APRIL 2025

inside zhero

Cyber through Time

Evolution of Cybersecurity

N-able Empower Berlin

Forward Never Stops

Cyber London CAN

Cyber for All

Message from Izak

Welcome everybody to our Easter edition of Inside Zhero.

This month, we look at the evolution of cybersecurity, leading up to current trends such as MDR and AI cyber. You can also check out our amazing trip to N-able Empower Berlin, where myself, Louis and Wesley took the stage.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature “Cyber through Time!” details how cybersecurity has adapted to changes in threats, particularly in the 2010s.

The market growth of MDR is 50% compared to the rest of the cybersecurity market at around 9%.

"I believe the future of cybersecurity is tough to pin down. Honestly, the whole industry is always changing. As cyber threats keep evolving, the tools we use to fight them have to keep up and constantly adapt to protect networks that are getting more and more complex."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now

Free 30-minute consultation

30% discount **cyberzhero542**

CYBER THROUGH TIME

Cybersecurity is essential for protecting digital assets, sensitive information, and the stability of individuals, businesses, and national security. It prevents unauthorised access, misuse, and damage to systems and data. Strong cybersecurity safeguards personal, financial, and health information, builds customer trust, ensures business continuity, and helps prevent financial losses from cyberattacks. It also protects government, military, and critical infrastructure networks against cyber threats that could disrupt society. Compliance with data protection laws and industry standards requires robust security measures, while effective cybersecurity defends against malware, phishing, and unauthorised access, preserving the integrity and functionality of systems. In 2025, cybersecurity is a critical component of society. The history and evolution of cyber is both interesting and informative. Let's take a looksee at its beginnings and how security measures have adapted to deal with the threats and challenges of today.

The first cyberattack

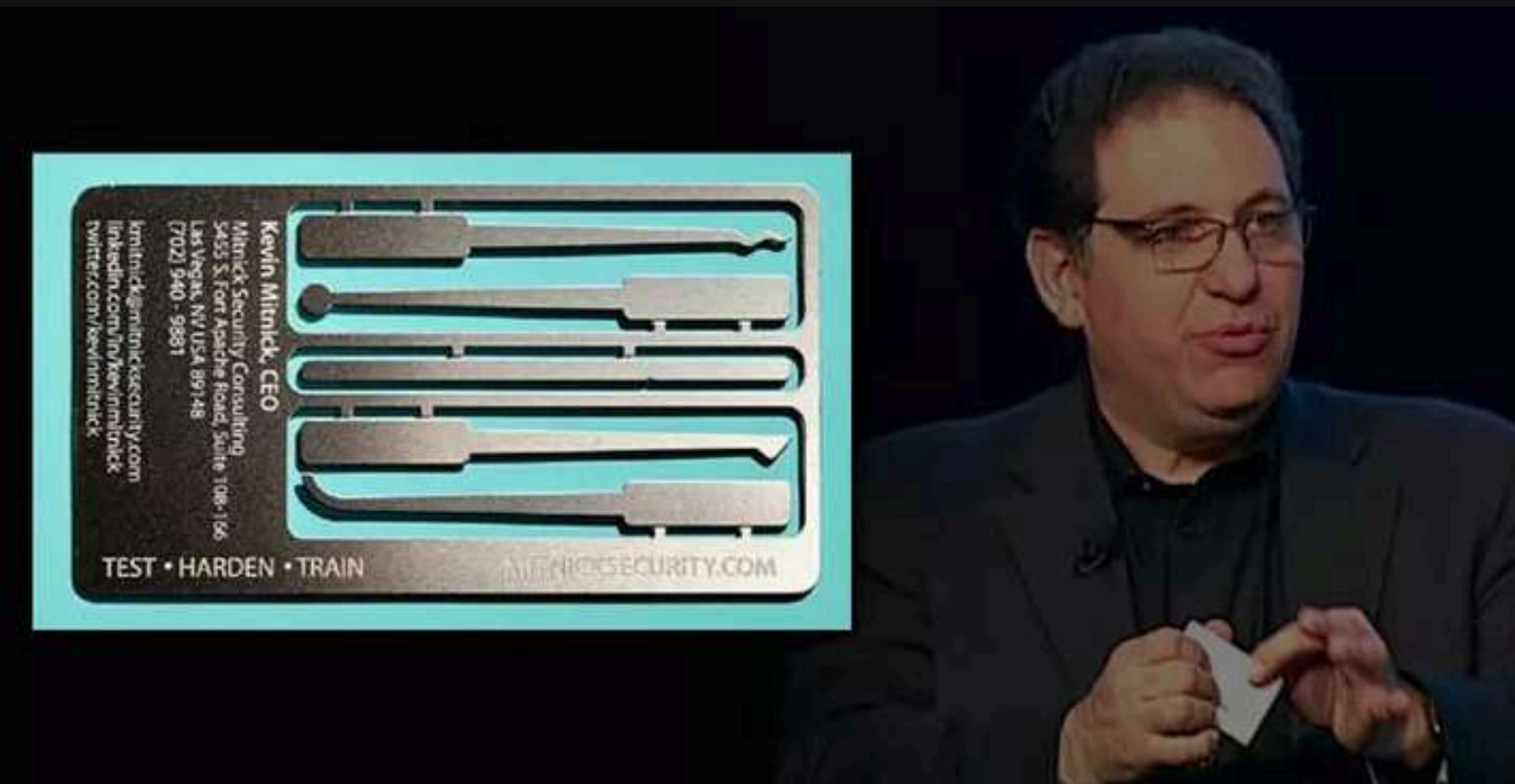
The first cyberattack is believed to have occurred in France in 1834 when two thieves hacked the French Telegraph System to steal financial market information. Over the years, other hackers emerged to disrupt phone service and wireless telegraphy, but things escalated in 1940 with René Carmille, considered the first ethical hacker. A punch-card computer expert and member of the French Resistance, Carmille discovered that the Nazis were using his machines to track Jews; he offered access to his systems, then secretly hacked and disrupted their efforts.

