SAFHE 2026
SOUTHERN AFRICAN HEALTHCARE CONFERENCE
SYNERGY IN ACTION: SHAPING THE FUTURE OF HEALTHCARE TOGETHER

9 – 10 JUNE 2026
CTICC 2 CAPE TOWN

The Cyber Threat Landscape of the Medical Sector in SA

MC Bekker

Introduction

What is the outlook for Cyber Security Trends for the Medical sector – both Globally and Locally?

I work at Orange Cyberdefense South Africa, and we have been part of the South African and Global Cybersecurity community for the past 26 years, and never in the history of the internet has there been as much rapid change as now, the Connected World is changing, we have Cloud, internet connections any place on earth, more computer power in your pocket than you had In your laptop 15 years ago.

Today, I will be talking about this change, and what does it mean for the Medical industry, and I will try to give you some advice on how you can harness this change and be more secure.

CYBERCRIME IS BUSINESS

Cybercrime is big business
But how big?

150 new domains are registered every minute*

Attackers are hiding in the noise

Business Email Compromise costs companies on average just over $4.5k per minute*

Orange Cyberdefense took down over 50,000 websites last year

Nearly 30 attempts to takeover corporate social networking accounts occur per year for each institution**

Over the past 10 years, there have been 300 data breaches involving the theft of 100,000 or more records***

Cybercrime would be the world's third-largest economy after the US and China****

Sources:
* Cyberthreat Minute: The scale and scope of worldwide cybercrime in 60 seconds, microsoft.com
** zerofox.com
*** forbes.com
**** Cyberwarfare in the C-Suite, Cybercrime Magazine

4

Recent Cyber attacks in South Africa

NATIONAL HEALTH LABORATORY SERVICE

Ransomware Attack on NHLS in 2024.

In mid June 2024, the Blacksuit Ransomware operator successfully Ransomwared the NHLS – leading to extended downtime, system outages and effectively stopping critical medical services to be rendered.

Access – Social Engineering –> phishing emails
Root cause –> Outdated systems and controls, weak credentials
Additional contributing factors –> not having adequate plans in place for Cyber Security Incidents.

Impact: Severe and the damage was Critical

Impact – Severe/Critical

Currently unquantifiable in Rands and Cents, but 1000's of hours lost, patients not receiving the right care timeously due to the service being offline, alternative services overwhelmed.

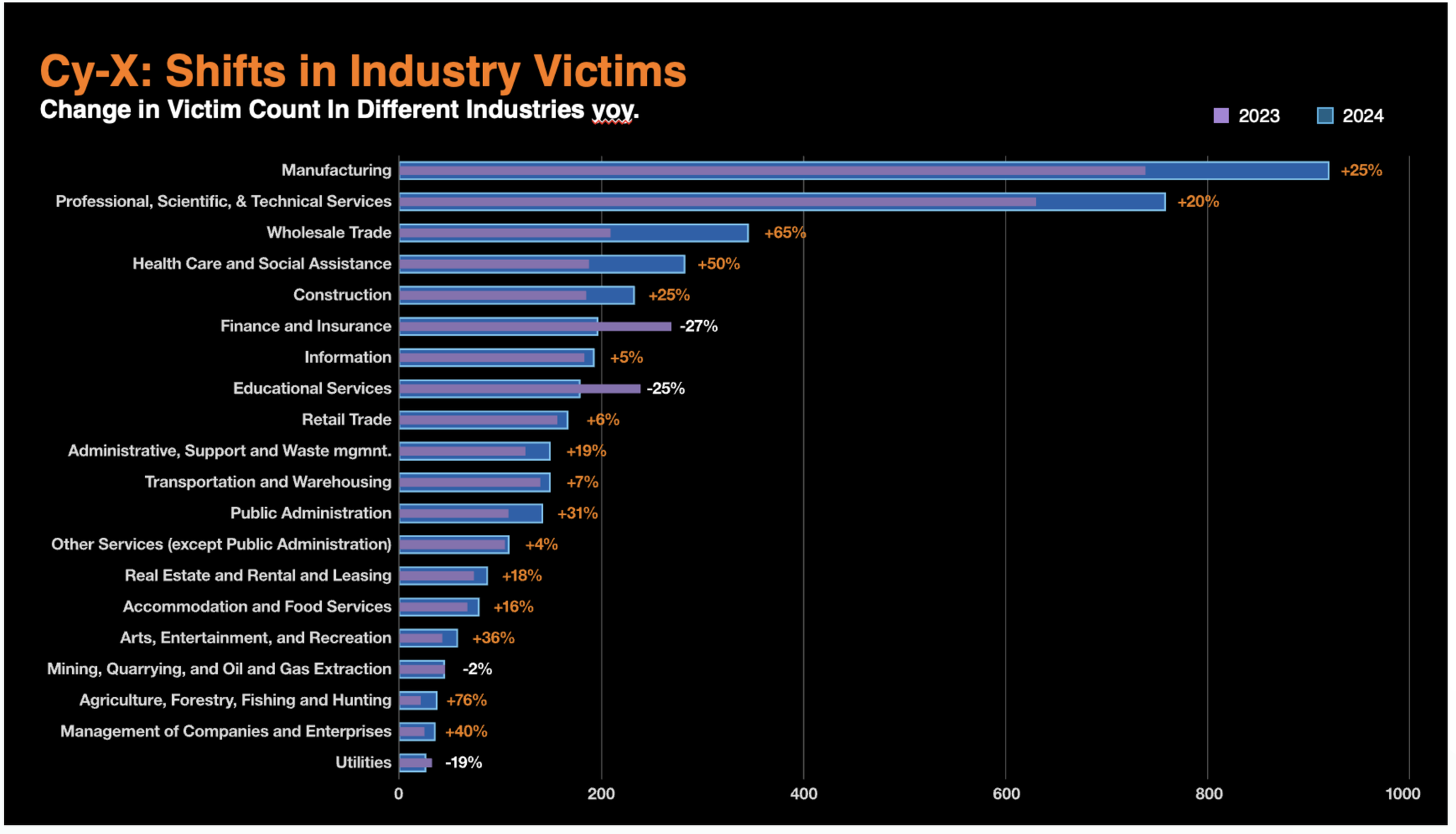
The Evolution of Cyber Extortion – (CyX)

