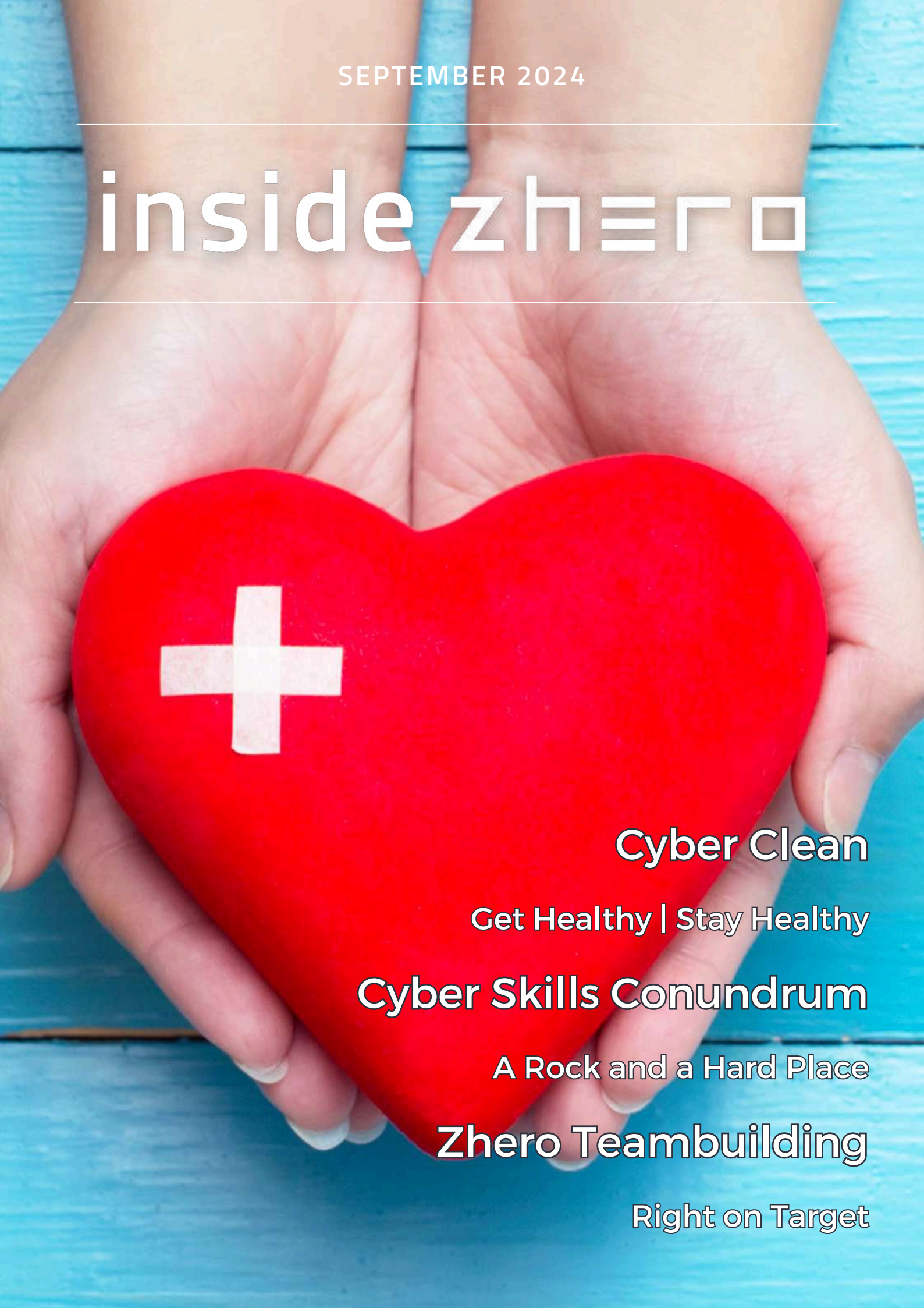
SEPTEMBER 2024

inside zhero



Cyber Clean

Get Healthy | Stay Healthy

Cyber Skills Conundrum

A Rock and a Hard Place

Zhero Teambuilding

Right on Target

Message from Izak

Hello again everybody and welcome to a super cyber edition of Inside Zhero.

