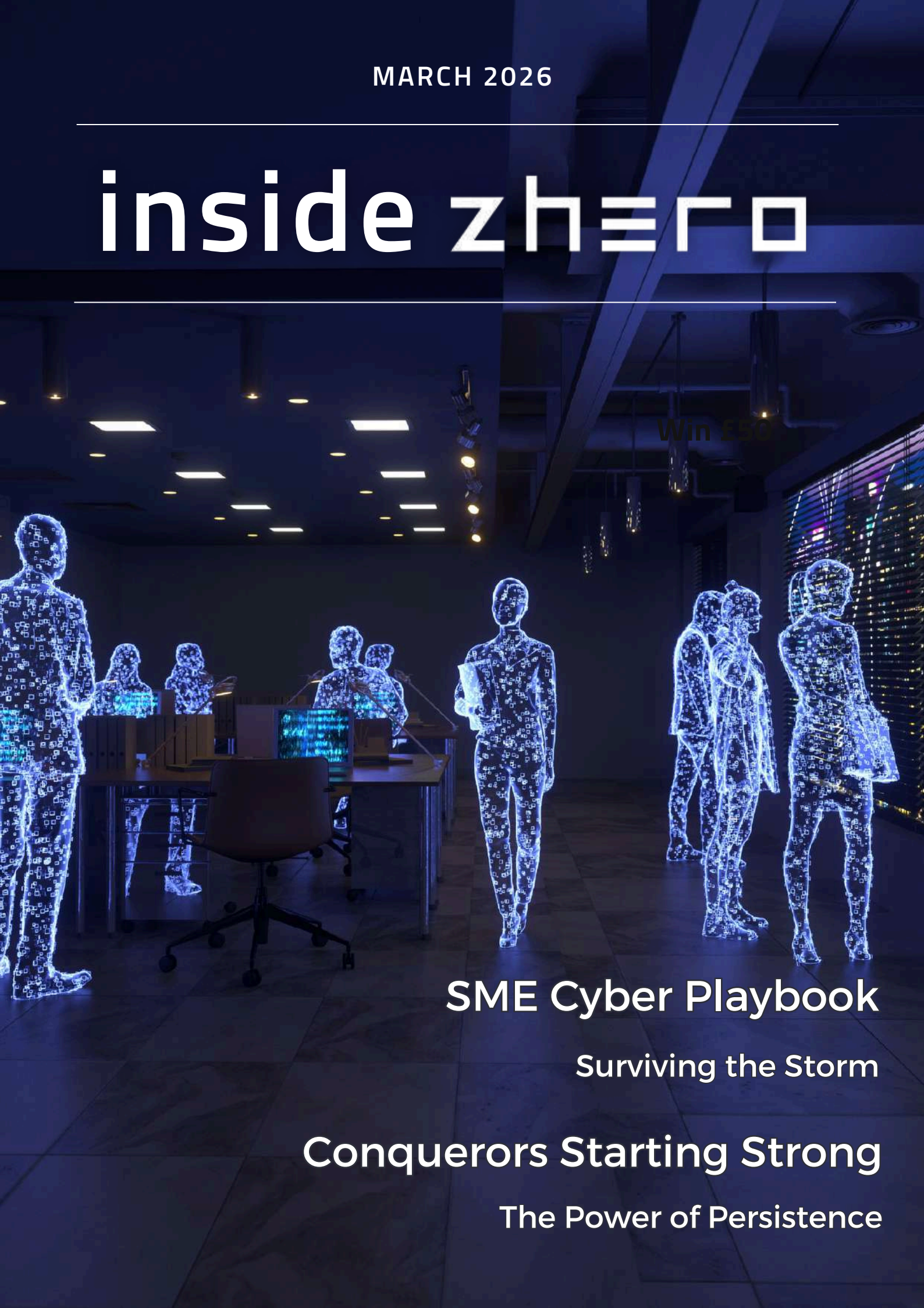
MARCH 2026

inside zhero



SME Cyber Playbook

Surviving the Storm

Conquerors Starting Strong

The Power of Persistence

Message from Izak

Welcome to our Spring edition of Inside Zhero, packed with cyber insights for SMEs.

This month, we dive deep into why cybersecurity is critical for UK SMEs, now more than ever, and how businesses can build their resilience. There are also profound words on persistence from our HR wizz, Liz Mentor.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature “SME Cyber Playbook” details the current cyber threats facing SMEs in the UK and how these can be countered.

