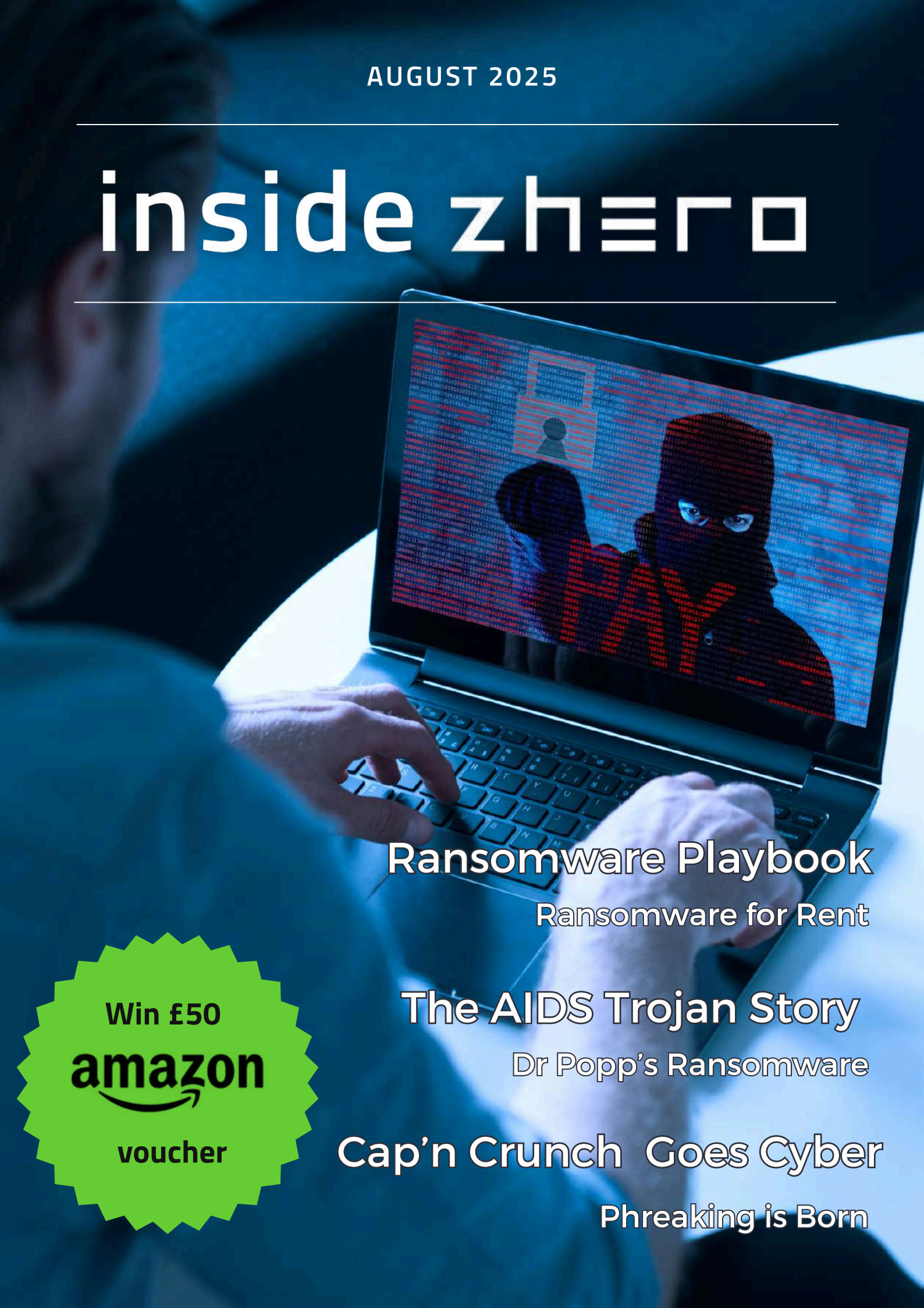
AUGUST 2025

# inside zhero



## Ransomware Playbook

Ransomware for Rent

## The AIDS Trojan Story

Dr Popp's Ransomware

## Cap'n Crunch Goes Cyber

Phreaking is Born

Win £50 amazon voucher

# Message from Izak

Welcome to this bumper August edition of Inside Zhero.

This time, we focus on ransomware, one of the most prevalent cyber threats we face today. There are also some amazing insights from Natasha Botha, our Head of Operations. Also, don't forget Windows 10 end-of-life in October.

**IZAK OOSTHUIZEN**
Chief Executive Officer,
Bestselling Author

## In this issue

Our feature "The Ransomware Playbook" details the current state-of-play of this formidable cyber threat and steps we can all take to protect our precious data from it.

13% of SMEs experienced a ransomware attack in 2024.