Cyber Extortion (Cy-X) Definition and explanation

Cyber extortion (Cy-X) attacks have become increasingly prevalent in recent years, posing a significant threat to organizations of all sizes and industries. These attacks involve threat actors gaining unauthorized access to a victim organization's IT network and data, then threatening to publish, encrypt, or destroy the data unless a ransom is paid. They can take various forms, including ransomware attacks, where attackers encrypt a victim's data and demand a ransom to provide the decryption key, or distributed denial of service (DDoS) attacks, where they flood a victim's website or network with traffic to disrupt their operations until a ransom is paid

Cy-X: Shifts in Industry Victims

Change in Victim Count In Different Industries yoy.



What is the Risks?

All Cyber incidents has a cost involved – some significant as shown in the initial examples.

Operational – Besides the financial cost, there is also the impact to day-to-day operations – bookings, files, billing etc, think of all the critical business operations tied to IT and IT Systems?.

Legal Risks – There is legal implications – POPIA, the Information regulator, Possible damages claims from victims, the new Cyber Crimes Act

Ethical Risks – Ethical considerations and risks as per the HSPCA guidelines include:

Booklet 5 (Confidentiality: Protecting and Providing Information): This guideline details the practitioner's responsibility to protect patient information from unauthorized disclosure.

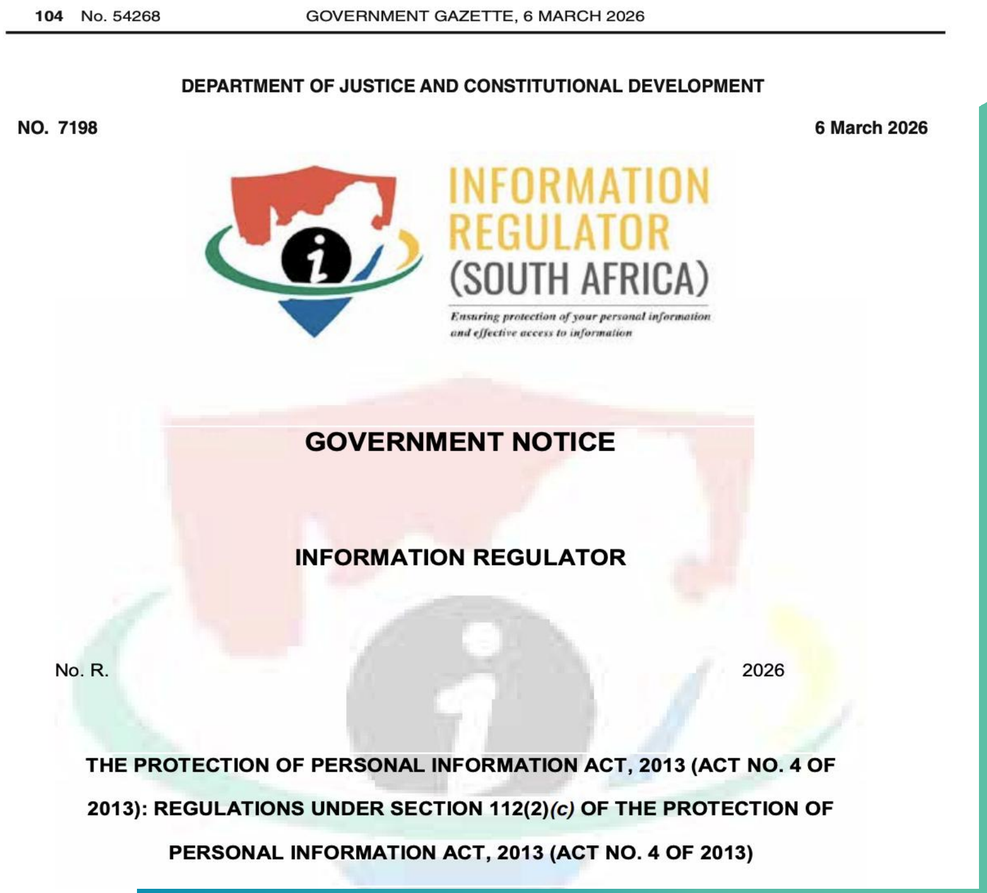
Booklet 9 (Guidelines on the Keeping of Patient Records): This outlines requirements for creating, maintaining, storing, and disposing of patient records, emphasizing security and confidentiality

Ethical Rule 27A: States that a practitioner shall at all times act in the best interests of their patients, which includes respecting patient confidentiality, privacy, choices, and dignity.

POPIA regulation update

In March 2026 – the Information Regulator of South Africa

Published and enacted- these updates and amendments to the POPI-Act is to clarify and assist organizations in interpreting section32(6) of the Act and provides a Framework for Enforcement by the Regulator.



104 No. 54268 GOVERNMENT GAZETTE, 6 MARCH 2026

DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 7198 6 March 2026

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