Passwords and viruses

In 1962, MIT introduced the first computer passwords to limit student access, but Allan Scherr, an MIT student, created a punch card to print all the passwords, using them to gain extra computer time and prank his teachers. The first computer virus appeared in 1969 at the University of Washington Computer Centre, where an unknown individual installed what became known as the “RABBITS Virus,” a self-replicating program that overwhelmed and crashed the computer.

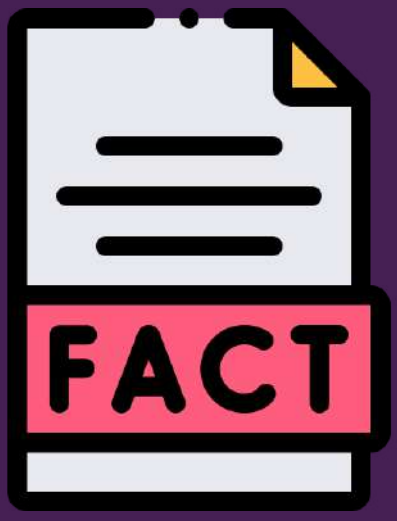
FBI's most wanted

Kevin Mitnick is often hailed as the world's first infamous cybercriminal, a modern outlaw who exposed just how vulnerable even the most secure systems could be. From 1970 to 1995, he launched a relentless spree of hacking, infiltrating top corporations like Motorola, Nokia, IBM, and even government networks. His weapon of choice wasn't just technology, but people — using masterful social engineering tactics to manipulate employees into handing over passwords, codes, and access without ever realizing they'd been deceived. Mitnick's ability to slip past defenses triggered one of the most legendary FBI manhunts in American history. When he was finally captured in 1995, authorities considered him so dangerous they kept him in solitary confinement, fearing he could spark global chaos with a mere phone call and cause a nuclear war. After serving nearly five years in prison, Mitnick reinvented himself, emerging from the shadows to become a cybersecurity consultant, keynote speaker, and best-selling author, turning his once-illegal talents into a force for good. He was also known for his mischievous businesscard in the form of a removable lockpick toolset. Mitnick died in Pittsburgh, Pennsylvania at age 59 in 2023.