*"In recent years, I've watched ransomware threats evolve into one of the most profitable forms of cybercrime. Hospitals, councils, and government agencies have all found themselves paralysed by attacks, and some experts even argue that ransomware now ranks among the most profitable crimes, rivalling traditional organised crime in both scale and impact. From my perspective, the combination of high rewards, relatively low technical barriers, and the ability to operate across borders makes it a near-perfect business model for criminals, yet a persistent nightmare for those of us on the defence side ."*

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author


Available Now

Free 30-minute consultation

30% discount **cyberzhero542**

# RANSOMWARE PLAYBOOK

Ransomware continues to be one of the most formidable cybersecurity threats on both sides of the Atlantic. The National Crime Agency warns that it remains the top organised digital menace, while the USA now accounts for 50% of all attacks worldwide. It remains so dangerous because the damage goes far beyond a locked screen: the financial fallout is crippling, with average recovery costs now exceeding £2 million per incident, and although global ransom payments fell to around £650 million in 2024, down over a third from the previous year, attack volumes continue to rise sharply. Nearly half of victim organisations still end up paying, often under immense pressure, while critical infrastructure - from hospitals to energy providers - has become a prime target. Last year alone, ransomware groups exfiltrated a record 238 terabytes of sensitive data before encrypting systems, using the threat of public leaks to force compliance. With criminals constantly refining their techniques, leveraging Ransomware-as-a-Service (RaaS) to lower the technical barrier for entry, and targeting high-value victims with ever-more sophisticated campaigns, ransomware is no longer a niche cybercrime. Instead, it's a fast-evolving, highly lucrative global industry that thrives on disruption, intimidation, and the sheer inability of many organisations to recover quickly enough to fight back.

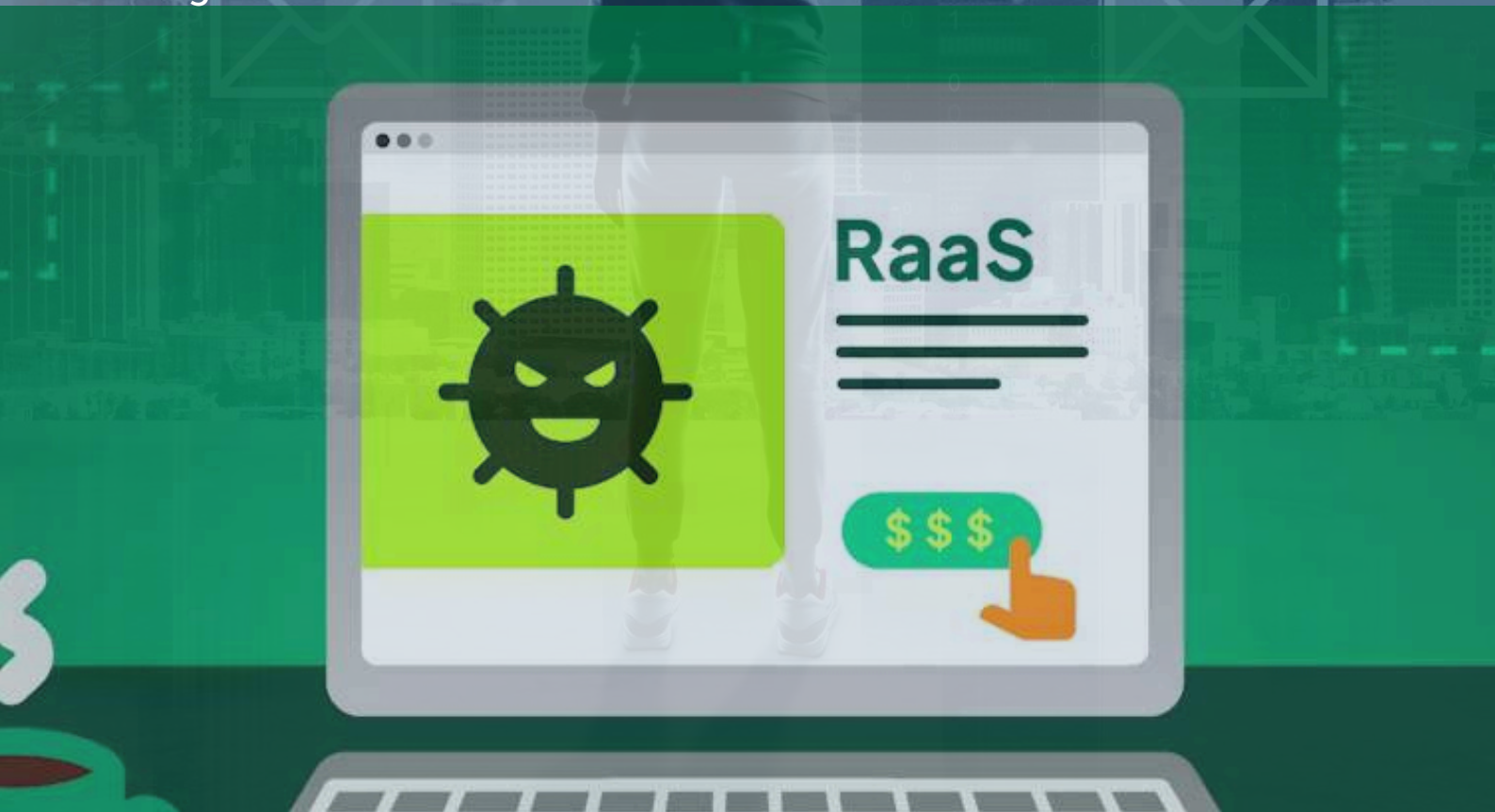
# Real-world ransomware

Ransomware is a type of malware that restricts access to computer systems or data until a ransom is paid. It typically works by encrypting files or locking users out of their devices, demanding payment, often in cryptocurrency, for the decryption key or access. How ransomware attacks unfold:

- **Infection** - Ransomware can enter systems through a variety of means, including phishing emails containing malicious attachments or links designed to trick recipients into downloading the malware, visiting compromised or fake websites that trigger automatic downloads, exploit kits that take advantage of software vulnerabilities without any user action, or direct manual attacks where cybercriminals gain access to an organisation's network and deploy the ransomware themselves.
- **Encryption or Lockout** - Once inside the system, the ransomware will either encrypt the victim's files, rendering them inaccessible, or lock the user out of their device entirely.
- **Ransom Demand** - Attackers then present a ransom note, typically demanding payment in cryptocurrency in exchange for a decryption key or to restore access. The note often includes a deadline and threats to delete or leak stolen data if the ransom is not paid.
- **Data Theft and Double Extortion** - Increasingly, criminals extract sensitive data before encryption, enabling a "double extortion" tactic. This allows them to demand payment both for restoring access and to prevent public release of the stolen information.
- **Payment and Decryption** - If the victim pays, the attackers may provide a decryption tool; however, there is no guarantee it will work as promised or that stolen data will not be misused. In some cases, the malware remains on the system, leaving the organisation vulnerable to repeat attacks.
- **Recovery and Aftermath** - Victims must remove the ransomware, restore data from backups where available, and patch any exploited vulnerabilities.

# Ransomware for rent

Ransomware as a Service (RaaS) is a business model in which ransomware developers, known as operators, create and distribute ransomware tools that affiliates then use to launch attacks for a fee. Essentially, it enables individuals with limited technical skills to participate in cybercrime by using ready-made ransomware tools. This model lowers the barrier to entry for cybercriminals, making it far easier for less-skilled individuals to carry out attacks. Ransomware operators are the individuals or groups responsible for developing the ransomware software, while affiliates are those who pay to use these tools to conduct attacks. RaaS is a criminal adaptation of the legitimate Software as a Service (SaaS) model, where software is provided on a subscription basis. By offering ransomware tools in this manner, RaaS facilitates almost plug-and-play cybercrime, enabling even those with minimal technical expertise to become cybercriminals, thereby increasing the number of potential attackers. The widespread availability of these tools also makes defending against ransomware far more challenging for organisations, as the variety and sophistication of attacks continue to grow.



*"Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication."*

**~ James Scott**

# Rising RaaS

The rise of RaaS groups and their affiliates, often backed by government entities, is run like large organisations, with business strategies, a large workforce and a vast amount of resources. Believe it or not, some even try to act "ethically" by choosing to keep healthcare, religious and charitable organisations off the hit list. Other threat groups aren't so ethical. Instead, their sole aim is to disrupt public services and hold them ransom/hostage until a fee is paid. The NHS is a prime example of this. NHS ransomware attacks on trusts have been well-reported over the past 18 months; the knock-on effect of these attacks can be detrimental; hospital appointments have been cancelled, and critical services have been forced to close. In highly regulated industries like healthcare and finance, the stakes are highest. IBM's cost of a data breach 2024 report highlighted that healthcare remained the costliest industry for breaches, with an average cost of $9.77 million per incident. For Critical and National Infrastructure, the stakes are even higher. There is not only a financial risk, but also the potential threat to human life. We have seen everything from food production lines halting, oil pipelines shutting off, and hospitals closing their doors. This is why cybersecurity for public services must be a top priority.

# Global cyber epidemic

The WannaCry ransomware attack was a global crisis that erupted in May 2017, targeting computers running Microsoft Windows. Victims' files were held hostage, with a Bitcoin ransom demanded for their release. The attack exploited outdated computer systems and poor awareness around the importance of software updates, meaning much of the damage could have been avoided. Cybercriminals leveraged a vulnerability in Windows using a hack known as EternalBlue, allegedly developed by the United States National Security Agency, which was later made public by the hacker group Shadow Brokers. Microsoft had released a security patch almost two months before the outbreak, but many individuals and organisations had not updated their systems, leaving them exposed. Initially, the spread of WannaCry was assumed to be via a phishing campaign, but EternalBlue allowed the ransomware to propagate rapidly, with DoublePulsar serving as a backdoor to execute the malware.

# Demands and lessons learnt

The attackers initially demanded $300 worth of Bitcoin, later raising it to $600, threatening to permanently delete files if victims did not pay within three days. Experts strongly advise against paying ransoms, as there is no guarantee of recovering data, and payments only encourage further attacks. This proved particularly relevant during WannaCry, as the ransomware's coding was flawed, payments could not be linked to individual victims, and it remains uncertain whether any files were restored. Some researchers claim no victims recovered their data, while F-Secure reported that a few did. The attack highlights the importance of keeping systems updated, educating users, and never giving in to ransom demands.

# World in lockdown


In 2017, the WannaCry ransomware attack hit around 230,000 computers globally. One of the first companies affected was the Spanish mobile company, Telefónica. By 12 May, thousands of NHS hospitals and surgeries across the UK were affected. A third of NHS hospital trusts were affected by the attack. Terrifyingly, ambulances were reportedly rerouted, leaving people in need of urgent care in need. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were cancelled as a result of the attack. As the ransomware spread beyond Europe, computer systems in 150 countries were crippled. The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated that this cybercrime caused $4 billion in losses across the globe.

