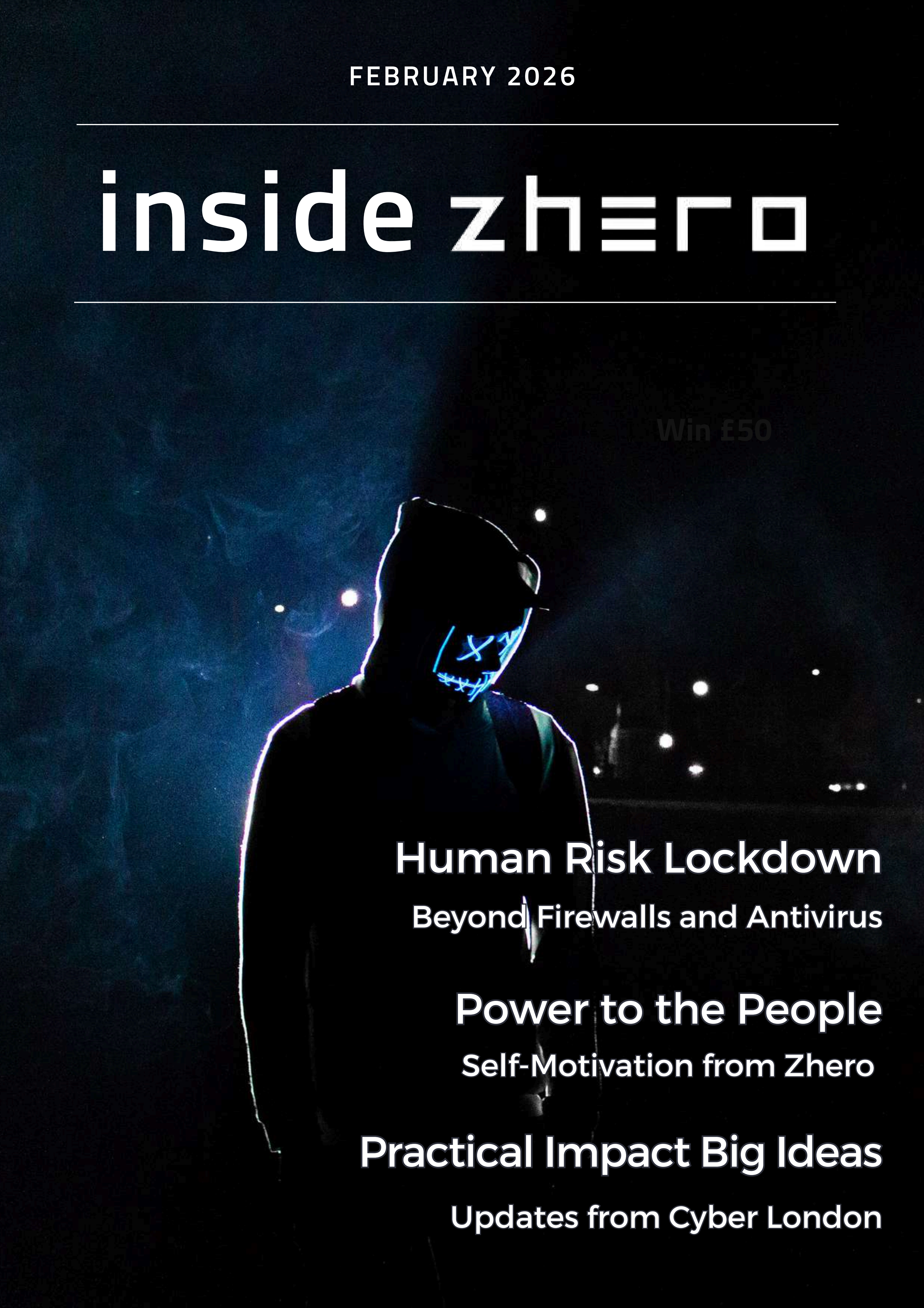
FEBRUARY 2026

inside zhero



Win £50

Human Risk Lockdown

Beyond Firewalls and Antivirus

Power to the People

Self-Motivation from Zhero

Practical Impact Big Ideas

Updates from Cyber London

Message from Izak

Welcome to our latest exciting edition of Inside Zhero, crammed with amazing news.

This month, we take a look at an often overlooked aspect of cybersecurity, human risk. There are also some encouraging words for our HR specialist, Liz Mentor, and updates on Cyber London from Lucindi.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature “Human Risk Lockdown” highlights the need for mitigation of human risk in cybersecurity.

