infrastructure and ensuring essential services like electricity remain operational or setting up a tablet for your child at home, your actions matter. By staying informed, practising safe online habits, and remaining vigilant, we can all contribute to strengthening our collective online resilience and protecting our digital world. "

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consulation

30% discount **cyberzhero542**

COUNTERING CYBER THREAT

The National Cyber Security Centre (NCSC) is all about tackling the cyber threats facing the UK. Whether it's dealing with state-sponsored hackers, the spread of commercial cyber tools, ransomware, or the latest AI-driven attacks, the NCSC uses its technical know-how and unique position in government to handle both old-school and cutting-edge challenges. They work closely with law enforcement and international allies to stay ahead of the game. Ransomware is still the most pressing and disruptive threat to the UK's critical national infrastructure (CNI). Some state-backed groups are even going after industrial control systems that keep essential services running. To tackle this, the NCSC's Incident Management team teams up with the Information Commissioner's Office (ICO) and experts from the legal and insurance industries to create guidance on "ransom discipline." This is all about reducing how often victims pay up after ransomware attacks. It's just one example of how the NCSC collaborates with government bodies and private companies to boost the UK's cyber defences and build resilience against growing threats.

NCSC annual review

In early December, the NCSC published its Annual Review 2024, highlighting key achievements and milestones from 1 September 2023 to 31 August 2024 and exploring the challenges ahead. In a nutshell, the report umbrellas the UK cyber landscape under four categories:

- Countering cyber threat
- Building cyber resilience
- Developing the cyber ecosystem
- Keeping pace with technology

National Cyber Security Centre

All about the NCSC

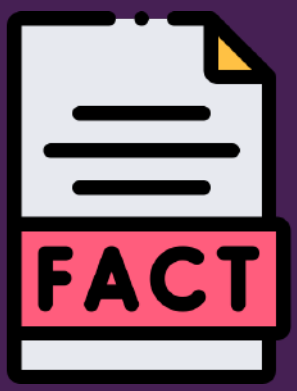
The NCSC was formed in 2016 by combining the government, MI5 and GCHQ, to create the UK's technical authority for cybersecurity. It aims to make the UK the safest place to live and work online. The NCSC supports the most critical organisations in the UK, the wider public sector, industry, small and medium-sized organisations and the general public. The NCSC reduces cyber risks to the UK by helping secure public and private sector networks and reduces the cyber threat by seeking to understand and disrupt it. The NCSC works collaboratively with law enforcement organisations, the UK's intelligence and security agencies, international allies and government partners. The NCSC works with the Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA) in the United States, NATO, the UN, INTERPOL, the FBI and many more household names.

Threats from China

China remains a highly sophisticated and capable cyber threat actor, targeting a broad range of sectors and institutions worldwide, including in the UK. In February, the NCSC issued an advisory highlighting compromises of the United States critical national infrastructure (CNI) by "Volt Typhoon," a China state-sponsored threat actor. The targeting of sectors such as energy, transportation, and water suggests potential preparations for future disruptive or destructive cyberattacks, underscoring China's intent to threaten essential networks. The NCSC continues to collaborate with government, international allies, industry, and academia to deter, disrupt, and detect the cyber threats posed by China

Richard Horne, CEO of the NCSC says:

"All the while, China remains a highly sophisticated cyber actor, with increasing ambition to project its influence beyond its borders."



Bigtime hackers

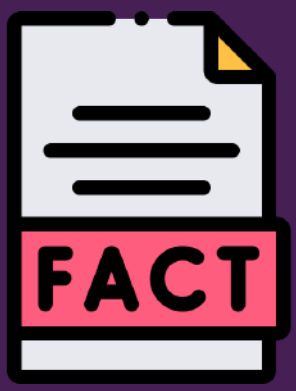
A few countries house the greatest cybercriminal threat. Russia tops the list, then Ukraine, China, the USA, Nigeria, and Romania. Russia is a major source of phishing attacks around the world. In 2023, over 30% of all unsolicited spam emails came from Russia.

Threats from Russia

Russia remains a capable, motivated, and reckless actor in cyberspace. Russian cyber threat actors have almost certainly escalated their operations against Ukraine and its allies, aligning with their military objectives and broader geopolitical goals. These activities in Ukraine have also emboldened non-state actors to launch cyberattacks on Western CNI. While these non-state actors operate without formal or direct state control, their actions remain ideologically aligned with Russian interests, and the Russian state bears responsibility for enabling these attacks. The NCSC continues to expose Russian cyber activities publicly, creating a more challenging environment for such actors to operate effectively.