60% of UK SMEs reported a cyberattack last year, each costing £20,000 on average.

"SMEs face an increasingly hostile cyber environment. AI-driven attacks, identity theft, and complex ransomware are on the rise every year. Protecting access with MFA, adopting zero-trust approaches, and building staff awareness are essential steps for any business. I have seen firsthand how human and insider vulnerabilities can undo even the strongest technical defences. Investing in cyber resilience, regular monitoring, and tested response plans can make the difference between a minor incident and a business-threatening crisis."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

50% discount **cyberzhero542**

SME CYBER PLAYBOOK

Cybersecurity has become one of the most critical business issues for UK SMEs, with 60% of small businesses reporting that they experienced a cyberattack in the past year, and ransomware incidents increasing by 40%. AI-powered threats are rapidly changing the cyber landscape. Cybercriminals are now using AI to create highly personalised phishing campaigns that can bypass traditional security measures. Identity is now considered the main perimeter for security. Compromised credentials and stolen single sign-on access are among the most common entry points for breaches. This makes Multi-Factor Authentication (MFA), passkeys, and zero-trust approaches essential for all organisations, including SMEs. Beyond external attacks, insider threats are rising, whether from intentional data leaks or unintentional errors, and supply chain or third-party vulnerabilities continue to expose businesses to risk. Ransomware and extortion schemes are also evolving. Given this rapidly changing environment, UK SMEs must focus on cyber awareness, behavioural training, robust access controls, and overall cyber resilience to protect sensitive data, maintain customer trust, and ensure business continuity.

Silent AI Wars

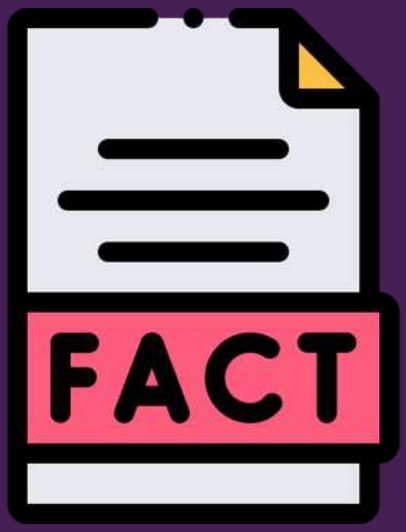
Cybersecurity has become a high-stakes battlefield where AI is changing the rules. Criminals are using AI to launch razor-sharp phishing campaigns, automated ransomware, voice cloning, and deepfake scams that can bypass traditional security measures. Recent studies show that 78% of cyberattacks now involve some form of AI, making attacks faster, more sophisticated, and far harder to detect. The financial impact is significant, with the average UK SME losing over £20,000 per incident, and ransomware attacks alone now account for 30% of these costs. On the defensive side, organisations are turning to AI and machine learning to detect unusual activity, automate responses, and respond more effectively than manual teams ever could. With over 60% of UK small businesses reporting a cyberattack in the past year, the threat is both widespread and escalating. For SMEs, investing in AI-powered security tools, staff training, and resilient systems is essential. Understanding and preparing for this new digital reality can make the difference between continuing operations smoothly and facing costly, disruptive attacks.

Identity Frontier

The traditional idea that a network perimeter alone protects a business is outdated. For UK SMEs, identity is now the perimeter, and the weakest link often lies in compromised credentials and stolen access. Reports show credential theft causes over 80% of successful breaches, making it a common and damaging entry point for attackers. Single sign-on accounts, poorly managed passwords, and excessive user privileges leave businesses exposed. Zero-trust security models are essential for SMEs. These approaches never trust access automatically, always verify identity, and apply least-privilege principles. Multi-Factor Authentication, passkeys, and strict access controls are critical to prevent unauthorised entry. As attacks become more targeted, investing in identity-focused security measures is no longer optional. SMEs prioritising identity management can reduce breach risk, protect customer trust, and maintain operational continuity in a digital landscape.

Human Weakness

Cyberattacks are no longer just about breaking through firewalls. For UK SMEs, the human element has become the most exploited weakness. 90% of successful cyberattacks involve some form of social engineering, making it the most common tactic for gaining unauthorised access. Employees are often tricked into giving away credentials, approving fraudulent payments, or clicking on malicious links, creating a direct pathway for attackers. Deepfake technology is now being weaponised to impersonate executives on calls and video conferences, with one study finding that 35% of UK businesses reported attempted scams using synthetic audio or video in 2025. AI-enhanced phishing emails are also on the rise, and these attacks mimic genuine communications so convincingly that even trained employees can be deceived. Awareness and behavioural defences are as critical as technical controls. UK SMEs that implement regular phishing simulations, staff training, and strict verification protocols can cut their risk of social engineering attacks by up to 70%, safeguarding sensitive data, customer trust, and operational continuity.



