JUNE 2024

inside zhero

Healthcare
Hackers Delight

Cyber London
Ready Steady Go!

Message from Izak

A warm welcome to this edition of Inside Zhero. It's hard to believe that we are already halfway through 2024!

This month we take another look at that bugbear of mine – ransomware!

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "Healthcare Hacks" focuses on the cyber vulnerability of the healthcare sector and why it is prone to ransomware attacks.

Businesses paid £800 million to ransomware threat actors in 2023.

“Ransomware remains the most severe cyber threat for most UK businesses. These attacks can affect every aspect of an organisation's operations. They can hit finances, compromise customer data, disrupt operational delivery, erode trust, and damage reputations.

The impact is short and long-term, especially for those who are unprepared. Recovery is usually lengthy and costly."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling author

Available Now

HEALTHCARE **HACKS**

The healthcare sector is a prime target for ransomware attacks, creating major patient care and confidentiality challenges. Studies show us that the healthcare industry is the most frequently targeted by these attacks, with over 76% of data breaches in the United States and 81% in the UK involving healthcare service providers.

The prevalence of ransomware attacks in this sector is largely due to the sensitive nature of its data and the potential for substantial financial gains. Providers seldom have room to negotiate as any prolonged downtime poses a potential risk to life. The latest stats show that 38% of attacked UK healthcare organisations pay a ransom demand to get their files back.

Ransomware recap

For those of us with short-term memories, let's do a quick ransomware roundup. According to the UK National Cyber Security Centre (NCSC), ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted. The attackers may also threaten to leak the data they steal.

The stages of ransomware

- **Access** - Attackers gain access to your network. They establish control and plant malicious encryption software. They may also take copies of your data and threaten to leak it.
- **Activation** - The malware is activated, locking devices and causing the data across the network to be encrypted, meaning you can no longer access it.
- **Ransom demand** - Usually you will then receive an on-screen notification from the cybercriminal, explaining the ransom and how to make the payment to unlock your computer or regain access to your data.

There's much more in Izak's international bestseller, You Don't Need a £1 Million Cybersecurity Budget. Now available on Amazon. Here's the link: https://amzn.eu/d/an8OqCU