Anne Keast-Butler, the Director of GCHQ tells us:

"There's been an increase in cyber operations against Ukraine and its allies in support of Russia's military campaign and its wider geopolitical objectives."



UK by numbers

- **In 2023, UK businesses experienced 7.78 million cybercrimes – that's 21,315 cyberattacks per day.**
- **The average cost of a cyberattack to a UK business was £3,230.**

Building cyber resilience

With emerging technologies like AI speeding up the volume and sophistication of cyberattacks, the NCSC is stepping up to protect the UK's critical systems from advanced threats while also bolstering defences against more common attacks across the economy. As part of GCHQ, the NCSC uses its unique insights and works closely with government, industry, and academia to keep the nation's digital landscape secure. From rolling out cutting-edge active cyber defence services and pushing for legislative and regulatory reforms to shaping security standards for new tech and growing the UK’s cyber ecosystem, the NCSC is focused on building strong cyber resilience across the board.

Developing the cyber ecosystem

The NCSC is a key player in strengthening the UK’s cybersecurity scene, which now pumps about £11.9 billion into the economy every year. By bringing together government, industry, and academia, the NCSC helps create a thriving ecosystem that supports everything from inspiring students in schools and opening doors in higher education to funding cutting-edge research and connecting innovative tech startups. This growing sector now employs nearly 61,000 people but keeping it strong means ensuring a steady stream of skilled professionals, quality products, and trusted services. To make that happen, the NCSC works with partners to set standards, validate products and services, and grow the talent pipeline needed to keep building resilience and boosting digital capabilities across the board.

Keeping pace with technology

As the UK's go-to authority on cybersecurity, the NCSC has to keep up with fast-moving technologies, especially those that have a big impact on critical systems and industries. Some of these changes directly affect everyday users—like switching from passwords to passkeys for better security and convenience. Others are more about helping developers, like improving how software is built to reduce vulnerabilities in the apps and devices we all rely on. To stay ahead of the game, the NCSC needs expertise across the tech world to spot new opportunities, risks, and threats. The team dives deep into research on emerging technologies, coming up with smart ways to reduce harm at scale. While some tech, like artificial intelligence, brings big, disruptive challenges that need careful attention, other areas evolve more slowly but still pack a punch. Take cloud computing and IoT - these might not feel "new" anymore, but because they're everywhere, even small tweaks to their standards or infrastructure can have a huge ripple effect on system resilience.

Wise cyber words

At the launch of the NCSC Annual Review 2024, Richard Horne described the cyber risks facing the nation as "widely underestimated" and called for collective action against an increasingly complex array of threats. He proposed an organisational commitment to cybersecurity as a prerequisite for UK business to thrive.

Richard says:

""We need all organisations, public and private, to see cyber security as both an essential foundation for their operations and a driver for growth. ."

Prof Raj Rajarajan, Zhero's Head of R&D, Professor of Security Engineering at City University of London, and a Director at Cyber London believes there is is an immediate need for organisational cultural change to incorporate cyber security into all aspects of the business.

Raj says:

"We need the boards to start educating themselves on cyber threats and make it part of their core business processes."

PAYING THE **PRICE**

Former IBM executive chairman and CEO Ginni Rometty described data as a transformative competitive advantage for the 21st century. He emphasized that cybercrime is, and should be recognized as, the greatest threat facing industries and organizations worldwide. According to Cybersecurity Ventures, global data storage is expected to reach 200 zettabytes by 2025 – a staggering total equivalent to one trillion gigabytes. This vast amount of data carries tremendous value, making it an ever-appealing target for cybercriminals.

Ransomware as-a-Service

A key factor driving the surge in cybercrime is the reduced need for advanced technical expertise to carry out attacks. For instance, malware can be easily purchased on the dark web, alongside illegal services offering Ransomware-as-a-Service (RaaS). These RaaS kits often include features like quality assurance, helpdesk support, and even money-back guarantees, making cyberattacks more accessible than ever before.