This month we're focusing on the importance of cyber hygiene your keeping your devices and data secure. We'll also look at how to address the existing gap in cyber skills.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Cyber Clean" examines the benefits of good cyber hygiene and strategies you can use to put principles into practise.

Only 70% of UK businesses use password policies.

"Your systems must be secured and your people educated on the principles of cyber hygiene. Technology and cyber issues aren't only the responsibility of IT specialists in the background. In today's digital age, these issues are front and centre. "

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consulation

99% discount with code **inside**

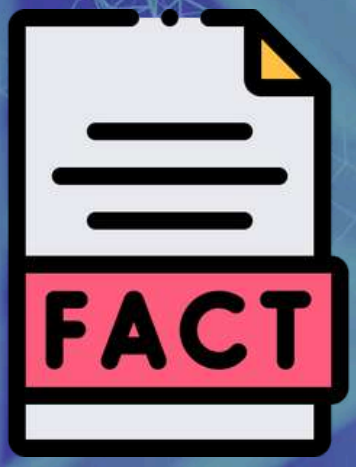
CYBER **CLEAN**

Cyber hygiene is all about the habits and routines that people and organisations use to keep their tech safe and secure. The goal? Protecting your valuable data from cyber threats and attacks. Just like brushing your teeth keeps you healthy, cyber hygiene is all about taking proactive steps to stop problems before they start and keep everything running like a well-oiled machine! In our connected world, good cyber hygiene is a must for protecting data and preventing costly breaches. Implementing these practices builds a strong foundation for long-term cybersecurity success. Poor cyber hygiene can pose serious risks to all types of organisations, as cyber-attacks often lead to the theft or encryption of sensitive data, resulting in significant financial losses.

The core of cyber hygiene

Keeping your systems safe takes a mix of strategies to handle the many cyber threats out there today. Here are the main things you can focus on:

- **Regular Maintenance:** Keep your software and systems updated, apply security patches, and back up your data regularly to avoid identity theft or data loss.
- **Boosting Security:** Good cyber hygiene reduces the chances of data breaches, helping everything run more smoothly and securely.
- **Training & Awareness:** Teach employees about cybersecurity to cut down on mistakes and accidental data leaks.
- **Ongoing Effort:** Cyber hygiene isn't a one-time thing—it's all about consistently monitoring and updating security measures.
- **Teamwork:** Cyber hygiene is everyone's job, not just IT departments.



Risk management

The Cyber Security Breaches Survey 2024 shows us that only 31% of UK businesses did cyber security risk assessments last year. Only 33% use security monitoring tools. Just over one in ten businesses say they review the risks posed by their immediate suppliers.

Benefits of being cyber clean

Cyber hygiene is all about building good habits and practices to protect your digital systems and data. Here's how you can benefit:

- **Better Security:** Strong cyber hygiene means less risk of getting hacked. It helps protect your business's data, client info, and devices from threats like ransomware and malware.
- **Staying Compliant:** Following cyber hygiene best practices keeps your business in line with regulations, helping you avoid fines and penalties while ensuring all the right security measures are in place.
- **Employee Awareness:** By educating your staff on how to spot threats and protect sensitive data, you can greatly reduce the chances of accidental data breaches. Employees play a huge role in keeping everything secure.
- **Saving Money:** Good cyber hygiene can save money by avoiding fines and cutting the need for costly security fixes. It can also keep your operations running smoothly, reducing the need for extra staff or pricey software.
- **Managing Risk:** Regular updates, strong passwords, and training help minimize security risks. Staying on top of cyber hygiene lets you better protect your valuable assets and reduce vulnerabilities.
- **Boosting Reputation:** A business that takes cybersecurity seriously earns more trust from customers and partners, which can lead to better sales and growth opportunities.
- **Increased Productivity:** By preventing cyber-attacks, you can avoid disruptions and security issues, saving time and resources while boosting overall productivity across the business.