- 95% of breaches involve human error
- 60% of SMEs fold within 6 months of a cyberattack
- 50% of passwords are reused across accounts
- 75% of employees admit to ignoring security policies
- 70% of malware infections are triggered by human action

Ransom Trap

Cyberattacks Ransomware has become one of the most destructive cyber threats UK SMEs can face. Criminals are weaponising Ransomware-as-a-Service (RaaS) to launch high-impact attacks with shocking speed, letting even inexperienced hackers cripple businesses and demand huge payouts. In recent years, attackers have advanced to double and triple extortion tactics, encrypting data, stealing sensitive information, and threatening to leak it publicly or pressure partners and customers for more leverage. Surveys now show that 65% of UK small businesses see cyberattacks as a bigger risk than inflation or recession. In one stark example in 2025, the Akira ransomware gang hit KNP Logistics, a 158-year-old Northamptonshire transport firm, after guessing a simple password. Attackers encrypted critical systems and demanded an estimated £5 million ransom. The company was unable to recover and was forced into administration, leaving around 700 employees out of work. For UK SMEs, relying on technology alone is no longer enough. Businesses that build strong backup strategies, test incident response plans regularly, and rehearse rapid recovery can cut downtime and financial losses dramatically. Awareness, preparation, and proactive resilience are now essential to survive and recover from ransomware attacks.

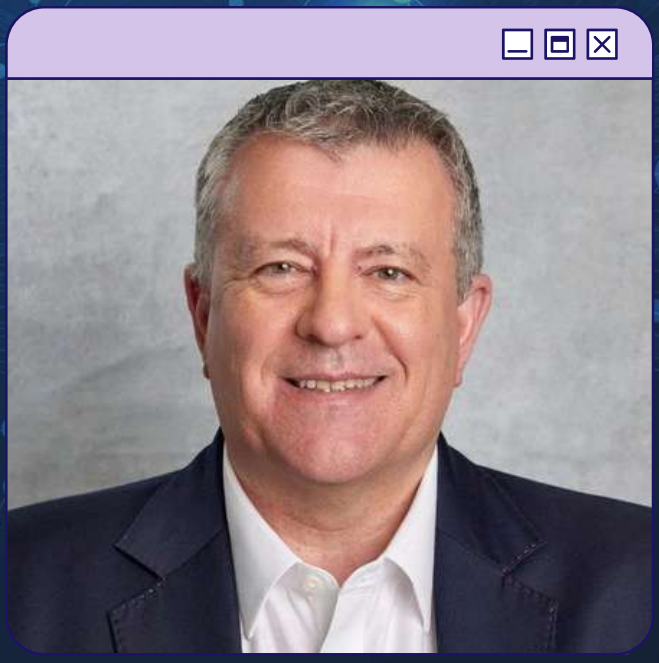
Hidden Backdoors

For UK SMEs, reliance on cloud systems, SaaS platforms, and digital supply chains has grown rapidly, but this convenience comes with hidden risks. Misconfigured cloud systems, unsecured APIs, and vulnerable third-party software can all provide attackers with a backdoor into critical business systems. Research shows that 27% of UK small businesses have been affected by a supply chain attack in the past year, often without realising the source until it is too late. One high-profile example involved a UK-based technology provider whose accounting software was compromised through a third-party plugin. Attackers were able to access client data across multiple SMEs, causing significant financial and reputational damage. The incident demonstrated how weaknesses in one partner can ripple through an entire network of businesses. For SMEs, securing cloud platforms, vetting third-party providers, and monitoring supply chain activity are essential. Implementing strict access controls, regular audits, and continuous risk assessments can dramatically reduce exposure to these indirect attacks and protect both data and business continuity.

Prevention vs. Resilience

Preventing every cyberattack is no longer a realistic goal. Threats are evolving too quickly, and even the most secure systems can be compromised. The focus is now shifting toward cyber resilience, the ability to detect, respond to, and recover from attacks rapidly. Research indicates that SMEs with tested incident response and recovery plans reduce downtime by up to 60% compared to those without, highlighting the tangible benefits of planning ahead. A real example comes from a mid-sized London-based marketing firm that suffered a ransomware attack in 2025. Thanks to regular backups and a rehearsed recovery plan, the company restored its systems within 24 hours, avoided major financial losses, and maintained client trust. For UK SMEs, investing in rapid detection, automated response systems, frequent backups, and recovery planning is essential. Building cyber resilience allows businesses to withstand attacks, minimise disruption, and maintain continuity even when threats succeed.