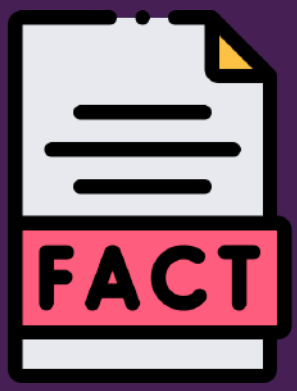
Economic costs

Cybercrime has exploded, becoming the world's third-largest economy after the U.S. and China, according to the World Economic Forum. It now makes more money than global drug trafficking, counterfeiting, and human trafficking combined. In 2023 alone, cybercrime cost $8 trillion, and experts think it could hit $10.5 trillion by 2025. To put that in perspective, Microsoft, one of the richest companies in the world, made about $200 billion in revenue in 2022. Cybercrime, on the other hand, operates on a scale 50 times bigger. The impact isn't just about the criminals getting rich—it's about the massive damage they cause to businesses and economies. Take the 2017 WannaCry ransomware attack: it spread to over 200,000 computers in more than 100 countries, hitting industries like healthcare and tech hard. In just four days, it caused $8 billion in damages. Some regions are hit worse than others. A study by the Centre for Strategic and International Studies (CSIS) and McAfee found that Europe loses the most to cybercrime, with costs equal to 0.84% of its GDP. North America isn't far behind, losing 0.78% of its GDP. Cybercrime is costing us big time.

Collateral damage

Estimating the true cost of cybercrime is challenging due to its vast scope, varying definitions, and inconsistent measurement methodologies. Costs span a wide array of impacts, including:

- Damaged intellectual property (IP) and confidential business data
- Stolen personally identifiable information (PII)
- Bank account and financial data theft
- ·Financial manipulation and insider trading
- Loss of trust and reputation
- Operational disruptions
- Ransom payments
- Corporate smear campaigns and disinformation via social media
- Political interference
- Costs of post-attack recovery

