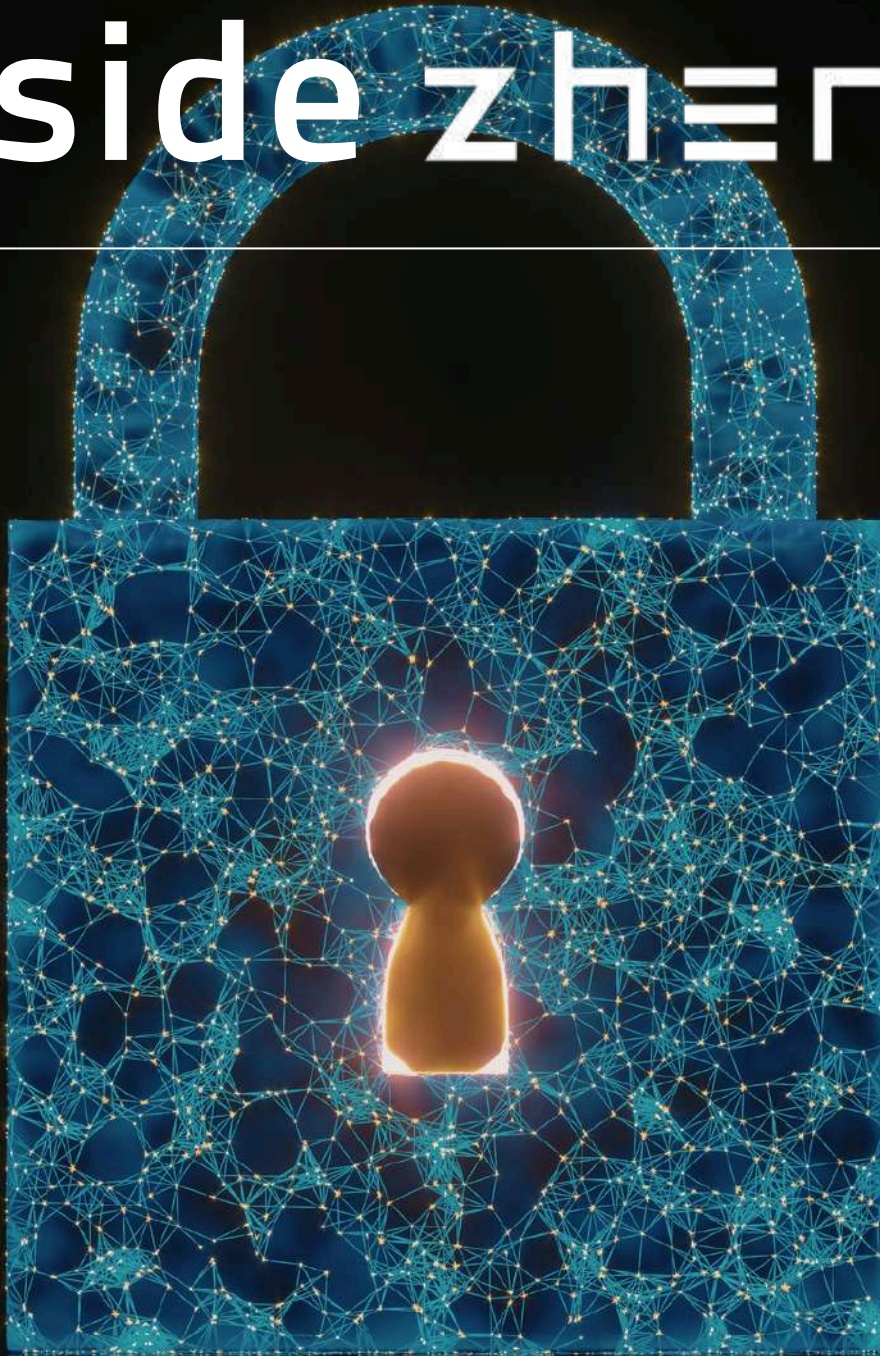


APRIL 2026

inside zhero



ISO 27001 Certified

Zhero's Data Security Milestone

Stay Safe in Teams

Secure Workplace Collaboration



Message from Izak

Welcome to our April edition of Inside Zhero, where we look at our ISO 27001 certification achievement and more.

We also explore our phishing simulation platform, enabling our clients to strengthen their security culture, reduce human-driven risk, and stay compliant without adding operational complexity.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author



In this issue

Our feature “ISO 27001 Milestone” explores the ins and outs of ISO 27001, and its benefits for both Zhero as a company and our amazing client base.

Less than 10% of UK MSPs have ISO 27001 certification.