Best practices

To keep your tech and data secure, use these essential cyber hygiene practices:

- **Use Strong, Unique Passwords:** Create complex passwords and use different ones for each account to make it tougher for hackers to break in.
- **Enable Multi-Factor Authentication (MFA):** Add an extra security step by using MFA. This usually means providing something extra, like a fingerprint or a one-time code, along with your password.
- **Keep Software and Systems Updated:** Regularly update your software, operating systems, and apps to protect against known vulnerabilities.
- **Back Up Your Data:** Regularly save copies of important data and store them securely. This way, if you face a data loss or ransomware attack, you won't lose everything.
- **Use Antivirus and Antimalware Software:** Install and update antivirus software to catch and remove malicious programs.
- **Watch Out for Phishing Scams:** Be cautious with links and attachments from unknown sources, as they could be attempts to steal your information.
- **Educate Yourself and Your Team:** Provide cybersecurity training to help everyone understand the importance of cyber hygiene and how to protect sensitive information.
- **Encrypt Sensitive Data:** Encrypting your data helps keep it safe both when it's being sent and when it's stored, ensuring only those with the right key can access it.
- **Use Firewalls:** Firewalls act as a barrier between your devices and the internet, blocking unauthorized access and keeping your data secure.

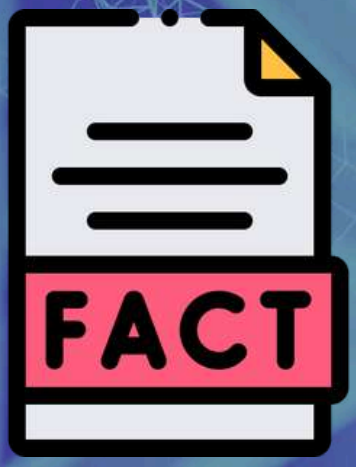
7 steps to hygiene heaven

To keep your tech and data safe, having a solid plan is key. Here's a straightforward checklist to help you stay on top of things:

-
- **Keep Software Updated:** Outdated software is a prime target for cyber-attacks. Make sure all your software, including operating systems and apps, is updated regularly.
- **Train Your Team:** Human mistakes are a big security risk. Regular training helps employees spot and avoid potential cyber-attacks.
- **Use Multi-Factor Authentication (MFA):** MFA adds extra security by requiring something more than just a password to access important systems.
- **Protect Against Phishing:** Phishing attacks are common and dangerous. Make sure you have strong protection against these scams.
- **Segment Your Network:** Break your network into smaller segments to limit the damage if a breach occurs. This helps ensure that a problem in one part doesn't compromise the whole system.
- **Back Up Data Regularly:** Regularly back up important data to protect against data loss from cyber-attacks, hardware failures, or even natural disasters.
- **Conduct Regular Security Audits:** Regularly check your security setup to find and fix any weaknesses before they can be exploited.

Cyber hygiene challenges

Keeping up with cyber hygiene isn't always easy. The world of cyber threats is always changing, so what's considered safe today might not be tomorrow. Organisations need to regularly update their systems, software, and protocols, which can take a lot of time, money, and know-how. One big challenge is the human element. Even with top-notch security systems, people can still make mistakes. Employees might fall for phishing scams or accidentally bypass security measures if they're not well-trained. That's why it's important not just to offer regular training but to build a culture where everyone is mindful of security. Modern IT setups are also often complex, with older systems mixed in with new tech. This can create security gaps that are tough to manage. Dealing with these challenges means taking a well-rounded approach - combining the right technology, ongoing training, and a strong security culture to stay ahead of cyber threats.



Phishing

Phishing is by far the most common type of cybercrime in the UK with a prevalence of 90% compared to all other types of attacks. In the last 12 months, UK businesses have experienced approximately 7.78 million cyber crimes of all types and approximately 116,000 non-phishing cyber crimes.

The mistakes we make

Sometimes it's easy to overlook basic cyber hygiene practices, and that can lead to big problems. Here are some common slip-ups to watch out for:

- **Weak Password Policies:** Don't just use strong, unique passwords. Make sure your organisation has rules for regular password changes and avoids easily guessable info.
- **Outdated Software:** Skipping updates on software and operating systems can leave you open to attacks. Keep everything up-to-date to get the latest security patches.
- **Not Knowing Your Data:** It's important to know where your sensitive data is stored and who has access to it. Use data protection best practices like sensitivity labels and data loss prevention policies.
- **Misconfigured Data Systems:** Make sure your data setups are properly configured to prevent unauthorised access and breaches.
- **Complacency:** Even if you've got solid cyber hygiene, don't get too relaxed. Stay alert and keep up with the latest threats and security practices.
- **Skipping Multi-Factor Authentication (MFA):** MFA adds extra security by needing something more than just a password, like a code sent to your phone.