92% of breaches involve a human factor, such as phishing or credential misuse.

“Cybersecurity isn’t just about firewalls or endpoints. Phishing, social engineering, and simple mistakes are often the easiest ways for attackers to get in. By focusing on identifying high-risk behaviours through simulations and embedding security awareness into daily workflows, we can reduce human error, protect critical data, and build confidence in our ability to strengthen cyber defences. The goal is to stop breaches before they happen by addressing behaviour, not just technology.”

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

50% discount **cyberzhero542**

HUMAN RISK LOCKDOWN

In cybersecurity, risk is fundamentally about the impact and probability of events, as defined by Douglas W. Hubbard and Richard Seiersen in How to Measure Anything in Cybersecurity Risk. They describe risk as a set of possibilities with quantified probabilities and losses, which provides a practical foundation for how organisations should understand and mitigate cyber risk. Yet many security strategies still focus heavily on protecting the perimeter through network, content, and asset controls, addressing only part of the challenge. People remain a decisive factor in how systems and data are actually used, which is why over 80% of cyber incidents globally involve a human element, and in the UK, almost 50% of businesses reported a cyber breach or attack in the past year. Even approaches such as Zero Trust Network Access are often applied uniformly, overlooking behavioural patterns, user context, and working environments across different teams. The result is a gap between technical protection and real business risk, one that can only be closed by treating human risk as a core part of cybersecurity strategy rather than an afterthought.

Humans First Systems Second

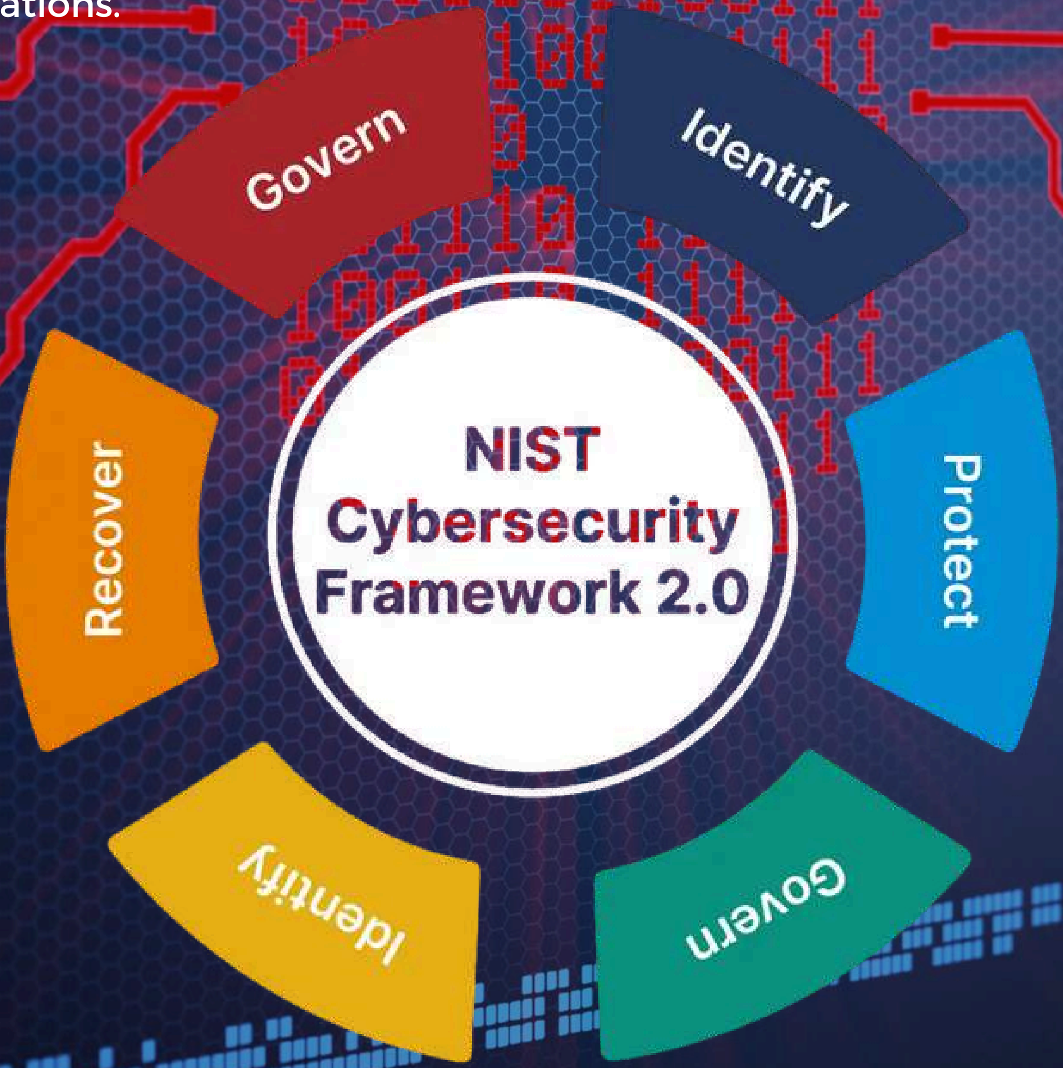
Human risk has long been one of the trickiest challenges in cybersecurity, especially for UK SMEs. Organisations often rely on awareness programmes, annual training, and simulations to tackle it, and these approaches can reduce careless handling of sensitive information, particularly in sectors like healthcare and intellectual property. Yet the reality is stark: a single successful breach by a malicious actor can inflict serious damage, highlighting that training and awareness alone are not always enough. Evidence shows that simulations can improve behaviours against threats such as phishing, but their impact tends to plateau after a dozen or so sessions. For compliance, mandatory cybersecurity training remains essential for meeting regulatory standards and securing relevant certifications. Meanwhile, tools like SIEM, UEBA, and SOAR are invaluable for incident response, but they rarely cover the “identify” and “protect” phases fully, as defined by the NIST cybersecurity framework, leaving SMEs exposed to persistent human risk.