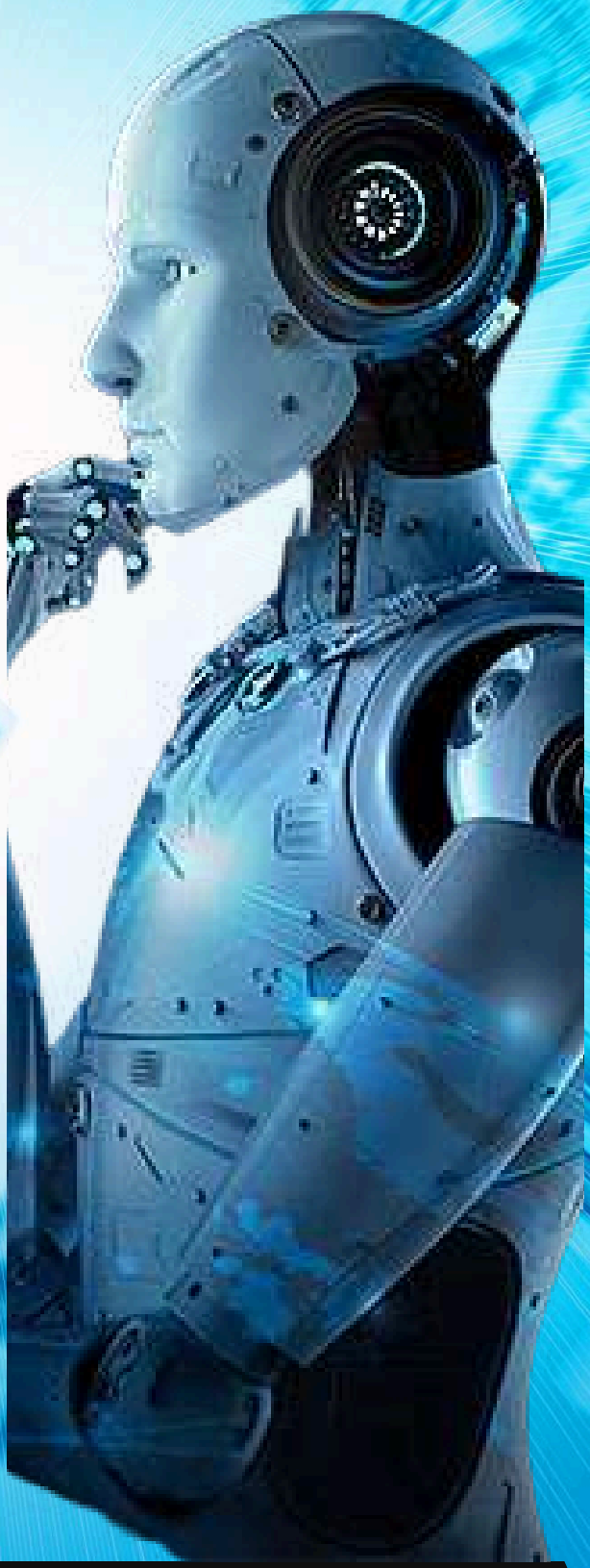


Reporting cybercrime

Based on the number of cyberattacks over the past year, there are an estimated 14.8 attacks against UK Businesses every Minute. Despite this, only 13% of cybercrimes in the UK are reported. A big reason for this is that many organizations don't want to admit they've been hacked because they're worried it'll hurt their reputation or make customers lose trust in them.

Impact of AI

To keep up with the rise in frequent and advanced cyberattacks, we need flexible strategies that can handle new threats as they emerge. One game-changer in this fight is the use of AI in cybersecurity. According to the International Data Corporation (IDC), AI in this space is growing fast - around 25% per year - and could be worth over $45 billion by 2027. Gartner also predicts that by 2025, the increase in AI-powered fraud will push companies to ramp up cybersecurity training and teach employees how to stay more secure online. The catch? AI is a double-edged sword. It helps defenders, but it's also giving cybercriminals new ways to pull off more complex attacks. That's why future spending on threat intelligence, both offensive and defensive, is expected to grow. Staying ahead of attacks means understanding how cybercriminals think and using that insight to stop them before they strike. The best approach to cybersecurity is stopping breaches before they happen. Fixing the damage after a breach is not only expensive but also disruptive. It can lead to downtime, lawsuits, fines, and long-term hits to a company's reputation. Building strong defences is the foundation of a good cybersecurity plan.



Protecting the economy

Future economic threats are increasingly emerging from the overlap of terrorism, political activism, and organized crime, with adversaries teaming up and using advanced technologies to their advantage. To stay ahead of these risks, organizations need strong cybersecurity practices, skilled teams, and solid policies and systems. Proactive measures like threat intelligence help identify and stop attacks early, saving money compared to fixing the damage afterwards.

Ethical hacking is another useful tool for spotting weaknesses before attackers can exploit them. Sharing knowledge is also critical since interconnected systems like IoT and supply chains mean one vulnerability can affect many. Collaboration between organizations and even governments, like the FBI's Silk Road 2.0 takedown, shows the power of working together, and standardized global cybersecurity regulations could further protect shared networks.

Advanced tools like AI and machine learning offer 24/7 monitoring and quick responses to cyberattacks, matching the speed of attackers using similar tech. However, human error, especially through phishing or social engineering, remains a major weak point, so employee training on recognising threats, using strong passwords, and adopting multi-factor authentication is crucial. Businesses should also have plans for disaster recovery and continuity to minimize damage if an attack succeeds. By focusing on prevention, collaboration, and advanced technologies, organisations can reduce both economic and operational risks while staying ahead of evolving cyber threats.

zhero

AI insights

Alan Ntini, one of our amazing Service Desk Engineers, has an inherent interest in AI regulation. He believes this area needs to get much more traction to counter the harmful uses of artificial intelligence. Here's Alan's story.

AI regulation is all about the rules, laws, and guidelines that shape how artificial intelligence is developed, used, and managed. The main goal is to make sure AI is safe, ethical, and beneficial for everyone while minimising the risks and harm it could cause. One big part of this is safety and risk management. AI used in critical areas like healthcare, transportation, or defence has to meet high safety standards to avoid accidents or being misused. These systems often need to go through rigorous testing and certification to ensure they work properly and can handle unexpected situations. Transparency and accountability are just as important. AI systems should be understandable—not just for developers, but for users and regulators too. That means we need clear explanations for how decisions are made, especially when those decisions impact people's rights or freedoms.

Privacy protection is another huge factor. AI works with massive amounts of personal data, and regulations like Europe's GDPR or California's CCPA ensure that this data is used responsibly. It's crucial to prevent AI from violating privacy or creating discrimination based on sensitive information. We also need to ensure fairness and non-discrimination. AI shouldn't be biased or treat people unfairly because of their race, gender, age, or any other characteristic. This is why regulations often include tools to detect bias, regular audits, and clear guidelines for fair use.