GOVERNMENT NOTICE

INFORMATION REGULATOR

No. R. 2026

THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013): REGULATIONS UNDER SECTION 112(2)*(c)* OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Link:
https://www.gov.za/sites/default/files/gcis_document/202603/54268gon7198.pdf

Updated Regulations – Medical Records

5. Appropriate safeguards

5.1. The responsible party that processes health information shall be responsible for maintaining the confidentiality, integrity and availability of such information in its possession or under its control by taking appropriate, reasonable technical and organisational measures in accordance with section 19(1) of the Act to prevent:

5.1.1. Loss of damage to or unauthorised destruction of health information; and
5.1.2. Unlawful access to or processing of health information.

5.2. The safeguards to be maintained under sub-regulation 5.1. must include appropriate measures for -

5.2.1. the security and confidentiality of records, which measures must address the risks associated with physical or electronic health records; and

5.2.2. the proper disposal of health records to prevent any reasonably anticipated unauthorised use or disclosure of the health information or unauthorised access to the health information following its disposal.

5.3. Processing of health information must be undertaken subject to a duty of confidentiality imposed by law, office, employment, profession, or written agreement, as contemplated in section 32(2) of the Act.

5.4. The responsible party must implement and maintain appropriate and reasonable technical and organisational measures to ensure the integrity and confidentiality of health information, in line with generally accepted information security practices applicable to its sector or industry, as contemplated in section 19 of the Act.

While the Appropriate and reasonable technical measures are not explicitly defined, the regulator has been building enforcement capacity the last 5 years.

ISAC HEALTH Threat Report

The ISAC Global Health Sector Threat Landscape Report -

Comprehensive Study from over 250 members of HEALTH -ISAC (Information Sharing and Analysis Centers) – which covers Hospitals, Medical Service Providers, Insurance Providers, and medical device manufacturers.

Link: https://health-isac.org/annual-threat-report-health-sector-2026/

What is the Top 5 Threats?