Bridging Human Risk

This highlights the need for a more holistic approach to human risk management, moving beyond traditional training and simulations. Truly effective cybersecurity requires a deeper understanding of human behaviour and the context in which people operate. There is a clear gap in most security strategies: while tools like SIEM, UEBA, and SOAR provide valuable data, they focus largely on malicious activity and often overlook unintentional human errors. The most effective human risk-oriented solutions go further, offering actionable insights that help predict and pre-empt threats before they materialise. Although the human factor is acknowledged in many organisational security plans, it often remains siloed from real-world threat scenarios, a situation worsened when employee behaviour and context are absent from perimeter policies. Integrating these human elements is essential to creating a complete, proactive human risk management strategy that genuinely protects people and business alike.

NIST

While NIST (National Institute of Standards and Technology) standards are not legally mandatory in the UK, they are widely recognised as a voluntary "gold-standard" framework for cybersecurity, particularly in defence, critical infrastructure, and international business. Many UK organisations adopt the NIST Cybersecurity Framework (CSF) to guide risk management, annual reviews, and incident response planning, using it to complement UK-specific standards such as Cyber Essentials, DEFSTAN 05-138, or ISO 27001. Although NIST originates from a US government agency and is only legally binding for companies working with US government bodies, its principles are highly regarded for international compliance, including alignment with the EU NIS 2 Directive. Voluntary adoption of NIST helps UK organisations enhance their security posture, provide structured governance, and build trust with global partners. By mapping UK regulations against NIST's framework, businesses can achieve a comprehensive approach to cybersecurity that meets both domestic and international best-practice expectations.



Complexity of Human Risk

Human risk requires a clear understanding of key concepts such as vulnerability, threat, risk, and risk outcome. Vulnerabilities are weaknesses that can be exploited, from poor password practices to inadequate incident reporting, while threats can be intentional, like cyberattacks, or unintentional, such as employees mishandling sensitive data. Risk reflects the potential damage when threats exploit vulnerabilities, considering the context of both the individual and the organisation. Human Risk Management (HRM) involves identifying, prioritising, and mitigating these risks, spanning individual behaviours to role-specific responsibilities across departments. Organisations must also consider specific risk outcomes they aim to prevent, such as data theft or privacy breaches, and recognise that organisational factors like culture, sector, and regional context shape overall risk profiles.

Mitigating human cyber risk relies on fostering a robust security culture, where leadership commitment, effective communication, and recognition of positive behaviours reinforce safe practices. HRM goes beyond awareness and training, using data-driven insights, automation, and scientific methodologies to quantify and manage risk effectively. By measuring the probability and impact of potential outcomes, organisations can prioritise interventions and reduce exposure, creating a resilient cybersecurity strategy that accounts for both human and organisational factors.