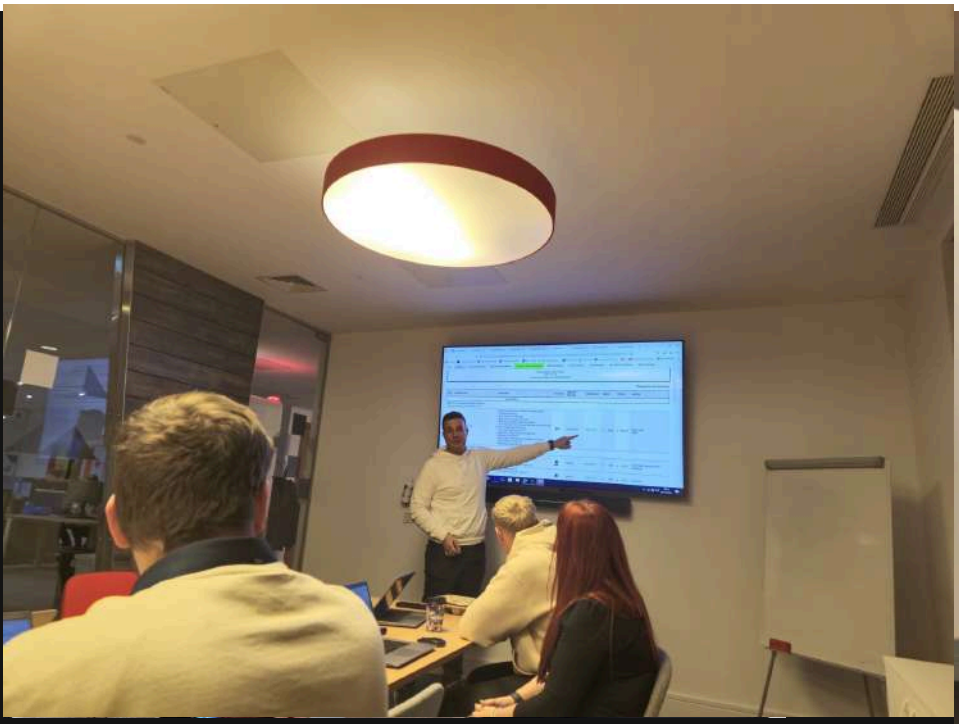
When it comes to ethics, AI has to align with values like human dignity, well-being, and autonomy. There are regulations to control how AI is used in areas like surveillance or military tech to ensure it stays within ethical boundaries. Then there's the issue of intellectual property (IP) and liability. With AI generating things like art, music, or inventions, we need clear rules on who owns the rights to what AI creates. And if an AI system causes harm, we need to figure out who's responsible—whether it's the developers, operators, or someone else.

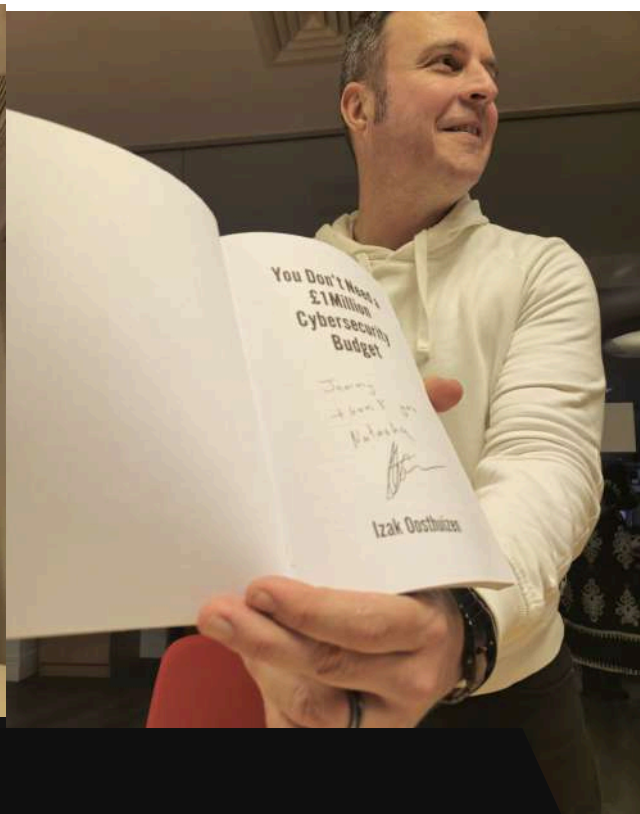
Different parts the world are approaching AI regulation in their own ways. The European Union is leading with its Artificial Intelligence Act, which categorizes AI systems by their risk level and sets rules accordingly. The EU's GDPR also has a big impact on how AI handles personal data. In the United States, there's no nationwide AI law yet, but some initiatives, like the National AI Initiative Act, are shaping policy, while states like California are setting their own rules with laws like the CCPA. Over in China, there's a focus on using AI for economic growth while addressing ethics, transparency, and safety concerns. At the international level, groups like the OECD and the United Nations are working on global standards to encourage collaboration and responsible AI development.