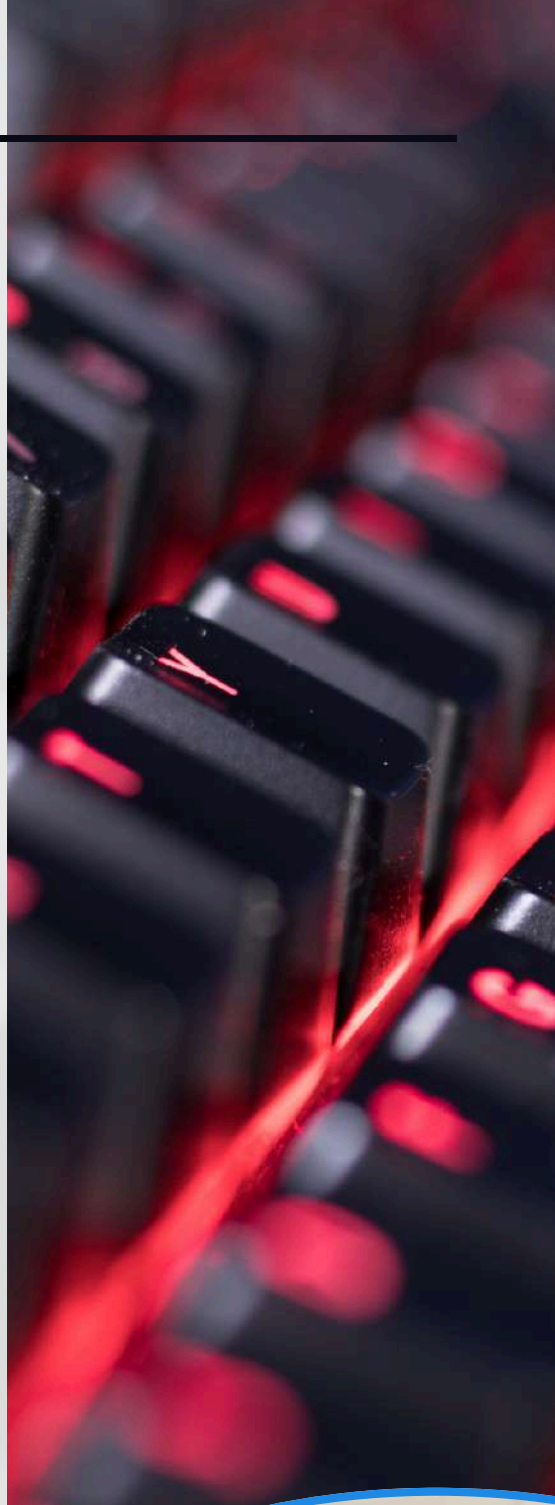
WannaCry 2017

The WannaCry global ransomware epidemic of 2017 was one of the first to impact the UK healthcare system. The attack spread through computers operating on Microsoft Windows, holding users' files hostage and demanding a Bitcoin ransom of $600 for release.

WannaCry affected approximately 230,000 computers worldwide. One of the first companies impacted was the Spanish mobile company Telefónica. By 12 May, thousands of NHS hospitals and surgeries across the UK were affected, with a third of NHS hospital trusts impacted. Ambulances were rerouted, leaving people in urgent need of care stranded.

The attack was estimated to cost the NHS a staggering £92 million, with 19,000 appointments cancelled. As the ransomware spread beyond Europe, it crippled computer systems in 150 countries, causing an estimated $4 billion in losses.

Much of the damage could have been avoided with up-to-date computer systems and better education on the importance of critical software updates.



BlackCat Hack

In June last year, the Barts Health NHS Trust was leaked on the dark web by the infamous Russian ransomware-as-a-service (RaaS) group BlackCat aka ALPHV. The gang claimed to have stolen over 7TB of sensitive data in a cyberattack, including CVs, financial reports, and internal hospital information.

An interesting aspect of this attack is that BlackCat skipped the deployment of ransomware and opted for data exfiltration alone, allowing the NHS to carry on as usual during the ransom period.

Why the attack? Like many parts of the NHS, the health service's cybersecurity requires investment but securing funding for tech projects is often challenging. It is difficult for the NHS to prioritise spending on new technology, leading to outdated and vulnerable IT systems.

Previous victims of BlackCat include the Ecuadorian Army, United States defence contractor NJVC and two German oil companies. Victims end up paying the ransom, which typically ranges from $400,000 to $3 million in cryptocurrency. NCSC CEO Felicity Oswald said:

“The NCSC does not encourage, endorse or condone paying ransoms, and it’s a dangerous misconception that doing so will make an incident go away.”

Dumfries and Galloway

In March, NHS Dumfries and Galloway in Scotland was the subject of a cyberattack and confirmed hackers accessed a significant quantity of data – approximately 3TB - including patient and staff-identifiable information.

The cybercriminal group, Inc Ransom, later released a "proof pack" that included confidential information on a small number of patients and warned that more would follow.

In May, the health board confirmed a large volume of data had been published on the dark web. A Scottish Government spokesperson said:

"The incident remains contained to NHS Dumfries and Galloway and we continue to provide support as they deal with this situation. This remains an ongoing police investigation."

DID YOU KNOW?

70% of attacks result in data encryption

NHS Synnovis attack

At the beginning of this month, hackers believed to be the Russian cybercriminal gang Qilin, launched a ransomware attack against a key NHS partner and third-party supplier, Synnovis. Synnovis is a company that helps manage blood transfusions and lab services for hospitals under the Guy's and St Thomas' NHS Foundation Trust and the King's College Hospital NHS Foundation Trust.

The attack crippled services at these hospitals and they were unable to carry out blood transfusions.

"This is a significant attack affecting a third-party supplier. As large organisations improve their cyber security, criminals look for vulnerabilities in the supply chain. The problem is so prominent that the NCSC recently published revised guidance on securing supply chains."

Simon Newman
Cyber London

The immediate impact

The London hospitals were forced to revert to using long-abandoned paper records, with porters hand-delivering blood test results because of IT network disruptions. Despite the large-scale ransomware, Synnovis, which analyses blood tests for the NHS, continued its work. The ransomware attack also increased the need for O-type blood donations, with this type being universally safe. Since blood only lasts 35 days, stocks must be continually replenished. Patients were also impacted. Professor Stephen Powis, the Medical Director for NHS England, said:

“Many operations and appointments have been postponed or diverted to other neighbouring hospitals not impacted by the cyber-attack, as we prioritise pathology services for the most clinically urgent cases.”