FACT

- Security training cuts phishing risk by 86%
- Trained organisations are 8× less likely to breach
- Awareness programmes reduce overall risk by 70%
- Phishing susceptibility falls 40% in 90 days
- 90% of employees say training boosts security engagement

"Amateurs hack systems, professionals hack people."

Behaviour Breeds Vulnerability

Human behaviour is at the heart of many cybersecurity incidents, driving phishing attacks, social engineering, and insider threats. Phishing tricks employees into revealing sensitive information or clicking malicious links, while social engineering manipulates individuals into actions that compromise security, such as sharing passwords or granting unauthorised access. Insider threats—whether deliberate or accidental—often arise from poor training, weak security practices, or personal motivations. Globally, 48% of SMEs experienced a cybersecurity incident in the past year. 25% say they have experienced more than one incident in the past year. For UK SMEs, the stakes are high: a single successful attack can result in significant financial loss, reputational damage, regulatory penalties, or operational disruption, potentially threatening business survival. Understanding these behaviours and their root causes is therefore critical. By identifying risk patterns and addressing human factors proactively, SMEs can strengthen their defences, reduce the likelihood of incidents, and build a resilient cybersecurity culture that protects both people and business.

“Cybersecurity is more than protecting your devices. It’s about protecting yourself.”

Managing Cyber Risk

Human cyber risk represents a major challenge for organisations, with the potential to cause data breaches, financial losses, and reputational harm. Measuring this risk requires identifying factors such as phishing, social engineering, and insider threats, and applying risk scoring to prioritise the most critical vulnerabilities. Effective human risk management relies on strategies like security awareness training and robust incident response plans. By implementing these measures, organisations can reduce human-related threats, strengthen their defences, and enhance their overall cybersecurity resilience.

Role of Integrations

Monitoring and analysing user-focused cyber risks is essential for identifying risky behaviours and potential threats. Platforms such as Google Workspace, SIEM systems, and endpoint security solutions help organisations understand user activities, enabling better decision-making around cybersecurity measures. With more data collected and trends observed, organisations are increasingly able to predict and prevent employee-caused security incidents before they occur.

- Users can receive real-time training nudges via Slack, MS Teams, or email the moment they exhibit risky behaviour, such as violating a DLP policy or visiting a malicious website. Training is now delivered in context, in real-time, making it more effective at changing behaviour rather than simply checking compliance boxes.
- There is a clear correlation between the volume of real-time nudges and a reduction in security alerts to the SOC over time. Fewer employee mistakes lead to fewer alerts requiring triage, demonstrating the impact of behaviour-focused interventions.
- Third: Aggregated data provides actionable insights for security teams. By understanding the full scope of user-generated alerts and which behaviours respond best to training, organisations can prioritise investments in controls, tighten configurations, and identify remaining security gaps.

Humans Drive Security

The journey of understanding and managing human risk in cybersecurity highlights the complex and multifaceted nature of this challenge. Effective Human Risk Management (HRM) requires recognising and adapting to human behaviour within the cybersecurity context. It is not enough to deploy advanced technologies; organisations must integrate these tools with a deep understanding of human factors, their behaviours, contexts, and the unique risks they present. To truly protect against the wide range of digital threats, organisations need a holistic approach to risk management. This goes beyond traditional training and preventive measures, focusing on a nuanced understanding of the human element in cybersecurity. For UK SMEs, this means:

- Reduces the likelihood of costly data breaches and operational disruptions.
- Strengthens overall security posture by addressing human behaviour, not just technology.
- Enables prioritisation of risk mitigation efforts based on actionable insights.
- Supports compliance with standards such as Cyber Essentials and ISO 27001.
- Builds a culture of security awareness, improving employee engagement and resilience.

“Cybersecurity is like brakes on a car. It’s not there to stop you, it’s there to give you control and confidence to move forward safely.”

zhero Cyber Challenge

1 - **Phishing Test**

You receive an email from "IT Support" asking you to reset your password urgently. The email address looks almost correct but has one extra letter. What do you do?

- A - Click the link and reset your password
- B - Verify the sender with IT or check via official channels
- C - Reply asking why they need it

2 - **Social Engineering Trap**

A new contractor calls claiming they need access to client files "for auditing," but you haven't seen their request in writing.

- A - Give access for speed
- B - Verify through your manager or official request channels
- C - Forward unrelated files instead

3 - **Device Security Check**

You step away from your laptop for a quick break. Which is safest?

- A - Leave it unlocked; you'll only be gone a minute
- B - Lock it before leaving
- C - Ask a colleague to keep an eye on it

4 - **Insider Risk Scenario**

A colleague accidentally emails sensitive client data to the wrong recipient. What's the best next step?