# Fighting back

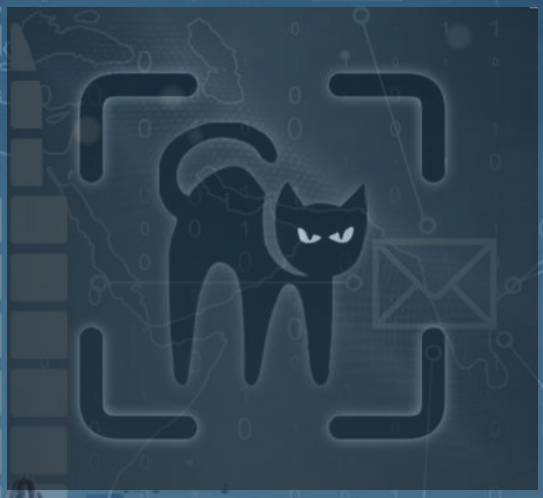
There's no magic fix  or silver bullet for ransomware, but there are proven strategies to reduce risk and recover faster:

- **Keep systems updated** – Patch vulnerabilities in operating systems, firewalls, and applications as soon as updates are available. Many ransomware campaigns exploit known and preventable flaws.
- **Educate and train employees** – Human error is still the number one way attackers get in. Phishing simulations and security awareness programs can make a big difference.
- **Back up your data** – Regular, offline backups are your best insurance policy. Test them to make sure they actually work.
- **Network segmentation** – Divide your network into zones so that a breach in one area doesn't give attackers free rein everywhere.
- **Incident response planning** – Create and rehearse a clear plan for containing, eradicating, and recovering from an attack.
- **Adopt Zero Trust security** – Verify every user and device, every time. Trust nothing by default.

# SMEs at risk

The 2024 saw authorities launch several successful operations to take down prominent cyber threat groups. The elimination of these larger groups is a positive development for threat defence:

- **LockBit** - a RaaS group, eliminated by law enforcement efforts led by the UK's National Crime Agency in conjunction with the FBI and Europol.



- **BlackCat** - another RaaS group that the FBI previously disrupted in 2023, ended operations in March 2024 following their successful attack targeting Change Healthcare, and a ransom payout reportedly worth over 22 million U.S. dollars.

- **Black Basta** - which appeared to have stopped operations now after leaked chat logs revealed concerns about law enforcement scrutiny after an attack on the US Health System Acension, which included 140 hospitals across 19 states.


However, the number of smaller groups and "lone wolf" threat actors propagating attacks has increased. Some groups have also shifted their aim downstream, avoiding critical infrastructure to reduce scrutiny by law enforcement and targeting small and medium-sized enterprises (SMEs) that often have weaker cyber defences.

*"One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats."*

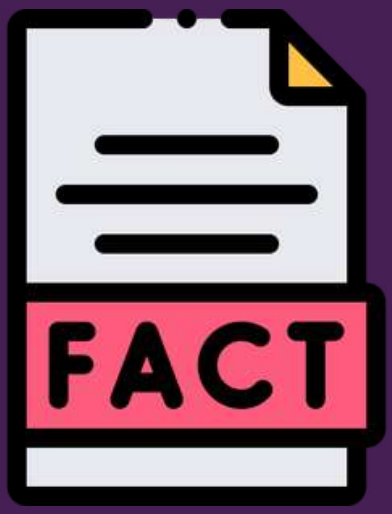
**~ Stephane Nappo**

# The power of people

We humans play a critical role in ransomware resilience. In a recent study, just 26% of organisations had a ransom payment decision process in place to guide a rapid response to payment demands based on potential impact. Many also lack procedures for informing law enforcement, which could aid in recovery and compliance. Over a third of organisations used internal team members to communicate with threat actors. The rest relied on third parties to assist them, including incident response specialists and ransom negotiation specialists. These specialists are indispensable for guiding engagement based on a detailed understanding of threat actor behaviour, which helps support more successful outcomes. Having internal team members communicate with threat actors can also inadvertently expose an organisation to additional risks and threats. What we need is a pre-defined chain of command for dealing with attacks. The chain of command helps ensure proper authorisation ladders and approvals for critical decisions during incident response, up to and including engaging with threat actors or paying a ransom.

# From chaos to resilience

No matter the day or time, it's always a bad time to experience a ransomware attack, which is why it's so important to have a roadmap for responding to such stressful and time-sensitive threats. Ransomware thrives on confusion and panic. For years, it was spoken about in hushed, technical terms, as if only cybersecurity experts could understand it. But the truth is, the concept is as old as crime itself: someone takes something valuable from you, then demands payment for its return. The difference today is scale and speed. The attacks are digital, but the consequences are human, affecting businesses, services, and lives. Understanding how ransomware works is the first step in defending against it. The second is preparation. And the third is resilience — the ability to recover without feeding the very criminals who caused the damage. Because in the end, the best defence isn't about being invincible. It's about making yourself a harder target and ensuring that when the stranger comes knocking, your doors stay locked from the inside.