“Catch me if you can!”

The history of cybersecurity is fascinating and is believed to have begun in 1971 when Bob Thomas, a computer programmer at BBN, created the first computer virus as a security test. Named "Creeper" after a Scooby-Doo villain, the virus was not malicious but exposed vulnerabilities in ARPANET, the early network developed by the U.S. Department of Defence that eventually evolved into the internet. Creeper was designed as a non-harmful, self-replicating program to demonstrate how mobile applications could work, but it ended up corrupting DEC PDP-10 mainframe computers at the Digital Equipment Corporation, displaying the message "I’m the creeper, catch me if you can!" on users’ teletype screens. In response, Thomas’ colleague, Ray Tomlinson, developed the Reaper program, a self-replicating software designed to hunt down and delete Creeper from the network. Reaper became the world’s first antivirus program and marked the earliest known effort at cybersecurity.



- There are millions of known computer viruses, with some estimates exceeding 1 billion.
- Every day, 560,000 new pieces of malware are detected.
- The global antivirus software market was valued at approximately $4.33 billion in 2024, and is projected to reach $5.6 billion by 2033.

1980s

The 1980s, a decade marked by glam metal, the rise of hip-hop, and Reaganomics, was also a pivotal era for cybersecurity as personal computers became widespread and a diversity of systems emerged. Many users connected through Bulletin Board Systems (BBS), making information sharing easier but also opening the door to new security threats, including the Elk Cloner virus (1982) targeting Apple II computers, the Brain virus (1986) affecting IBM PC-compatible systems, and the Morris Worm (1988), one of the earliest widespread malware attacks created by Robert Tappan Morris. The introduction of the Domain Name System (DNS) in 1983 simplified internet navigation, but security practices, especially regarding password protection, remained weak. Government agencies, however, began recognising the importance of cybersecurity, leading President Ronald Reagan to issue National Security Decision Directive 145 in 1983 to safeguard telecommunications and computer systems.

AIDS Info Disk

The decade also saw the first ransomware attack, the Aids Info Disk, distributed via floppy disk by Joseph L. Popp to World Health Organisation conference attendees, resulting in multiple blackmail charges. Innovation, exploration, and early connectivity defined the 1980s, as individuals began exploiting vulnerabilities out of curiosity or challenge, and cyber espionage emerged when German hacker Marcus Hess used ARPANET in 1986 to infiltrate over 400 U.S. military computers within minutes.

1990s

Along with the birth of grunge music and The Simpsons, the 1990s were defined by the rapid rise of personal computing, the explosive growth of the Internet, and the emergence of cybersecurity as a critical industry. As digital technologies evolved and the web became commercialised, Internet usage soared—and with it, new cybersecurity challenges emerged. Online communities like IRC and America Online (AOL) created opportunities for unauthorised access, social engineering, and distributed denial-of-service (DDoS) attacks.

Setting the stage

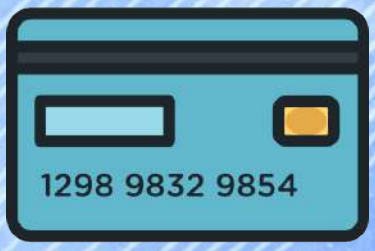
Microsoft Windows, now the dominant operating system, became a major target for malware such as viruses and worms, prompting companies to develop firewalls as a line of defence. The Electronic Frontier Foundation (EFF), founded in 1990, played a crucial role in advocating for digital rights, pushing legal discussions about cybersecurity and personal data protection into the public spotlight, a mission the organization still pursues today. Meanwhile, governments and law enforcement agencies began forming electronic crime task forces to investigate and prosecute cybercriminals, as concerns like the Y2K bug heightened global awareness of system vulnerabilities. Overall, the 1990s laid the foundation for cybersecurity as a serious and evolving field, setting the stage for the complex digital landscape of the 21st century.