"SMEs are the backbone of our economy, yet they are losing a staggering £3.4 billion annually due to inadequate cybersecurity. Investing in robust cybersecurity is no longer optional — it is a business imperative."



Nick Gliddon
CEO Vodafone Business UK

The Cyber Crossroads

For UK small businesses, the stakes have never been higher. Limited IT teams and tight budgets make smaller businesses particularly vulnerable, yet cyber threats are scaling rapidly, amplified by automation and AI on the attacker side. Recent industry surveys reveal that many SMEs now rank cyberattacks as their top business risk, surpassing even inflation and recession concerns. Cybersecurity is no longer just a technical concern; it is the backbone of business survival. To stay protected, SMEs should focus on the most effective measures. Multi-Factor Authentication and strong identity controls safeguard access. Employee security awareness training reduces the risk of social engineering and insider threats. Regular patching, backups, and tested incident response plans ensure resilience when attacks occur. AI-enhanced security tools can detect anomalies and automate defences, while robust controls for cloud systems and third-party access close potential backdoors. By prioritising these areas, SMEs can reduce risk, protect sensitive data, maintain customer trust, and ensure operational continuity in an increasingly hostile digital landscape. Cybersecurity is now a strategic priority that can determine the success and survival of a business.

CONQUERORS Starting Strong

Our amazing HR Manager, Elizabeth-Anne Mentor, tells us how Zhero's 2026 values focus on persistence, excellence, leadership, innovation, and humility, encouraging daily growth, teamwork, problem-solving, and celebrating every contribution toward success. This month we look at persistence.

The Power of Persistence

At Zhero, we've kicked off the year with one mindset: never ever give up. Being a Conqueror isn't just about crossing the finish line. It's about the grit, resilience, and determination we show along the way. It's about how we tackle challenges, adapt when obstacles pop up, and keep moving forward, even when the path gets tough.

Think back to the last time a problem seemed impossible. Maybe it was a tricky client issue, a tight deadline, or a project that just wouldn't go your way. How did you respond? Did you push through, find a solution, or reach out for support? That's what being a Conqueror is all about. Every challenge is an opportunity to grow smarter, stronger, and more capable.

"It does not matter how slowly you go as long as you do not stop."

~ Confucius

Persistence shows up in the little things that make a big difference. It's making that extra call to a client who needs reassurance, carefully troubleshooting a tricky ticket, or going the extra mile for a teammate. These actions build trust, sharpen our skills, and prove that we're problem-solvers who never quit.

Starting strong means embracing challenges head-on and asking yourself: What obstacles can I tackle this week? Where can I push a little harder, even when it feels tough? And how can I support a teammate while navigating my own challenges? Every "no" we overcome, every roadblock we conquer, is a step toward personal growth and team success. Persistence is about showing up, staying committed, and proving, to ourselves and each other, that we can rise above difficulties.

Let's make this quarter one of resilience, victories, and breakthroughs, both big and small. Celebrate your wins, learn from setbacks. Together, we are Conquerors. Every day is a chance to prove it.

TAKE ACTION

Share a moment this month when you persisted against the odds, whether with a client, a project, or a colleague, by emailing HR@zhero.co.uk. Let's celebrate every win and inspire each other to keep conquering.

"Continuous effort, not strength or intelligence, is the key to unlocking our potential."

~ Winston Churchill

Meet the team

Melissa Musekiwa

INTERNAL SALES

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

Hi! My love for mathematics and problem-solving. Achieving A grades in major maths exams inspired me to pursue a career in technology.

What's your most-used productivity tool?

Copilot – it helps me refine emails, speed up research, and organise information efficiently.

How would you describe yourself?

Curious and growth-oriented, always eager to learn and improve both professionally and personally.

What do you enjoy the most about your role?

I enjoy the opportunity to work with new technology and the satisfaction that comes from solving problems.

Do you have any hidden talents or hobbies?

I enjoy cooking. It's my therapy, and I love experimenting with different cuisines.

What is your favourite movie or TV show?

The Blacklist – I enjoy the mystery, strategy, and problem-solving in the storyline.

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