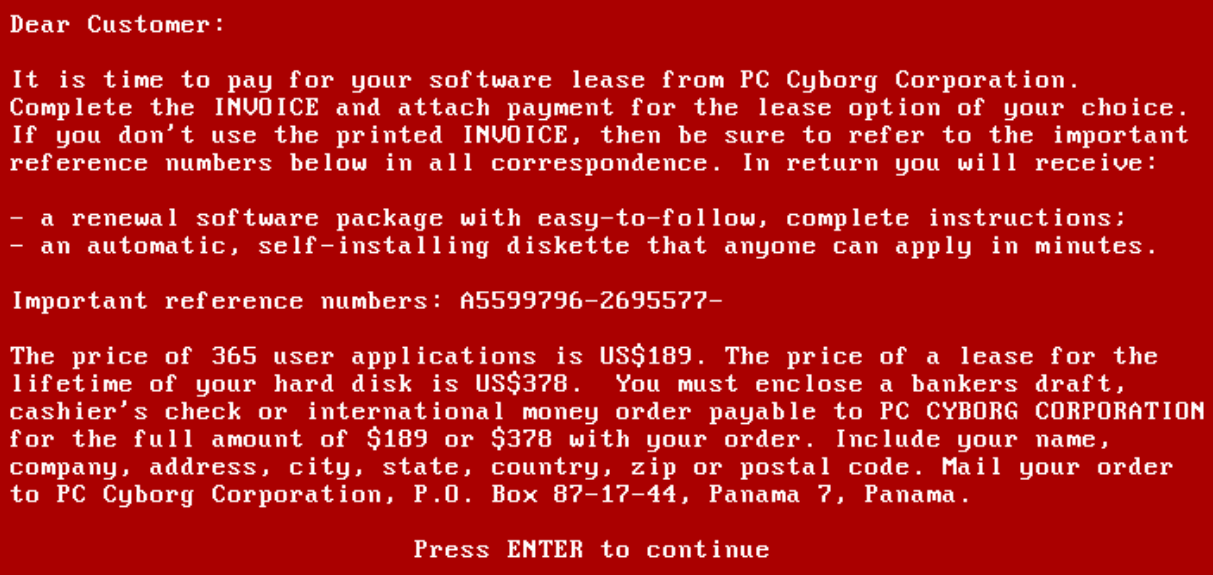

- 66% of organisations were hit by ransomware in the last year
- 13% of SMEs experienced a ransomware attack in the past year
- 41% of those who paid a ransom failed to recover all their data
- 40% of enterprises laid off employees after a ransomware attack
- 80% of businesses that paid the ransom were subject to another attack


# AIDS TROJAN

Ransomware isn't new – it predates email and the Internet as we know them. The first recorded attack reads like a thriller: a global pandemic, the World Health Organisation (WHO), a high-profile conference in Stockholm, organisations worldwide compromised, airport authorities on alert, law enforcement scrambling, and a legal system unsure how to respond. The culprit? The PC Cyborg virus, also known as the AIDS Trojan, was unleashed in 1989 by evolutionary biologist Dr Joseph Popp, a part-time WHO consultant researching AIDS. Dr Popp distributed 20,000 disks to conference attendees, labelled "AIDS Information – Introductory Diskettes," claiming they contained a computer-based questionnaire to assess AIDS risk. Each disk included a warning: the software would "adversely affect other program applications" and users would owe "compensation and possible damages to PC Cyborg Corporation." Many ignored the warning, proving that, even then, no one read the terms and conditions.