Early 2000s

The early 2000s witnessed a massive surge in internet usage, with more than a billion people online by 2005, but cybersecurity was often an afterthought, relying mainly on basic passwords, firewalls, and antivirus software for defence. Hackers during this period were largely motivated by a desire to experiment, build their reputations, or cause disruption, unleashing infamous malware like ILOVEYOU, Code Red, and MyDoom. This era was marked by limited digitisation and minimal regulatory oversight, as slow adoption of digital processes in sectors like accounting meant most financial data remained stored in physical files, making them less vulnerable to cyber threats but still exposed to physical breaches. Meanwhile, regulatory frameworks for the digital world were still in their infancy, with the Data Protection Act of 1998 - one of the few guiding principles for organisations handling personal information - only just beginning to shape early discussions around digital security and privacy.

Data Protection Act 1998

Mid 2000s



The mid-2000s marked a turning point as cyber threats grew more sophisticated, with a sharp rise in malware, phishing attacks, and data breaches prompting organisations to take cybersecurity more seriously by adopting passwords, access controls, firewalls, and antivirus software as standard defences. Hackers began monetising their activities, scamming users through malware like Zeus and Vundo, while botnets such as Storm were deployed to conduct DDoS attacks against firms fighting back against these scams, leading to increasingly organised spam campaigns and the emergence of 'malvertising.' As firms digitised more of their operations, sensitive data became significantly more vulnerable, and breaches often resulted in serious financial and reputational damage, with high-profile examples like TJX, the parent company of TK Maxx, paying out US$41 million in 2007 after 45 million credit card details were stolen. At the same time, companies faced mounting compliance pressure as regulatory bodies began introducing cybersecurity requirements, forcing the industry to strengthen its digital defences and risk management strategies.

2010s

The 2010s witnessed a significant cybersecurity revolution. High-profile data breaches, like the TJX incident in the mid-2000s, shifted cybersecurity to a board-level concern for many organisations. New technologies, such as artificial intelligence and machine learning, were integrated into systems to enhance detection and prevention efforts. As the cybercrime market matured, research from the Home Office in 2018 revealed that sellers of stolen data were earning between £24,000 and £95,000 in profit, while the buyers of this data were making between £6.1 million and £25.2 million from its use.

Ransomware on the rise

Ransomware attacks also became more prevalent, automating the spread of malware and extorting victims. High-profile attacks like WannaCry and NotPetya exposed vulnerabilities in global supply chains, leading to over US$10 billion in damages. This period saw the introduction of more robust cybersecurity measures, including encryption, multi-factor authentication, and secure cloud solutions. As cybersecurity became a specialised function, many organisations began appointing Chief Information Security Officers (CISOs) to oversee their efforts. Recognising the growing importance of cybersecurity, regulatory bodies implemented stricter compliance requirements, such as the General Data Protection Regulation (GDPR), enforced by the Information Commissioner's Office (ICO), which also began issuing penalties for serious breaches of data protection laws. With the rising importance of cybersecurity, the demand for skilled professionals skyrocketed, creating a talent shortage in the field.

The new normal

Today, cybersecurity is integral to the operations of almost every organisation. More companies are adopting a proactive approach, with teams – either in-house or outsourced – that continuously monitor for threats and invest in the latest security technologies like Managed Detection and Response (MDR). As businesses become more reliant on third parties for services, suppliers have also become targets of cyberattacks, with a significant number of recent breaches resulting from supplier vulnerabilities. The growth of remote work during the pandemic has further expanded the attack surface, making it more complex to secure systems and data. As a result, organisations are focusing on securing home networks and educating employees about best practices. Many businesses have migrated to cloud-based software, which offers improved security and accessibility, though these systems must be properly configured and continuously monitored to ensure protection.