Good cyber hygiene is crucial in today's connected world. Using top-notch tools and staying proactive helps keep your data safe and sound.

CYBER **SAVVY**

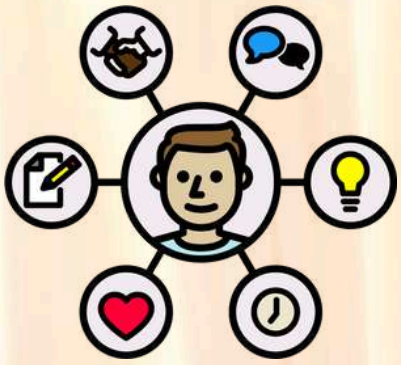
Finding, training, and keeping cybersecurity professionals is crucial to keeping organisations and online communities safe. While the global cybersecurity workforce grew by 12.6% from 2022 to 2023, there's still a huge gap, with a need for about four million more experts worldwide. This shortage is a big deal everywhere, affecting countries and various industries. By 2030, we might see a global shortfall of over 85 million workers. This gap could lead to an eye-watering £6.8 trillion in lost annual revenue—about the same as the GDP of the third-largest economy in the world, right behind the US and China.

Global shortage

The shortage of cyber talent is a big issue not just in Asia-Pacific and North America, but around the world. For example, India, which produces about a third of the world's STEM graduates, had a huge gap in May 2023, with 30% of its 40,000 cybersecurity jobs still open. In Africa, there are only around 20,000 certified security pros for a population of 1.4 billion. This isn't just a problem in developing countries either. In the UK, 43% of small and medium-sized businesses (SMEs) can't find the cybersecurity help they need. Even in the US, which is known for its digital edge, there are still over 500,000 unfilled cybersecurity roles.

Zhero's Head of R&D, Prof Raj Rajarajan says:

"Unfortunately, there is a lack of global standards to unify the skills needed. There is also more digital transformation in traditional sectors like manufacturing, creating a need for new cyber skill sets"



Rock and hard place

In 2023, the National Cyber Security Centre (NCSC) reported a 64% rise in serious cybersecurity incidents in the UK. But despite this increase, the growth in the cyber workforce hit a snag due to a skills gap. So, what's missing? For SMEs, there's a big need for "jack-of-all-trades" types who can juggle various tasks. This gap is getting worse as cyberattacks get more complex. The wider cybersecurity field also struggles with talent shortages across roles like analysis, engineering, and consultancy. It's not for lack of interest—there are plenty of keen candidates—but the problem lies in the supply-demand mismatch. There are few entry-level spots and many mid-level jobs, but not enough qualified people to fill them. A real rock and a hard place story.

"There is high 'burnout' in the cyber security industry which is not attracting sufficient smart people to the sector."

The big five

The cybersecurity skills gap comes down to a few big challenges:

Rising Demand: With tech becoming more complex and essential, the need for cybersecurity pros is growing fast. Securing today's systems and data is tougher, so companies need larger teams with a wide range of skills.

Diversity Issues: Only around 25% of cybersecurity workers are women, and the field is still mostly made up of older white men. Diversity is improving, but it's a slow process.

Unrealistic Job Requirements: Many job ads ask for degrees, tons of certifications, and years of experience, which puts off great candidates who might think they don't meet all the criteria or don't get a call back if they don't tick every box.

Outdated Skills: Tech and threats evolve quickly, but many workers struggle to keep up. Overworked staff often don't have time for training or new certifications, and this includes non-technical skills like communication.

High Turnover: Over a third of cybersecurity professionals are considering changing careers. The field struggles with constant staffing shortages and high pressure, leading to even more people leaving.

"There is not enough time to learn and grow as the threat landscape is changing so fast."

Bridging the gap

To effectively address the cyber skills shortage, we need a global approach that encompasses recruitment, education and training, and most of all, retaining the high flyers. There's no way to bridge the cybersecurity skills gap overnight, but we can start making progress by doing these three things:

- **Reach Out to Underrepresented Groups:** Make an effort to recruit from diverse communities, like women and Hispanic Americans. Show them the variety of roles in cybersecurity and think about offering paid internships to get them on board.
- **Build Skills In-House:** Instead of just hiring experts, focus on training and supporting new hires. You don't always need degrees or years of experience—just a willingness to learn and grow in cybersecurity.
- **Support Your Current Team:** To keep your team happy and avoid burnout. You can automate boring or repetitive tasks to make their workday better. Also, train your IT staff to handle some cybersecurity tasks. Rotate roles to give people a break from stressful positions and help them pick up new skills. Let employees truly disconnect during time off. No work check-ins or being on call - everyone needs a real break!

zhero

on target

Team Zhero had an awesome teambuilding day at Lourensford Wine Estate in Stellenbosch.. As usual it was work hard and play hard.Here are the highlights of clay pigeon shooting, sharing good food and drink, and having fun in the sun.