# Trojan strikes

The malware lay dormant until the computer was switched on 90 times, then activated, freezing systems and displaying a ransom demand. Victims were told to print a note demanding a minimum $189 license fee, or $378 for a full license, payable to a PO box in Panama. Panic ensued: some victims deleted entire drives, and an Italian AIDS organisation lost ten years of invaluable research. Weeks later, Dr Popp attended a WHO seminar in Nairobi, unaware the Trojan had made him a global target. On his return to the U.S., he drew authorities' attention at Schiphol airport by scribbling "DR. POPP HAS BEEN POISONED" on another passenger's suitcase. A search revealed links to PC Cyborg Corporation. Arrested by the FBI for ten counts of blackmail and criminal damage, he was extradited to Britain, the site of the virus's first reports – a time when no law existed for this type of cybercrime.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                    Press ENTER to continue
```

# Digital legend?

In November 1991, Judge Geoffrey Rivlin ruled Popp unfit to stand trial and deported him back to the U.S., where he continued his evolutionary research, published Popular Evolution, and created the Joseph L. Popp Butterfly Conservatory in upstate New York. Years later, cryptographers Adam Young and Moti Yung dissected Popp's code and pioneered crypto virology, demonstrating how public-key cryptography could lock victims' data securely, forcing ransom payments for decryption – effectively planting the seeds of modern ransomware.

zhero

# A Journey into Cybersecurity

This month, Natasha Botha, our awesome and formidable Head of Operations and Finance, tells what led her into the world of cyber and IT support.

Back in 2017, I swapped gas pipelines for network cables and left the gas industry to join the fast-paced, unpredictable world of managed IT services. I thought I knew what "change" meant... I was wrong.

In technology, nothing stays still. What worked yesterday could easily break today. What was safe last week could be a major security risk tomorrow. It was an eye-opener. Not only the pace of change, but also how many people underestimate the importance of cybersecurity. And here's the kicker: keeping up with it all can cost a fortune. At my previous IT company, we chased every new trend — a fresh service here, a shiny solution there. Every month, something new to sell. But it felt like running on a treadmill: lots of movement, little progress.

Then I joined Zhero. That's when I learned an important lesson — you don't have to reinvent yourself every time the market shifts. Consistency matters. Stick to the basics. Build scalable systems. Deliver premium service without the premium price tag.

Seven years later, I've worked with businesses in all sorts of industries, each with its own challenges and goals. I never thought I'd find another calling beyond finance, but here I am — in love with what I do, both operationally and financially. And the best part? Helping clients succeed never gets old. Every day brings something different — a new problem to solve, a smarter way to do things. It keeps me intrigued, motivated, and passionate.

# Windows 10 EOL

**On** 14 October 2025, Windows 10 Home and Pro will reach end of support or end of life (EOL). End of Life (EOL) is when a software application is taken off the market or not renewed. The manufacturer may still provide some support, such as security patches and updates. End of Support (EOS) is the complete discontinuation of all support services for the software.

## WHAT THIS MEANS

- No more free updates - After October 14, 2025, Windows 10 users will not receive any further free security updates, feature updates, or technical support from Microsoft.
- Security risks - Running Windows 10 without security updates will expose your device to potential security threats, malware, and vulnerabilities.
- Upgrade or replace - Microsoft advises users to either upgrade to Windows 11 (if their hardware is compatible) or replace their devices with new ones that support Windows 11.
- Extended Security Updates (ESU) - Microsoft offers an ESU program for Windows 10, which provides paid security updates for a limited time after the EOL date, but it's not a long-term solution and doesn't include new features.
- Windows 11 advantages - Windows 11 offers a modern and efficient experience with enhanced security features, designed to meet current demands.
- Free upgrade - Upgrading from Windows 10 to Windows 11 is free for eligible devices.
- PC Health Check - If you're unsure whether your PC is compatible with Windows 11, you can use the PC Health Check app to check its eligibility.

# Windows 10 EOL

## WHAT WILL HAPPEN

Your PC will continue to work, but all support for Windows 10 is discontinued.

## WHAT YOU CAN DO

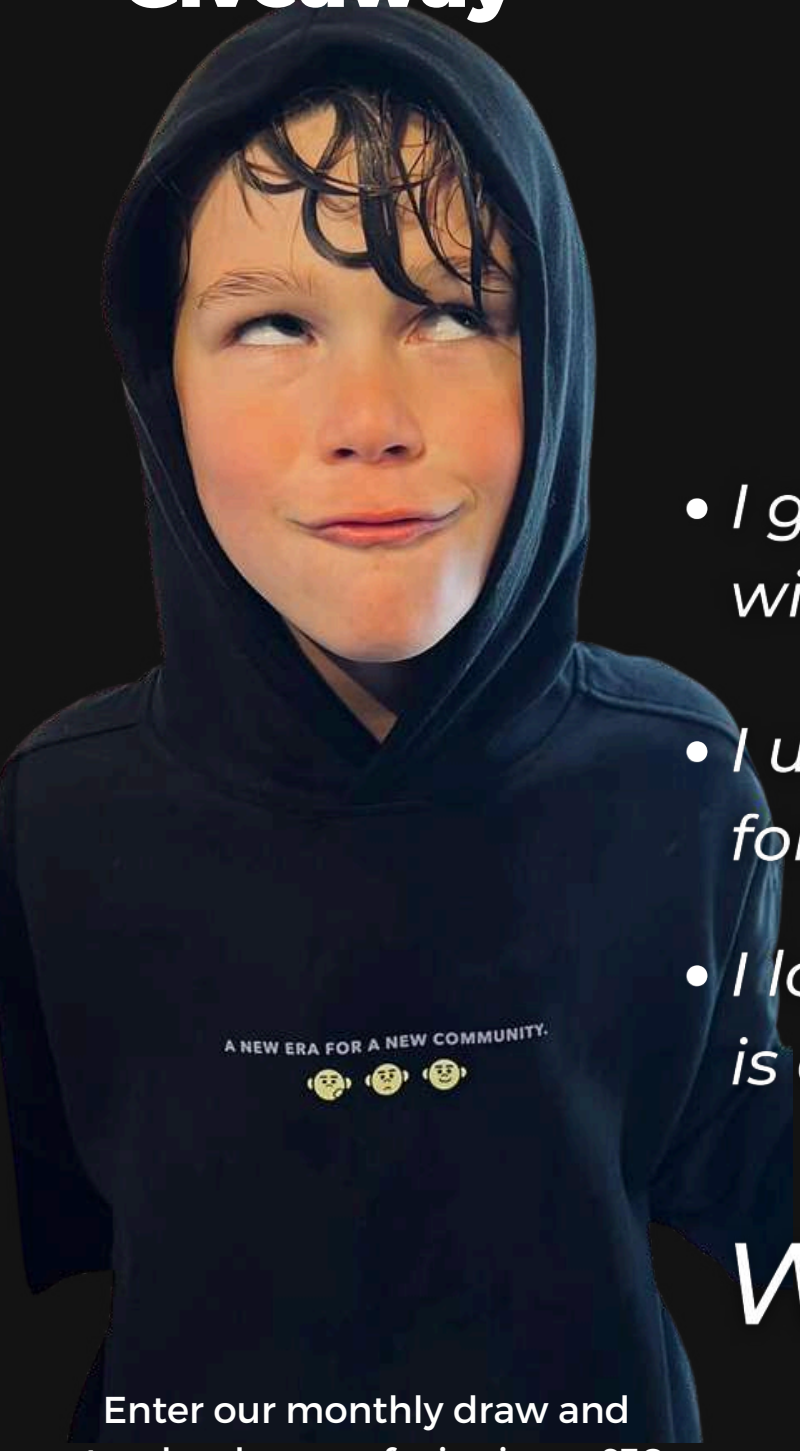
- You could ignore the EOL deadline completely. This is NOT recommended as your PC is no longer receiving updates and security patches from Microsoft. This means your PC is vulnerable to malware infections and other cyber threats. You will also experience performance and compatibility issues.
- You can pay Microsoft for security updates for Windows 10. With the Extended Security Updates package you can keep your current Windows 10 device fully protected for up to 3 years. According to Microsoft, the first year of protection will cost £50. This increases to £100 in the second year and £150 in the final year of cover.
- You can upgrade your existing PC to Windows 11 or buy a new laptop with this latest OS already installed.

## WHAT WE WILL DO

Zhero recommends switching to Windows 11. We will assess whether your existing PC can be upgraded and is capable of running Windows 11 or if you will need a new workstation.  While making the change to a new OS may seem daunting, we are here to support and assist you in every way we can.

# Digital Defender Giveaway

Win £50 amazon voucher




- *I give you access without typing a word*
- *I use what the cops look for at a crime scene*
- *I love it when your face is clear and clean*

## *What am I?*

Enter our monthly draw and stand a chance of winning a £50 Amazon voucher. The winner will be announced in the next edition of Inside Zhero.
Competition ends 21 September.
Good Luck!

## August Winner!

Congrats to Wincent Olivier, one of Zhero's Service Desk Engineers, for winning last month's draw and a £50 Amazon voucher.

**Enter Now**


# CEREAL TO CYBER

In the early 1970s, the seed of a technological revolution was planted in the most unlikely of places, the bottom of a cereal box. John Draper, a U.S. Air Force veteran with a knack for electronics and an ear for tone, discovered that a small plastic toy from a Cap'n Crunch box, the Bo'Sun whistle, emitted a perfect 2600 Hz tone. This was no ordinary sound. AT&T's nationwide long-distance network still relied on a signalling method called "in-band signalling," where the same line that carried a voice call also carried control tones. The 2600 Hz tone, in particular, told the system a line was idle and ready for instructions. Draper realised that by blowing the whistle into a payphone handset, he could trick the network into believing it was speaking to a telephone operator. That single quirk opened a secret back door into one of the most advanced communication systems in the world.

# Birth of phreaking

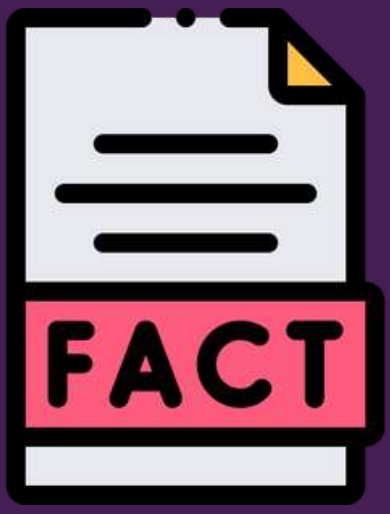
What Draper stumbled upon became the foundation of a new underground culture known as “phone phreaking.” With the right set of tones, phreakers could do far more than make free long-distance calls. They could hop onto unused trunk lines, explore hidden test circuits, and eavesdrop on parts of the network never meant for public access. The phone system was, in essence, a vast and mysterious machine, and phreakers were its early explorers. The era lacked the concept of “cybersecurity” as we know it, and telecom companies did not yet imagine that hobbyists armed with cereal toys and soldering irons could pose a threat. It was an age where curiosity, ingenuity, and a dash of mischief could outpace the multi-billion-dollar infrastructure of corporate giants.