10 steps to security

Cybersecurity has undergone significant changes over the past 20 years, driven by advancements in technology and evolving work practices. As emerging technologies like the Internet of Things (IoT), blockchain, quantum computing, and automation continue to develop, we can expect the cybersecurity landscape to keep evolving. It's crucial to stay cyber-aware and take proactive steps to protect your business from a wide range of cyber threats. While cybersecurity technologies continue to advance, the fundamental principles of good cyber hygiene remain unchanged. The National Cyber Security Centre's (NCSC) "10 Steps to Cyber Security" offers a valuable guide on essential controls organisations should implement, including access control, vulnerability management, user training, and vendor management.

zhero

Security insights

Louis Oosthuizen, our amazing Developer, here provides a snapshot of how Zhero is leveraging Managed Detection and Response (MDR) to ease the pain of continuous data monitoring and logging in real time.

Cybersecurity has evolved substantially in the last 10 years. From standardizing endpoint protection to migrate customers from signature-based AV to behavioural based EDR, from heaping logs into a syslog server to categorizing them in a siem solution, migrating on premise Active Directory servers to Cloud Active directories and much more. These changes have brought with it however a massive increase in logging capabilities, making nearly every isolated service capable of reporting on granular activity via logging.

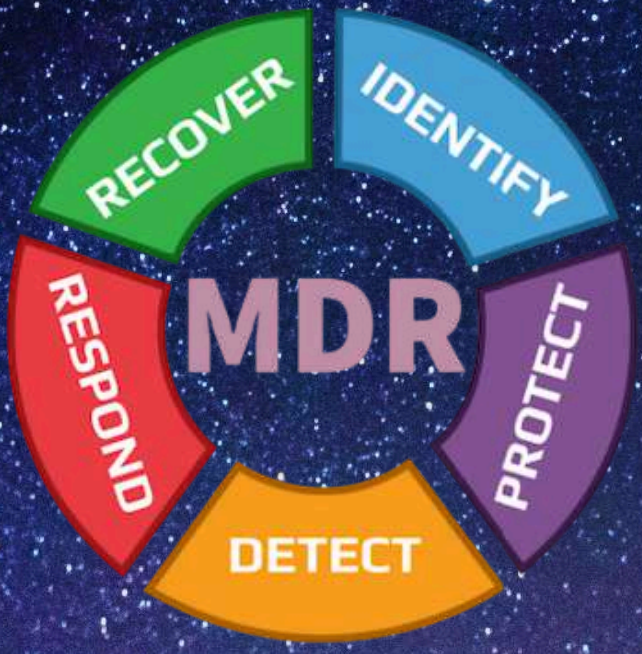
For SOC and NOC teams this has significantly increased the ease of which monitoring, reporting, evidence gathering and so much more can be executed. The negative connotation to this is the sheer number of real-time logs these engineers need to be able to process, categorize and garner sentiment on. This is where XDR to MDR services now have entered the market to ease, standardize and narrow down what is important (and what isn't) and ensure that pro-active and real-time measures can be taken to react on logs i.e., displaying suspicious/malicious behaviour.

zhero

Security insights

,For Zhero Cybersecurity & IT Support this has taken the form of two approaches. To all of our customers, we're developing and using internally formulated XDR services which assist in tracking down suspicious behaviour in our plethora of logs. To customers who have a larger need, as per our recent webinar with the amazing Lewis Pope, we're presenting the incredible technology from N-able Technologies in the form of MDR. This technology supplements not just our own SOC team but also ensures that for these select customers we are able to pull detailed reports on suspicious activity, action on true positive suspicious behaviour in real-time (faster than life) and align customers to our baseline security principles on a higher standard based on their expanded needs.

In short, MDR is breaking down the overwhelming job of sifting through trillions of logs in real-time to ensure that suspicious behaviour is caught faster and as a result acted upon faster.