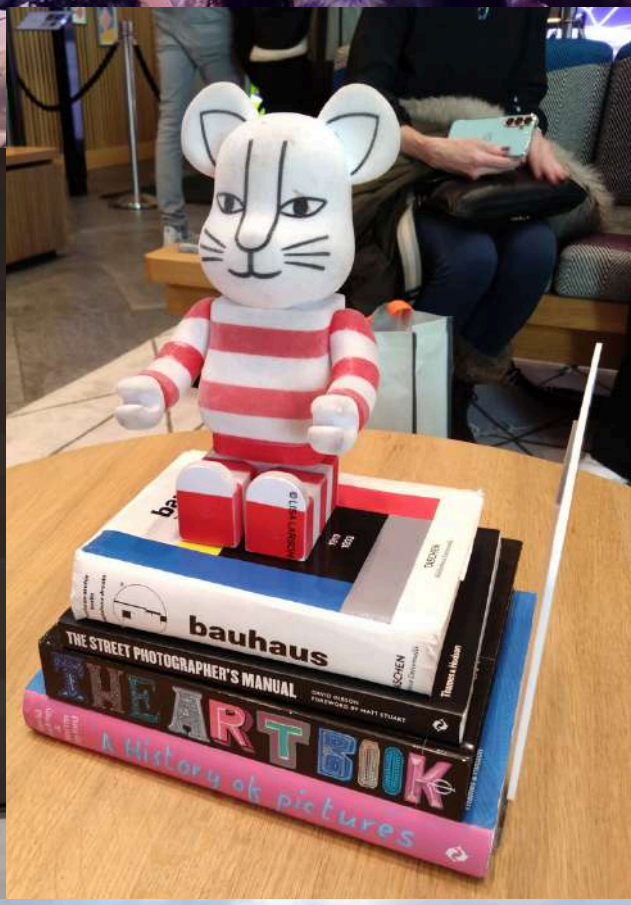
zhero

on target

On Friday, 13 September – lucky for some – Izak was a guest and the primary keynote speaker at the R3CON event "The Future of Tech & Security Liabilities." Held at the awesome Samsung KX at King's Cross in London, the place rocked with over 300 attendees including cyber and tech experts, government representatives, students, and academia. Izak was last up on stage – but not least! His presentation of the current state of play of cybersecurity in UK SMEs proved to be an eye-opener for many. Zhero also had the opportunity to launch its mentorship programme for budding cyber enthusiasts. Overall, a great evening and a great summit. We can't wait for the next one!

zhero
crush the chaos
CYBER
FUTURE CHALLENGES
IoT
AI
SaaS
Lack of awareness
No clear standards
zhero zhero zhero

SAMSUNG


bauhaus
THE STREET PHOTOGRAPHER'S MANUAL
THE ART BOOK
A History of pictures

SAMSUNG

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Zak Ahmed

APPRENTICE ONSITE ENGINEER

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

What drove me to get into the IT industry is the fact that IT is what drives the world in all aspects. There is no cap in how far IT can go and i want to be apart of the force that is the IT industry.

What's your most-used productivity tool?

MS Teams because it's the best and easiest way to reach out to all my team members.

How would you describe yourself?

I would say i am a humble, friendly and eager to learn type of person. Someone who is happy to help in anyway i can.

What do you enjoy the most about your role?

I love and enjoy being able to go to meet different types of clients and resolving their IT issues they may have. I love being able to make their day better by resolving their problems!

Do you have any hidden talents or hobbies?

My hobbies are spending time with friends, listening to music, watching football - Arsenal all the way!

What is your favourite movie or TV show?

My favourite TV show is Game of Thrones. Nothing and i mean NOTHING! comes close to this masterpiece!

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

START THE PROCESS

zhero
crush the chaos