"I'm incredibly proud that we've achieved ISO 27001 certification. For me, this isn't just a badge, it's a commitment etched into how we think, operate, and protect what matters most. It means our clients can trust that their data is handled with resilience and relentless attention to security. In a world where data holds immense value yet faces constant threat, ISO means we're not just keeping pace with risk, we're staying ahead of it."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author



Available Now

Free 30-minute consultation

50% discount [cyberzhero542](#)

ZHERO



ISO 27001 Milestone

We're excited to announce that Zhero has been ISO 27001 certified, making us one of a few UK MSPs holding this premium information security management framework. An enormous shoutout to Team Zhero and also those involved in this rigorous certification process, and in particular, the amazing Lucindi Storme and Louis Oosthuizen.

What is ISO 27001

ISO 27001 certification is the leading international standard for information security management systems (ISMS), providing a risk-based framework to protect data confidentiality, integrity, and availability. It certifies that an organisation has implemented comprehensive and systematic, third-party audited controls to manage security threats effectively.

ISO 27001 Benefits for Zhero

A well-implemented ISO 27001 framework quietly rewrites the organisation in powerful ways, strengthening its overall security posture by ensuring risks are identified, prioritised, and actively managed rather than discovered the hard way. It reduces both the likelihood and impact of breaches through effective controls, continuous monitoring, and structured incident response, leading to fewer surprises and faster recovery. It builds regulatory confidence by supporting alignment with standards such as UK GDPR, helping to ease compliance pressures and minimise the risk of fines. ISO 27001 creates a competitive edge, with certification often acting as a decisive factor in enterprise and public sector tenders, while also improving internal processes through clear policies, cutting through inefficiency. Crucially, it enhances business resilience, preparing organisations to handle disruptions ranging from cyber attacks to human error, and fosters a cultural shift where security becomes embedded in everyday thinking.

"For me personally, ISO is a valuable milestone because it validates the work already being done and shows our ongoing commitment to doing things properly."



Lucindi Storme - Compliance Consultant

Benefits for Clients

For clients, working with an ISO 27001-certified company brings a noticeably higher level of confidence and clarity, with the assurance that their data is handled in line with internationally recognised and audited best practices. It reduces their risk exposure by lowering the likelihood of data being compromised through systems, while also providing transparency and accountability through clearly defined processes for how information is managed, stored, and protected. In the event of an incident, clients benefit from structured and well-tested response procedures, ensuring issues are handled quickly and effectively. This foundation of security means stronger partnerships, giving clients the confidence to integrate systems and share sensitive information, while also supporting their own compliance efforts, including alignment with compliance regulations such as UK GDPR.

"For me, ISO showcases our commitment to aligning our organisational policies across the board with internationally recognised practices to in turn achieve world-class levels of service."

Louis Oosthuizen - SOC Team Leader





Stay Safe in Teams

Microsoft Teams phishing attacks, often called "vishing", meaning voice or chat phishing, use social engineering to trick users into clicking malicious links, opening infected files, or granting remote access. Attackers pose as "IT Support" or trusted colleagues, often using external, spoofed accounts to deliver payloads or steal credentials. Common Attack Techniques include:

- **Fake IT Support Chat** - Attackers send a message claiming a "technical issue" to initiate a chat. They may offer to fix it, leading to a request for remote access via tools like Quick Assist.
- **Impersonation** - Attackers create Microsoft 365 accounts that appear as legitimate, familiar names within the organisation.
- **Shared Link/File Phishing** - Users receive messages with malicious links (e.g., SharePoint, SharePoint-styled phishing sites) or shared files containing malware.
- **Fake Meeting Invites** - Invitations to fake Teams meetings that ask for credential authentication to join.

Identifying Attacks

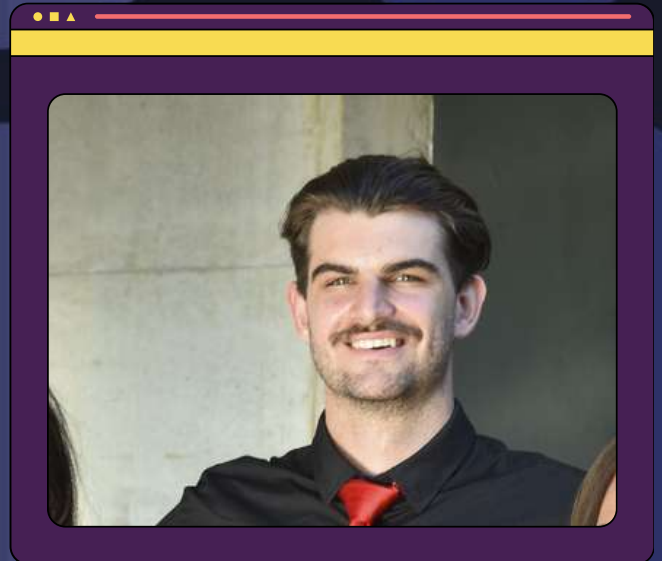
- **Watch for External Labels** - Be suspicious of messages from external users claiming to be from your company.
- **Verify Identity** - Double-check the sender's identity, including their actual email address, before trusting the chat.
- **Never Click/Download Immediately** - Do not click on links or download attachments in unexpected messages, even from known contacts.
- **Use Official Channels** - If "IT" reaches out in Teams, verify the request by calling the helpdesk via their official, internal number.
- **Report Suspicious Activity** - Report phishing attempts to IT immediately, especially if you have already clicked on a link.
- **External Access Settings** - Companies should consider limiting which external domains can send messages to their users in Teams settings.