Earlier this month, Izak, Zhero's Head of Development, Wesley Harris, and our superstar developer, Louis Oosthuizen, had the pleasure of presenting at the N-able Empower conference in Berlin. They were accompanied by Natasha Botha, Head of Finance and Zaheer Rahman, Zhero's Head of Engineering. Izak was a panellist on the "Future Focus: 2025 MSP Horizons Report Panel Discussion", providing future-focused IT and MSP insights to help drive businesses forward. The panel was hosted by N-able CMO Jeff Nulsen, with other panellists including Canalys principal analyst Robin Ody, SYNAXON head of managed services Markus Rex and Infinigate Group CGO Denis Ferrand-Ajchenbaum. Sally-Anne Jones, N-able's EMEA Security Sales Manager, said: "Great to see Izak in Berlin - absolute natural on stage with insights that will definitely support the growth of his peers."

N-ABLE™

Louis led the way at Empower, along with Ben Lee from N-able, and explored how Microsoft is adapting to address the latest IT challenges across enterprises and SMEs. The next day, Wesley was a panellist in the "AI and Automation" panel discussion, joined by Atlee Bols from Red Rhino, Casper Stekelenburg from ICT Concept B.V. and Donald McKay from Kick ICT Group Ltd. Izak said: "@Wesley lol respectfully you were the best .... 👆"

UK C3
UK Cyber Cluster Collaboration

CYBER LONDON

UK CYBER SECURITY COUNCIL

Cyber London CAN

In March, Cyber London was privileged to be part of the Cyber Access Network (CAN). CAN is an initiative of the UK Cyber Security Council in collaboration with UKC3, the UK Cyber Cluster Collaboration. CAN aims to empower and support the next generation of cybersecurity professionals, both students just starting out and career changers exploring new opportunities. Cyber London proudly held three in-person events and two webinars – one for students and the other for employers – to promote and support CAN.

The three in-person CAN events were at City, St George's University of London.

- Unlocking Cyber Careers: Skills, Pathways & Opportunities – featuring Prof. Raj Rajarajan, Security Operations Leader, Anas Amer, and Solmaz Gharoun, the Outreach Ambassador for Cyber London. Zhero's awesome Head of Sales, Twané Janse van Rensburg, made a guest appearance with an inspiring story of career progression.

- Cyber for All: Expanding Opportunities and Breaking Barriers – again orchestrated by Raj, with guest speakers, Harry Hetherington, a key member of the UK Cyber Security Council, cyber trailblazer, Moona Ederveen, and two of Cyber London's directors, Paresh Deshmukh and Mark Child.

- Cyber for Everyone: Real Stories, Real Pathways – led by Cyber London director, Simon Newman, this engaging event featured Matthew Eccles from Action Fraud, a division under the UK's Metropolitan Police, along with Bryan James, General Manager at TR7, Alexandra Forsyth, a threat intelligence specialist, and closing words from Solmaz sharing how she secured internship opportunities.

Meet the team

Wajahat Khan

ONSITE ENGINEER

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

I owned a PC since I was 5, and I enjoyed gaming. That developed my interest in IT primarily, and my passion got me into pursuing a degree in software engineering so that I could learn how to develop games.

What's your most-used productivity tool?

Microsoft Outlook - it keeps my tasks, emails and calendar organized and synced across all devices.

How would you describe yourself?

Adaptable, Solution-focused, Calm under pressure with a strong drive to learn and improve constantly.

What do you enjoy the most about your role?

I enjoy solving real-time issues on site, meeting new clients and contributing to the mission of the Zhero i.e. Crushing IT Chaos.

Do you have any hidden talents or hobbies?

As a youngster, I used to mimic rap songs even though English is not my first language, but still I managed to memorise a lot of songs. Gaming is my hobby, I'm very fond of and I love watching football.

What is your favourite movie or TV show?

My favourite movie is The Pursuit of Happiness starring Will Smith, and TV show is El Marginal, a Spanish crime drama.

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