But let's be honest, regulating AI isn't easy. It's a global effort, and every country has different priorities, which makes coordination tricky. Plus, AI technology evolves so quickly that regulations often struggle to keep up. And there's always the challenge of finding the right balance: too many rules might slow innovation, but too few could open the door to unethical or harmful uses. At the end of the day, AI regulation is all about making sure we use this incredible technology responsibly. As AI continues to play a bigger role in our lives, we'll need to adapt the rules to deal with new challenges and opportunities. It's a work in progress, but it's essential for building a future where AI benefits everyone.

N-ABLE™

At the end of last month, Izak and other amazing Zhero A-Team members, Technical Lead Zaheer Rahman, Head of Development Wesley Harris and Louis Oosthuizen, our awesome Developer, headed up to Edinburgh to meet with N-able. Izak showcased integration, internal automation and DevOps, emphasizing collaboration and product development with N-able. Izak also got to share the secrets of his success with his #1 Amazon bestseller.





On 27 November, Zhero and Citygate had their annual Christmas meetup in Covent Garden in London. The evening started at All Bar One and then Izak, Simon and the gang all made their way to Smith & Wollensky, one of the capital's premium steakhouses. An amazing time was had by all, including devouring some of the best steaks known to humans. This happens to be a bone of contention with Marc, one of our Service Desk Engineers, who claims that the world's best beef comes from his grill at home.

To wind things up in preparation for the Festive season, Team Zhero, our clients, friends and family had a Christmas feast at a Central London venue. A big shoutout to everybody who made it happen, especially to the South African crew who, as always, went further than above and beyond.

Merry Christmas

zhero

crush the chaos

CYBER.
LONDON

CRUSH IT CHAOS

Tune in here:

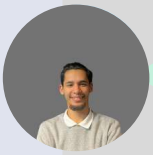
zhero | PODCAST

Meet the team

Ryan O'Connor

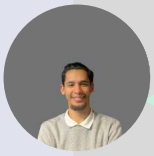
INTERNAL SALES

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



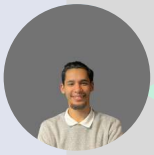
I think it was the ever-evolving nature of technology that drew me in. IT is an industry where change isn't just expected—it's the norm. There's always something new to learn, a fresh challenge to tackle.

What's your most-used productivity tool?



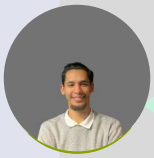
Microsoft 365 is my go-to. Whether it's smashing through emails in Outlook, organizing my life with Teams, or putting together presentations in PowerPoint, it's my Swiss Army knife for work.

How would you describe yourself?



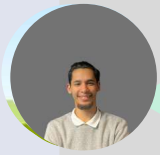
I'd say I'm hardworking and goal-driven, with a side of determination and a sprinkle of curiosity. Once I set my sights on something, I'm all in.

What do you enjoy the most about your role?



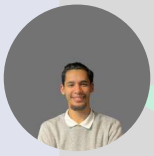
For me, it's all about the people. I love getting to interact with so many different personalities, hearing their perspectives, and figuring out how I can help them.

Do you have any hidden talents or hobbies?



When I'm not deep in IT work, you'll probably find me on a football pitch. I love playing the game—it's a great way to blow off steam, stay active, and channel that competitive spirit!

What is your favourite movie or TV show?



I'm a huge fan of Howl's Moving Castle! There's just something magical about the way Studio Ghibli brings its worlds to life.

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos