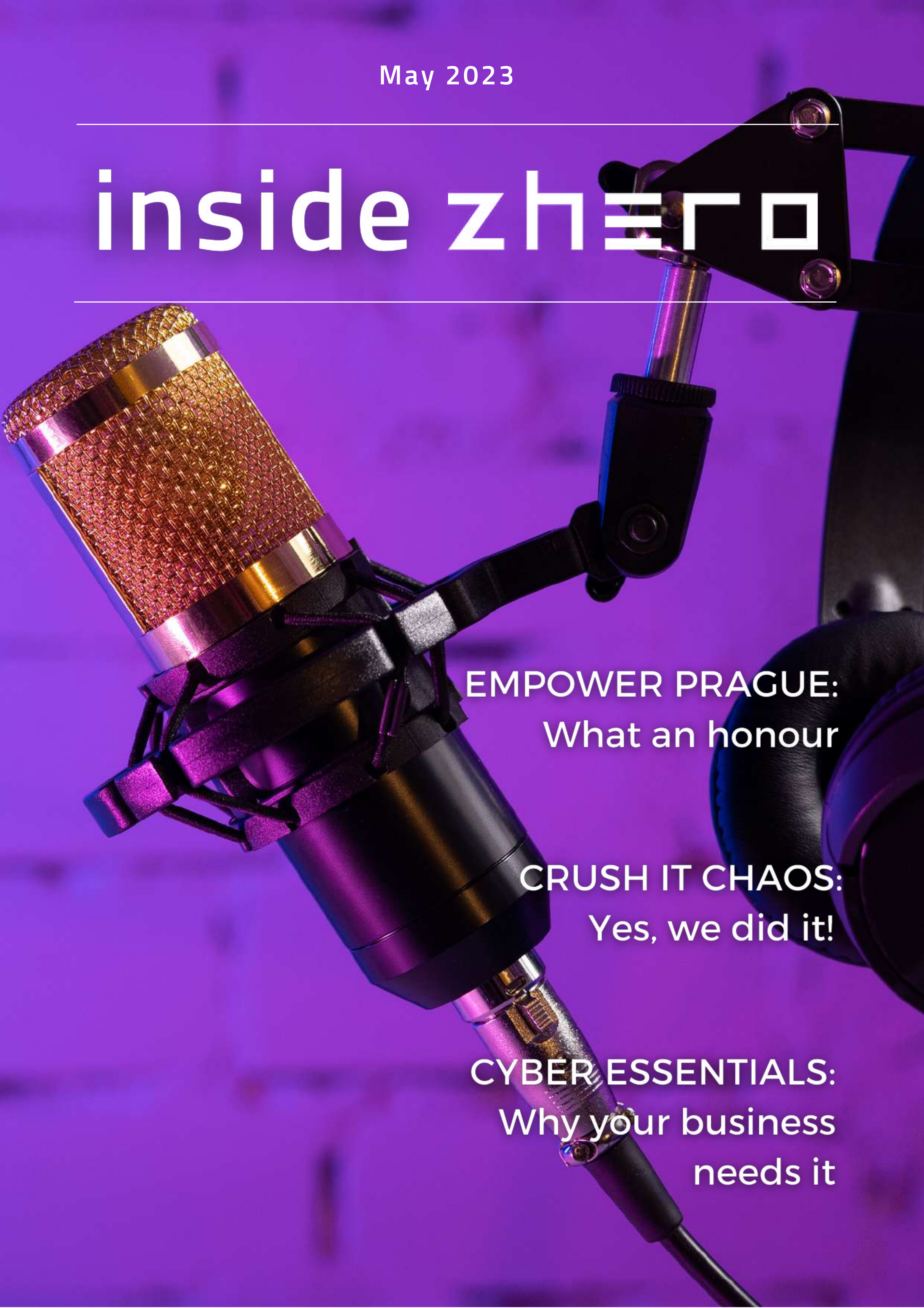
May 2023

inside zhero



EMPOWER PRAGUE: What an honour

CRUSH IT CHAOS: Yes, we did it!

CYBER ESSENTIALS: Why your business needs it

Message from Izak

Welcome to the May edition of Inside Zhero. I'm writing this all the way from Prague while attending the Empower Prague conference, hosted by N-able!

This month we'll see how Cyber Essentials certification will help you level up your online security game.

IZAK OOSTHUIZEN
Bestselling Author,
Founder and MD

In this issue

Our feature "Up Your Cybersecurity Game" explores the practicalities of Cyber Essentials.

We also take a look at five technologies that promise to change the way we work.

Empower Prague by N-able

Earlier this month, Zhero's amazing founder and MD, Izak Oosthuizen, was in Prague attending the Empower Conference. Izak was hand-picked by the hosts, the U.S. cloud technology company, N-able, to be a guest speaker.

On Thursday 11 May, he shared his invaluable knowledge, experience and insights in cybersecurity. Izak's 30-minute presentation, entitled "Building your security stack and cyber resiliency of your customers", focused on how Zhero delivers 24/7 and highly-scalable unlimited cybersecurity support to clients across a broad spectrum of industrial sectors.

Izak was one of 50 MSPs from all over the world selected to participate in #EmpowerPrague. The conference, sponsored by Cisco, CompTIA and others, was an intimate, hands-on mingling of N-able, its partners, and industry leaders. It was designed to empower everybody with actionable insights and ideas to solve problems and improve business.

In the words of David Weeks, the conference organiser and N-able VP Partner experience:

"If you just came to listen, you came to the wrong event."

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

UP YOUR GAME

A sure bet

More than 80% of cyberattacks on UK businesses could be prevented by implementing basic security controls. To address this issue, the government introduced the Cyber Essentials Certification scheme in 2014. The scheme, run by the National Cyber Security Centre (NCSC), is a government-backed and industry-supported initiative aimed at helping businesses combat common cyber threats by executing basic security controls. Industry support for the Cyber Essentials (CE) scheme was strong at launch, with backing from organisations such as the Federation of Small Businesses, the Confederation of British Industry (CBI), and several insurance companies offering incentives to businesses. Since its inception, the scheme has awarded over 120,000 certificates to a range of organisations, including SMEs, charities, and educational institutions.

Contracts and tenders

From 1 October 2014, suppliers bidding for contracts that handle sensitive information must be certified by Cyber Essentials.

Ensuring the integrity of government information not only protects against potential breaches but can also provide a competitive edge when competing for public sector tenders. By obtaining certification, businesses also demonstrate their commitment to cybersecurity.

Although the CE scheme focuses only on the fundamentals of cybersecurity, it offers tremendous benefits to those who become certified. By following the scheme's guidelines, businesses can prevent the vast majority of cyberattacks.

What you need to do

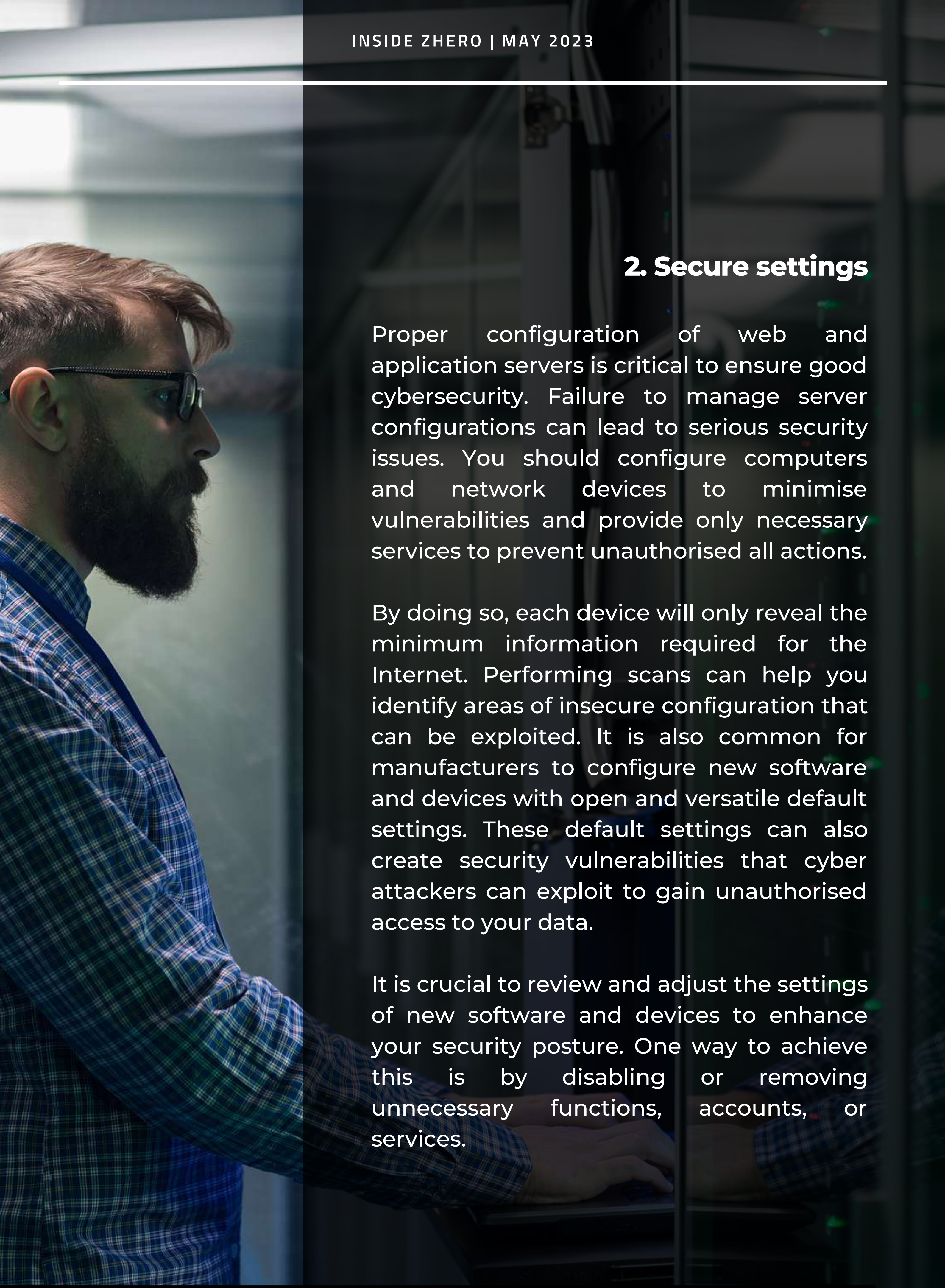
To achieve Cyber Essentials certification, you need to provide evidence against 5 technical controls:

1. Firewalls

The Cyber Essentials Scheme mandates that any device that connects to the internet must have a firewall installed to provide a protective buffer between your device and external networks. A firewall serves as a barrier separating your IT network or device from the internet and other external networks.

As part of the Cyber Essentials Certification, it is necessary to deploy and configure a firewall for all devices that connect to the internet, particularly those that use untrusted or public Wi-Fi networks. This requirement applies to various internet-connected devices such as desktop computers, laptop computers, tablets, routers, and servers.

The aim of this directive is to limit access to only necessary and safe network services from the internet.



2. Secure settings

Proper configuration of web and application servers is critical to ensure good cybersecurity. Failure to manage server configurations can lead to serious security issues. You should configure computers and network devices to minimise vulnerabilities and provide only necessary services to prevent unauthorised all actions.

By doing so, each device will only reveal the minimum information required for the Internet. Performing scans can help you identify areas of insecure configuration that can be exploited. It is also common for manufacturers to configure new software and devices with open and versatile default settings. These default settings can also create security vulnerabilities that cyber attackers can exploit to gain unauthorised access to your data.

It is crucial to review and adjust the settings of new software and devices to enhance your security posture. One way to achieve this is by disabling or removing unnecessary functions, accounts, or services.

3. Patch management

Technical vulnerabilities are a common weakness in all devices and software. Cybercriminals are quick to exploit any vulnerabilities that are discovered and shared publicly. Criminal hackers can exploit known vulnerabilities if operating systems and third-party applications are not properly patched or updated. Updating software and operating systems – aka patch management - is essential to fix these known weaknesses.

It is crucial to act quickly and close any programmes that could be used to gain unauthorised access.

4. Access control

To minimize the risk of damage caused by account misuse or theft, employees accounts should only have the necessary access to perform their duties. CE Certification requires controlling access to data through user accounts and limiting administrative privileges to authorised employees.

User access control measures should be implemented on all internet-active devices and platforms, ensuring access is granted only to authorised personnel and necessary applications, computers, and networks. These measures help protect all sensitive data against cyber threats.

5. Malware and virus protection

Safeguarding your business from malicious software is crucial as malware can easily attempt to gain access to sensitive files stored on your system. Malware can wreak havoc by stealing confidential information, damaging files, and denying access unless a ransom is paid.

Employing measures to defend against a wide range of malware is imperative to protect your computer, your privacy, and your critical documents from malicious attacks.

In a nutshell, the CE objective here is to restrict the execution of known malware and untrusted software and to prevent harmful code from causing damage or accessing your sensitive data.

Getting certified

There are four main steps to becoming CE certified:

- Complete the self-assessment questionnaire online at your own pace.
- Confirm compliance of your company's IT systems with the 5 essential cybersecurity controls.
- Provide assurance of protection against the most common cyber-attacks to a certification body.
- Successful organisations then receive a certificate and a CE branding package.

On average, SMEs take around 2 weeks to complete the Cyber Essentials assessment. Once the assessment is submitted, it typically takes about 3 days for the certification body to provide a response. If the assessment is up to scratch and all requirements are met, the business will be awarded the Cyber Essentials certification.

CE vs CE Plus

The scheme offers two levels of certification: CE and CE Plus. The standard CE certification involves an online self-assessment, while the CE Plus certification requires a more thorough on-premises verification in addition to the self-assessment. SMEs may find that the standard certification is sufficient for their needs, but larger businesses or those seeking to demonstrate their cybersecurity measures to clients, insurers, and professional bodies may want to consider the added assurance provided by CE Plus.

WEBINAR

CYBER ESSENTIALS: YOUR PROTECTION AGAINST AI THREATS

Get ready to level up your security game! Join us for an engaging webinar on Cyber Essentials with cybersecurity expert and CEO of the Cyber Resiliency Centre of London, Simon Newman.

In just 30 mins on 31 May at 10 am DST, he'll show you why Cyber Essentials is a must-have for any business looking to protect itself from online threats.

You'll learn about the importance of Cyber Essentials and why your business can't afford to ignore it – or be without it. Brilliant and friendly as always, our host Jamie Chamberlain will explore the basics of IT security, giving you the tools you need to stay safe and secure online.

Don't miss this opportunity to take control of your business's digital security – sign up now for our Cyber Essentials webinar.

- Wednesday, 31 May
- 10:00 BST

Click here to reserve your spot!

YOUR CYBER SAFETY NET

If you operate a successful SME and already have Cyber Essentials, you could think about adding cyber insurance to your toolkit. This kind of coverage can help you deal with the aftermath of data breaches, security failures, or any other nasty stuff that cybercriminals might throw your way. And let's face it, cyberattacks can be a real headache - they can cost you a lot of time and money to fix. Whichever way you look at it, cyber insurance can help you build up your defences and deal with the risks of the digital age. Reinsurance expert, Torsten Jeworrek, says:

“Cyber insurance is fundamental for the successful digitalisation of the economy.”

Cyber insurance cover

Before buying cyber insurance, it's important to understand how crucial your organization's data, systems, and devices are to your operations so that you can get the right amount of coverage.

Make sure you know exactly what the policy covers and what's excluded. For example, some policies won't cover losses due to business email compromise (BEC) fraud. This is just one example where a standard cyber security policy may not cover a common incident. If this is a concern for you, check that your policy covers it. Keep in mind that cyberattacks are always evolving, and you may become a victim of a new type of attack that didn't exist when you took out the policy.

Check with your broker to see if you'd be covered in case of a new type of cyberattack that's not inherent to your current policy.

Typical first-party cover

First-party coverages include direct costs incurred by your business as a result of cybercrime. Usually, your insurer will cover:

- **Investigating a cybercrime** - paying experts to help you find the source of the cybercrime that affected your business.
- **Managing an attack** - hiring legal experts to advise you about regulations you need to comply with regarding a breach.
- **Reputation management** - covering the costs of a public relations campaign to repair your reputation or even paying for free credit monitoring services or credit protection services for affected customers.
- **Recovering lost data or software programmes** - hiring experts to repair and/or restore this data or software.
- **Restoring computer systems** - hiring experts to restore computer systems damaged by cybercrime.
- **Business interruption** - covering loss of revenue if a cyberattack or data breach prevents you from doing business
- **Notification costs** - covering the cost of notifying affected third parties such as your customers and suppliers of a data breach.

Did you know?

Cyber insurance generally does not cover property damage, which includes computer and other equipment damaged during a cyberattack.

This can be problematic if the hardware has become so corrupt that it's unfixable or more cost-efficient to be replaced.

Ransomware and cyber insurance

According to the 2022 Verizon Data Breach Investigations Report, ransomware accounted for 25% of all cybersecurity breaches.

IBM revealed that the average ransomware payment is around £700,000 for companies who opt to cough up.

That said, in June 2021 the meat-processing vendor, JSA USA, was hit by an attack and reportedly paid $11 million in ransom to criminals that were using the REvil ransomware.

As such, insurers can be wary about covering ransomware or might offer it at a premium price.

Josephine Wolff, a Professor of Cybersecurity Policy at Tufts University in Massachusetts, says of the rise in ransomware:

“Policyholders started filing a lot more ransom claims, and the insurers were making a lot less money – and they were worried that would even start losing money.

I definitely think that having insurance coverage for ransom payments changes the calculus for companies deciding whether or not to pay. It’s the difference between, ‘Am I going to be out of this money myself, or am I going to file a claim with my insurer and have them cover most or all of it?’”

THE STATS ARE TELLING

Cyber insurance pricing increased 66% in Q3 2022, rising faster in the UK than in any other regional market.

56%

Only 56% of medium-sized businesses and 40% of small businesses have cyber insurance.

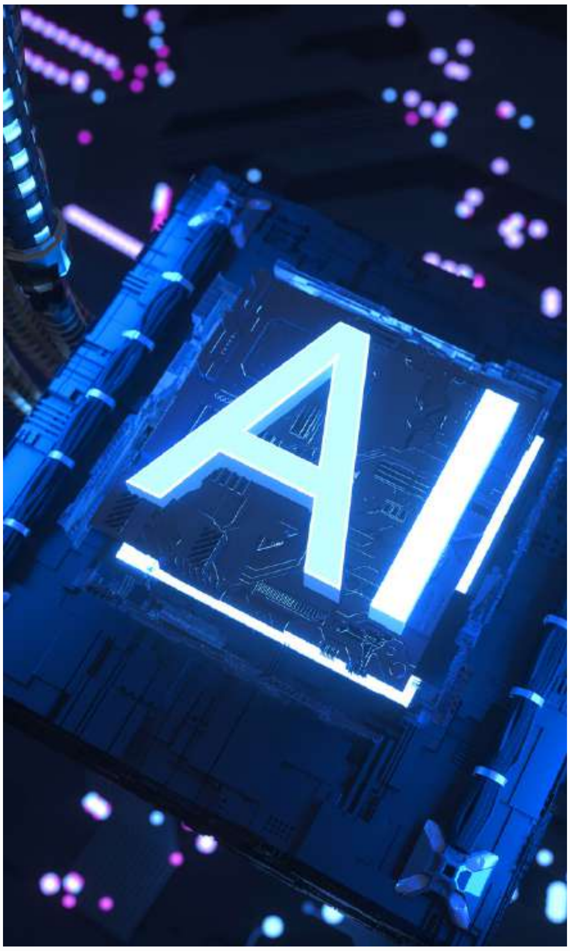
Cyber insurance premiums in the UK typically range from £800 to £7,000 annually depending on the size of your SME and what cover you need.

$92billion

The cyber insurance market is expected to generate $92 billion globally in 2031. Last year the market was valued at $13 billion.

Game-changing technologies

Keeping up with the latest trends and developments in technology is crucial for business leaders to stay competitive and relevant in their respective industries. With that in mind, let's examine five technologies that are gaining the most traction at the moment.



Artificial intelligence

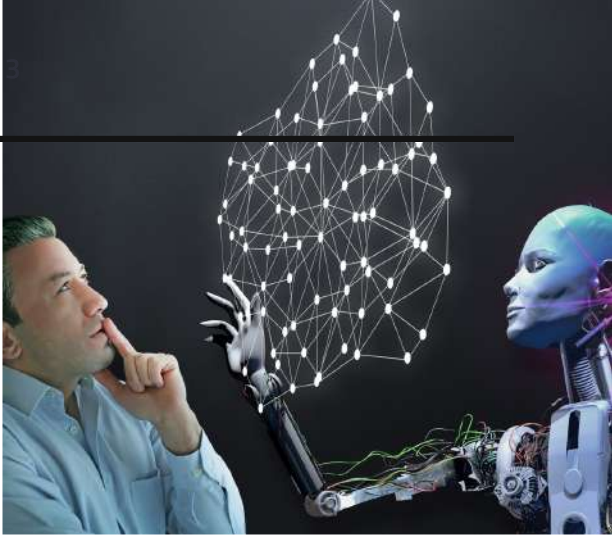
The rise of AI is set to revolutionise how businesses operate – and there's more to this than ChatGPT and other chatbots. With the emergence of no-code AI platforms, companies of all sizes can leverage the power of the technology to create more intelligent products and services. This trend is already visible in the retail market, where companies like Stitch Fix are using AI-enabled algorithms to recommend clothes that match their customers' sizes and tastes.

In the coming years, contactless, autonomous shopping and delivery will be a major trend. AI will make it easier for consumers to pay for and receive goods and services without any human interaction.

Metaverse

The metaverse is an exciting concept that has been gaining more attention lately. Essentially, it’s a more immersive internet that allows us to work, play, and socialise on a persistent platform. As the world becomes increasingly digitised, the metaverse is seen as a logical next step in the evolution of the internet.

Experts predict that the metaverse will add $5 trillion to the global economy by 2030, making it a huge potential market for businesses. This means that companies are likely to invest heavily in metaverse technology over the coming years, which will accelerate its development and adoption.



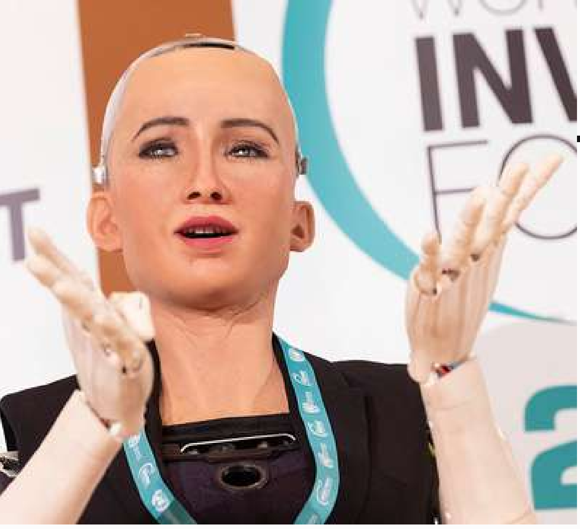
Web 3.0

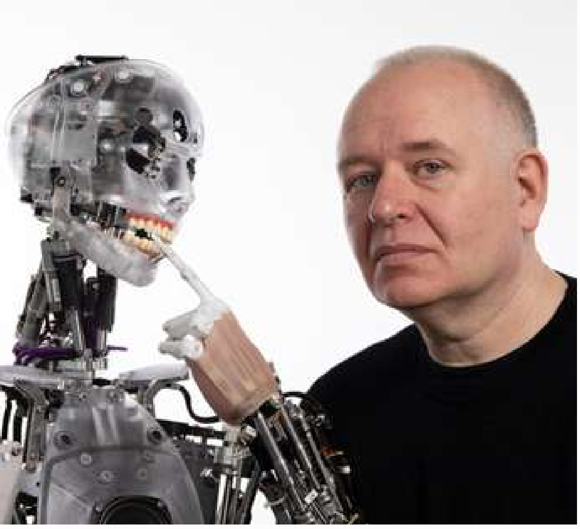
We can expect blockchain technology to make significant advancements, leading to the creation of more decentralised products and services. This technology has the potential to transform the way we store and access data by decentralising data storage and encrypting it using blockchain. This will make our information more secure, and we will have innovative ways to access and analyse it. Non-fungible tokens (NFTs) are also expected to become more practical and widely used in 2023. For instance, NFT tickets to concerts will potentially offer access to backstage experiences and exclusive memorabilia. In the future, we could use NFTs as the keys to interact with many of the digital products and services we purchase.

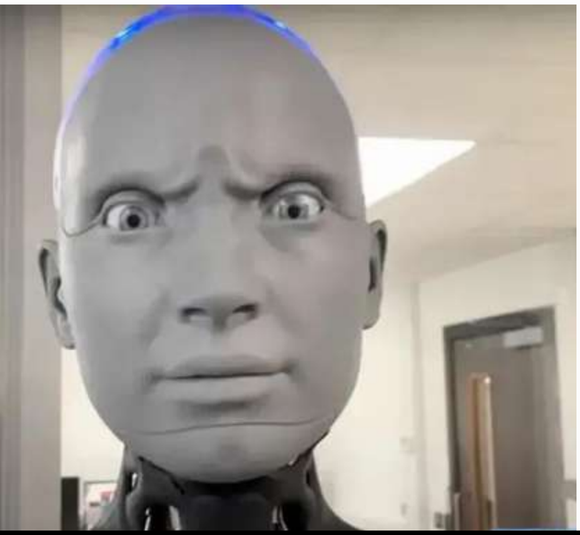
Quantum computing

The development of quantum computing at scale is a global race that is rapidly gaining momentum. Quantum computing, which utilises subatomic particles to process and store information, is a disrupter that is anticipated to provide computers capable of operating a trillion times faster than the quickest conventional processors currently available.

However, there is also a significant risk associated with quantum computing – it has the potential to render our current encryption methods useless. This means that any nation that can develop quantum computing at scale may be able to breach the encryption systems of other countries, businesses, and security systems. This is a trend that will be closely monitored as countries such as the US, UK, China, and Russia that invest heavily in developing quantum computing technology.







Human robots

Robots will become even more advanced in their appearance and capabilities, closely resembling humans. These robots will be increasingly utilised in real-world scenarios as event greeters, bartenders, concierges, and even companions for elderly individuals.

Furthermore, robots will be performing complex tasks in warehouses and factories, working alongside humans in manufacturing and logistics.

One noteworthy company is actively developing a human-like robot that can seamlessly integrate into our homes. During Tesla's AI Day in September 2022, Elon Musk revealed two prototypes of the Optimus humanoid robot and stated that the company will be ready to accept orders within the next 3 to 5 years. This robot will be capable of performing simple tasks such as lifting objects and watering plants, which could lead to the possibility of having "robot butlers" that assist with household chores.

Ameca, created by Cornwall-based firm Engineered Arts, can have a conversation with humans and answer just about any question she's asked. This is the most advanced human-shaped robot ever made.

Team Zhero, our success

Nowadays most of us work in fasted-paced, highly pressured environments. Zhero’s employees are no exception to this situation. As such, we know the importance of supporting our staff through downtime to reduce stress levels. The company arranges monthly social events that serve as a means to sit back, relax, and enjoy quality time together. The gatherings create a sense of camaraderie among team players and help everybody to cope with any stresses and strains of highly-pressurised work.

Recently, we were able to embrace the wonderful weather and enjoy a delightful day at a local wine farm. It was time to unwind and fun was had by all.

Meet the team

Jamie Chamberlain

NEW BUSINESS EXECUTIVE

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

As far back as I can remember I've always had a gamepad in my hand. Seeing how tech has progressed over the years, makes me excited for the future. I'm a natural people's person, that combined with my love for tech, makes me ideal as an IT salesman!

What’s your most-used productivity tool?

Hubspot for sure... Automating the most manual repetitive parts of my day using this tool is beyond a relief!

How would you describe yourself?

Outgoing, naturally conversational, devoted family man who is a sucker for a couple of beers and a few games of Warzone 2.0 on the weekend.

What do you enjoy the most about your role?

I love connecting with new people and talking about how we can take away their pain. I find myself learning new skills everyday, which is something that keeps me excited!

Do you have any hidden talents or hobbies?

My partner says I can multi-task - I am able to talk and annoy her at the same time! Apart from that, I love walking in the Welsh scenery and gaming a lot with my son.

What is your favourite movie or TV show?

I am a huge Marvel fan! Series, it would have to be Game of Thrones, but if my partner had it her way, I would be watching Friends or Kardashians all day...

LONDON

162 Farringdon Road
London
EC1R 3AS

SPEAK TO US

+44 20 7183 3975

zhero

delivering better IT faster