# Whistles to blue boxes


Draper’s exploits inspired him to go further. He engineered an electronic device called the “blue box,” which could reproduce the full range of control tones used by AT&T’s system. The blue box did not just open a single hidden door; it handed over the master keys. Two ambitious young students at the time, Steve Jobs and Steve Wozniak, were fascinated by Draper’s creation. They built their own versions, selling them to fellow students out of dorm rooms, and spent nights dialling into the phone system just to see where it would take them. It was not only about free calls, but it was also about mastering a system that seemed untouchable. Jobs would later say, “If it hadn’t been for the blue boxes, there would have been no Apple.” In that moment, the line between prankster and pioneer blurred, and a new kind of tech entrepreneur was born.

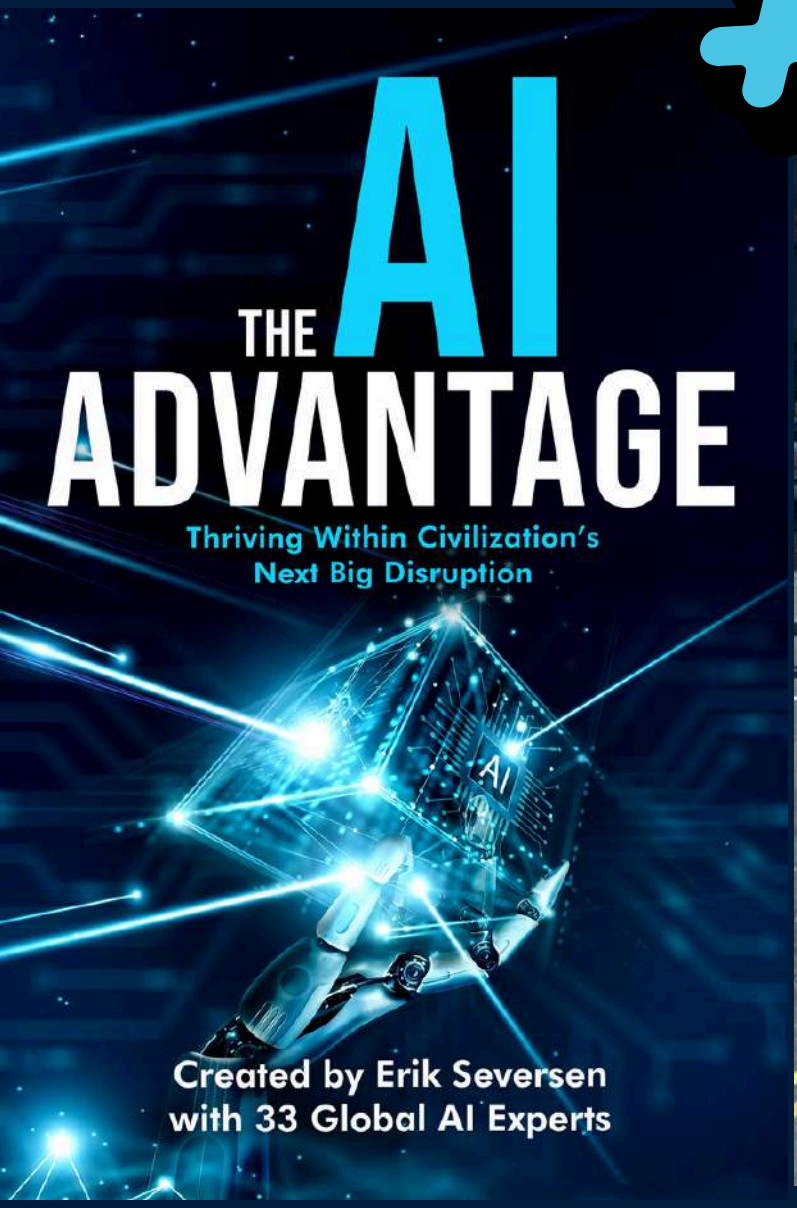
# The first hackers

Many historians call the phreakers the first modern hackers, although the roots of hacking run deep, back through wartime codebreakers, medieval lockpickers, and even ancient engineers who found ways to bypass physical mechanisms. What set the 1970s apart was the scale and interconnectedness of the systems being explored. A cereal-box whistle was no longer just a toy; it was a skeleton key to a sprawling technological empire. Phreaking quickly evolved into a culture of exploration that spilt over into the computer world. By the early 1980s, groups inspired by phone hackers were breaking into time-sharing systems and corporate mainframes; one 1983 FBI report estimated that over 1,000 major computer intrusions had already been logged in the U.S., many traced back to techniques pioneered by phreakers. Within a decade, the number of reported hacking incidents jumped from just 6 in 1988 to over 2,400 by 1995. What began with blue boxes and cereal whistles had laid the foundation for a global hacking community. The lesson still holds today: vulnerabilities do not always hide in lines of code; they lurk in assumptions, in overlooked systems, in the forgotten quirks of design. Whether it is a breakfast toy, a pop song, or a protocol nobody remembers, clever minds will always find a way in. And in doing so, they remind us that security is never just about defending against known threats; it is about imagining the ones no one has thought of yet.




- The term "hack" originated at MIT in the 1950s and 60s, initially referring to clever programming solutions and shortcuts
- In 1971, Bob Thomas created the “Creeper” program as an experiment on ARPANET, displaying the message: “I’M THE CREEPER: CATCH ME IF YOU CAN”
- In 1999, a 15-year-old known as “c0mrade” hacked into NASA computers, downloading $1.7 million worth of software. NASA had to shut down systems for three weeks

# BESTSELLER #FOUR





Joining the ranks of Izak's three other Amazon bestsellers, 'Adapt and Overcome', 'Cybersecurity Now' and 'You Don't Need a £1 Million Cybersecurity Budget', is his fourth, "The AI Advantage: Thriving Within Civilization's Next Big Disruption." Created by Erik Seversen along with 33 global AI experts, the book is a blueprint for personal and professional growth, exploring how AI tools are already reshaping industries, automating tasks, unlocking new creative possibilities, and enhancing decision-making. In his chapter on the role of AI in cybersecurity, Izak details that artificial intelligence is a key player in cybersecurity, evolving from a promising idea into a vital tool for identifying, mitigating, and preventing cyber threats. Izak also tells us that looking ahead, predictions suggest that AI will play an even greater role in detecting and responding to threats, using machine learning and AI-driven tools to spot sophisticated cyber risks at an early stage.

Get your copy on **Amazon**

# Meet the team

## Shaikh Afraz

ONSITE ENGINEER

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

Everything today is run by IT.. isn't it.. You are in IT without realising IT. FUN to be in IT!

What's your most-used productivity tool?

Microsoft Teams – it keeps communication flowing and collaboration effortless.

How would you describe yourself?

Team worker.Enjoy to be part of a team which helps build relationships which last more than a while!

What do you enjoy the most about your role?

It allows you to be casual despite being professional at the same time.

Do you have any hidden talents or hobbies?

I like to yell (sing ?)

What is your favourite movie or TV show?

My favourite  movie is "Terminator" because it's an action movie.

# 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