Survey Findings

Health Sector Security Professionals ranked the top five cyber threats facing their organizations in 2025 as follows:

1. Ransomware Deployments
2. Phishing Attacks
3. Third Party/Partner Breaches
4. Data Breaches
5. Zero-Day Exploits

Health Sector Security Professionals ranked the top five cyber threats facing their organizations, looking ahead toward 2026, as follows:

1. AI-Enabled Attacks
2. Ransomware Deployments
3. Third Party Breaches
4. Zero-Day Exploits
5. Phishing/Spear Phishing

What is the Top 5 Threats - Continued

Medical Device Manufacturers reported the top three challenges in developing secure medical devices such as:

1. Integrating security into the design and development process
2. Providing regular and secure updating and patching for medical devices
3. Designing for the ongoing security of medical devices over their long operational lifespan

Conversely, the top three impacts on Healthcare Delivery Organizations were reported as:

1. Disruption in the normal operation of medical technology
2. Unauthorized access, theft, or exposure of patients' personal health information (PHI)
3. Disruption of overall hospital operations, including administrative processes, scheduling, and communication

How does AI Feature into all of this?

AI is here to Stay, and has changed the World forever, brining innovation and progress, but also Risks.

AI is not just a future risk, and it is not just a productivity tool. It is already changing how adversaries operate and what the enterprise must protect. Both Sides, Attackers and Defenders are Using AI, but what does this mean Practically?

New Vulnerabilities are discovered at a rate never seen before – especially in legacy systems – think about that for all your environments, Systems and IOCD (Internet of Connected Devices).

We are developing more code everyday, than any day before, but it does not mean that code is secure – we are seeing vulnerabilities we have not seen in years.

The Impact of AI - Practically now:

#1 Social engineering:

Attackers continue to find innovative ways to manipulate victims to perform malicious actions that circumvent or weaken security controls. What's already worked before can now be transformed into any representation, language, or style. This ability to synthesize new content allows attackers to adapt around their target environment with little effort. In April 2026, for example, the Microsoft Defender Security Research team shared information relating to an AI-enabled phishing campaign that steals authentication tokens[3].

#2 Deepfakes and cognitive persuasion:

The ability for attackers to mimic a real person's features enables them to introduce more believability into their social engineering attack. Attackers can use fake voice, video or images along with fabricated narratives to spread and amplify disinformation. In early 2024, for example, the Arup group revealed that they lost $25 million in a fraud case that involved deepfakes[4]. Apart from the direct threat of scams, these insidious attacks can erode essential pillars of trust. The ability of attackers to distort our reality will put strain on societies as we struggle to discern what is true.

#3 Vulnerability crunch:

Improved LLM capabilities are now also democratizing abilities like vulnerability discovery and exploit writing. For example, a researcher published findings showing how they spent $2,283 using Claude Opus to find a vulnerability and build a working exploit impacting Google Chrome[5].

The Impact of AI - Practically now:

#4 Scaling malicious capability is virtually free:

Between December 2025 and February 2026 an attacker used Claude Code and GPT 4.1 in cyberattacks against 9 Mexican government agencies to exfiltrate data[6]. Anyone can now use LLM tools shaped by playbooks or harnesses to orchestrate multiple agents. These harnesses are getting more capable with each iteration and are widely shared. Parallel attack streams with minimal participation allow attackers to industrialize the cyber-kill-chain with a few carefully chosen prompts.

#5 Subversive behavior:

As humans remain susceptible to manipulation, so do LLMs. Agentic AI is driven by LLMs and thus creates the potential for attackers to change the intended behavior of the system. Agentic systems ingest data from everywhere and can expose valuable corporate resources, resulting in leaked information and malicious actions. The complex systems required to build, host, maintain, authorize, expose and integrate AI systems all increase the attack surface in complex and nuanced ways, each with significant risk implications. At the same time more code is being generated at a faster pace. The assumption that the code will bug-free will be tested continuously. Ask Straiker, who disclosed in April 2026 that they discovered an indirect prompt injection in Cursor AI that permits remote tunneling and remote shell[7].

So what Should we do?

Cyber risks affects all in the Medical Industry – and fitting with the Theme for the conference:

SYNERGY IN ACTION:

All Teams, role players and participants will have to work together to address the Cyber Risk,and implement effective Controls.

That means, SHIFTING security left – Making it part of from the Beginning and building in Cyber Security Standards and baselines from the design and planning phase.

Building in Compliance with Procurement – Finance and Operations teams.

Using AI as an enabler to increase security effectiveness.

SAFHE 2026

SOUTHERN AFRICAN HEALTHCARE CONFERENCE

SYNERGY IN ACTION: SHAPING THE FUTURE OF HEALTHCARE TOGETHER

Thank you / Q&A