Phishing Simulation

An estimated 90% of security breaches are caused by us humans, yet many organisations still lack structured programmes to address the human attack surface. Zhero offers security awareness training and phishing simulation to reduce this risk, helping our clients recognise and respond to phishing attempts before they become incidents. It combines practical education with simulated attacks to build real-world cyber awareness across teams. The platform sends realistic, mock phishing emails to test employee responses. It includes plug-and-play kits that mimic real-world threats from brands like Microsoft and LinkedIn.

"Phishing simulations are effective because they safely mimic real-world attacks, helping employees recognise and respond to threats without real risk. They also improve security awareness through targeted training."



Kian Botha - Service Desk Team Lead

Security at Scale

Alongside improving employee vigilance, the platform automates training campaigns and reporting, making ongoing security awareness easier to manage at scale. It also supports cyber insurance requirements and regulatory compliance by demonstrating active risk reduction through continuous training. Our platform is also fully automated, featuring "set-it-and-forget-it" campaign modules that automate training delivery and reporting, providing automated reports on campaign results, showing which employees clicked on links or failed simulations. Zhero helps clients implement and manage phishing simulation programmes, enabling organisations to strengthen their security culture, reduce human-driven risk, and stay compliant without adding operational complexity.

Essential Cyber

Cyber Essentials (CE) is a UK government-backed, industry-supported certification that helps organisations defend against the most common cyber threats. It sets out five key technical controls, including firewalls, secure configuration, access control, malware protection, and regular patching, giving businesses a clear, practical framework to strengthen their security and reduce risk. For UK SMEs, Cyber Essentials is particularly important because it provides an affordable, accessible way to build strong cyber hygiene without needing a large internal security team. It helps protect against the majority of routine attacks, safeguards customer data, and demonstrates a credible commitment to security, which can build trust with clients and partners. It is also often a requirement for working with government bodies and larger enterprises, making it not just a protective measure but a valuable commercial advantage.

CE Key Aspects

- Cyber Essentials is structured across two levels. The standard **Cyber Essentials** certification is based on a self-assessment that is reviewed by an independent assessor. **Cyber Essentials Plus** builds on this by including a hands-on technical verification of systems to ensure the controls are properly in place.
- CE focuses on five key technical controls. These include using firewalls to secure internet connections, applying secure configurations to devices, managing user access to ensure appropriate permissions, deploying malware protection, and keeping all systems up to date through regular patching.
- CE helps protect against the majority of common, low-level cyber attacks, strengthens an organisation's reputation, and can even contribute to lower cyber insurance premiums. It is also a requirement for bidding on certain government contracts.
- Certification is valid for 12 months and must be renewed annually to ensure security measures continue to meet the required standard.



Simon Newman - Cyber London Director

"Cyber Essentials demonstrates that you have achieved a level of compliance against a recognised government scheme around cyber. It shows that you take data and cyber seriously, not just your own but your customers' as well."

Time for Change

On 27 April, CE is being updated to introduce stricter requirements, with a strong focus on cloud security and authentication. Multi-Factor Authentication (MFA) will become mandatory for all cloud services that support it, and failing to enable it will result in automatic non-compliance. All cloud platforms that store or process organisational data will fall within scope, along with tighter rules for patching, access control, and assessment marking. The changes will strengthen baseline security standards and improve consistency across CE assessments.

Teach IT Better

Zhero has a structured journey to Cyber Essentials certification, helping SMEs understand and implement the required security controls with confidence. Through expert training and practical guidance, we make it easier to meet the five key technical requirements and strengthen everyday cyber hygiene. Our approach ensures you are prepared for certification and protected against common cyber threats.



info@zhero.co.uk



zhero.co.uk/certification-training/

Meet the team



Khiara Van Wyk
INTERNAL SALES

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



Hi! I've always been interested in how technology works and solving problems. I realised I enjoy learning new systems and finding solutions, which drew me to IT.



What's your most-used productivity tool?



Microsoft Teams - it keeps collaboration sharp and lets me balance creative direction with internal communication.



How would you describe yourself?



I'm outgoing and a total social butterfly. I love making people laugh, and my humour keeps the energy light. I adapt easily to different situations, which helps me connect with all kinds of people .



What do you enjoy the most about your role?



Seeing ideas come alive - whether it's a campaign, a caption or a client solution - and knowing it makes a real impact.



Do you have any hidden talents or hobbies?



I'm naturally energetic and thrive on staying active - whether it's connecting with people, creating content, or exploring new experiences.



What is your favourite movie or TV show?



Currently I am obsessing over Animal Kingdom, though I will have Heartland playing as soon as a new episode is released.





zhero

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975



START THE PROCESS

zhero
crush the chaos