What do the attacks mean?

The NHS, which serves the UK's 68 million residents through 229 trusts, faces significant cybersecurity challenges, as highlighted by the WannaCry incident in 2017 and recent attacks like BlackCat, Inc Ransom, and Qilin. This extensive network makes the NHS the custodian of one of the richest and most comprehensive national health datasets globally. With 1.7 million employees, the NHS is also one of the world's largest employers, surpassed only by the U.S. and Chinese militaries, Walmart Inc., and McDonald's Corp. Such scale makes it an attractive target for financially motivated cybercriminals

Preventative measures

The NHS breaches serve as a bleak reminder that all organisations – big and small – need robust cyber defences and continuous vigilance. So how could this enormous healthcare provider have avoided these attacks? A combination of these proactive measures would be a step in the right direction: regular and comprehensive employee training on cyber hygiene, stringent access controls, timely software updates, and an investment in advanced threat detection systems.

By fostering a culture of cybersecurity awareness and implementing best practices, the NHS can better protect itself against future threats, ensuring the security and privacy of patient data remain uncompromised. Cybersecurity is not just a technical necessity but a fundamental aspect of maintaining public trust in healthcare systems.

Future ransomware trends

- **Targeted attacks** - Expect more ransomware attacks on specific industries like healthcare, finance, and critical infrastructure, with hackers doing their homework to find the most valuable targets.

- **Double extortion tactics** - More cases where attackers not only encrypt data but also steal it, using the threat of leaking or selling it to pressure victims into paying up.

- **Supply chain attacks** - More attacks on supply chain partners by exploiting weak spots in third-party software or services to get to the main target.

- **RaaS evolution** - RaaS models will keep evolving with better encryption, evasion techniques, and even customer support to make ransom payments and data recovery easier for victims.

A global phenomenon

Cisco Systems Inc.'s Talos threat intelligence division tells us that healthcare providers were the most targeted by ransomware gangs last year. This is due to the sector's generally underfunded cybersecurity budgets and low tolerance for downtime.

Cybercriminals have repeatedly breached various parts of the healthcare sector, from major hospital systems to one of America's largest health insurance companies.

Last year, the FBI received more reports of ransomware attacks in healthcare and public health than in any other of the 16 critical infrastructure industries.

"When healthcare systems and data are unavailable, lives are potentially at risk. This makes the sector a tempting target for criminals. Outages put pressure on management to pay off the attackers to restore availability quickly."

Martin Lee
Cisco

Cyber London 2024

On Friday, 21 June, Zhero proudly participated in the official launch of **Cyber London** at City, University of London. Cyber London is a non-profit organisation whose focus is on helping the cyber industry innovate, share best practices and develop effective partnerships to build a healthy cybersecurity ecosystem.

Hosted by one of the venerated Directors, Simon Newman, the launch was packed with interesting and insightful presentations and lively discussions. The event focused on how innovation through collaboration will pave the way to make London a global centre of excellence for cyber. Izak, along with Simon, Paresh Deshmukh, CEO of Baseel and David Weeks, VP of Partner Experience at N-able, participated in a razor-sharp panel on the current state-play play of cybersecurity in the UK.

Sponsored by Zhero, N-able, Mastercard and others, the launch was an unforgettable day of learning, sharing and networking. With its emphasis on community and developing skills for tomorrow, Cyber London will surely go from strength to strength as it impacts London's tech landscape. Exciting times are ahead and we can't wait for what happens next!

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Marc van Romburgh

SERVICE DESK COORDINATOR

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

I was extremely into gaming. I watched a YouTube channel called Linus Tech Tips and discovered my love for the IT industry.

What's your most-used productivity tool?

It's Google because it is an amazing source of knowledge and information.

How would you describe yourself?

I'm patient, professional and content.

What do you enjoy the most about your role?

As a Service Desk Coordinator, I love the people I work with.

Do you have any hidden talents or hobbies?

I play the guitar, bass guitar and drums and build custom gaming computers as a hobby.

What is your favourite movie or TV show?

The crime drama series, Monk, with Tony Shalhoub. I watched it on as a kid and that it is available on Netflix I am watching it again.

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

zhero
crush the chaos