- A - Ignore it; mistakes happen
- B - Immediately report the incident to IT/security
- C - Ask the recipient to delete it quietly

5 - **Remote Working Risk**

You need to join a client meeting while at a café. What is safest?

- A - Use public Wi-Fi directly on your laptop
- B - Connect through the company VPN
- C - Use your phone hotspot without security checks

✅ How Did Your Do?

- 5 correct - Cyber Hero 🏆 You're alert and ready.
- 3–4 correct - Cyber Aware ⚡ Good, but watch out for tricky attacks.
- 0–2 correct - Cyber Dunce 🔐 Refresh your cyber knowledge!

@ **info@zhero.co.uk for the answers**

Power to the People

Our incredible HR Lead, Elizabeth-Anne Mentor, reminds us that people aren't just part of the strategy, they are the strategy. Her inspiring words highlight how our teams' energy, ideas, and commitment drive real business impact every day.

Every plan, goal, or strategy only comes to life because of the people behind it. It's your energy, ideas, and commitment that turn good intentions into real progress. Without that effort, even the best-laid plans stay on paper. When we feel engaged and connected to what we do, our impact grows. Taking pride in your work, looking for better ways of doing things, and supporting one another doesn't just make the day more satisfying. It drives results for the team and the business. Every small action adds up.

That's why investing in ourselves and each other matters so much. Learning new skills, looking after our wellbeing, and building trust create the kind of environment where everyone can thrive. When we feel supported, we're more willing to take on challenges, adapt, and contribute ideas that make a difference. Success is something we build together. Leadership provides direction, but it's the day-to-day actions of every individual that keep the organisation moving forward. When we all step up, collaborate, and take ownership, we don't just execute plans, we shape the future of the business.

> ***"Alone, we can do so little, together we can do so much."***
>
> ~ Helen Keller

Practical Impact Big Ideas

Lucindi Storme, Cyber London's Community Manager, provides an overview of what we can expect from the official cyber cluster for London this year.

If you have ever wondered what it looks like when a community decides to make London one of the safest digital cities in the world, the answer is surprisingly glamorous. Think strong coffee, calendars stacked like a game of Tetris, and someone confidently saying, "This will only take five minutes," just before it takes three hours. Welcome to Cyber London's year ahead.

This year, we are doubling down on what we do best: bringing people together, turning complex cybersecurity topics into practical action, and building real momentum across London's cyber ecosystem. Whether you are a founder, practitioner, student, public sector leader, policy thinker, or simply trying to keep up with AI and quantum, there is something here for you. Cyber London exists for one clear reason: to make London safer in the digital world through collaboration, skills development, and real-world initiatives that help organisations genuinely improve their security posture.

Our focus this year is practical, community-led impact. That means webinars, round tables, reports, and hands-on security events designed to share what works, tackle what does not, and turn conversation into action across the ecosystem.

Cybersecurity is a team sport. We are building partnerships that support the community in meaningful ways, with sponsors and partners contributing expertise, insight, and support that go beyond a logo on a slide. If you believe in collaboration over transaction, you will fit right in, whatever sector you work in.

FREEDOM

Congratulations and a big shoutout to Cyber London's amazing co-Founder and Director, and our very own Head of R&D, Prof. Raj Rajarajan, who has been honoured by the City of London Corporation with the Freedom of the City of London, a civic honour for notable achievements in the Square Mile. A truly remarkable accomplishment. Raj says:

> ***"The square mile hosts the majority of the UK's financial institutions and contributes to the wider UK economy. I'm pleased to have received this honour for making a meaningful contribution towards protecting the City of London's digital infrastructures".***

Meet the team

Chris Hannie

ESCALATION ENGINEER

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

Hi! I realised I wanted to go into IT because I enjoy solving problems and working with technology to create practical solutions.

What's your most-used productivity tool?

My most used productivity tool is Visual Studio Code because it allows me to code efficiently and test commands in one place.

How would you describe yourself?

I would describe myself as motivated, adaptable, and detail-oriented.

What do you enjoy the most about your role?

I enjoy solving technical challenges and making processes more efficient for others.

Do you have any hidden talents or hobbies?

In my spare time, I enjoy training on the athletics track and supporting my two boys in their activities.

What is your favourite movie or TV show?

My favourite movie is Iron Man because it showcases innovation, problem-solving, and the power of technology.

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