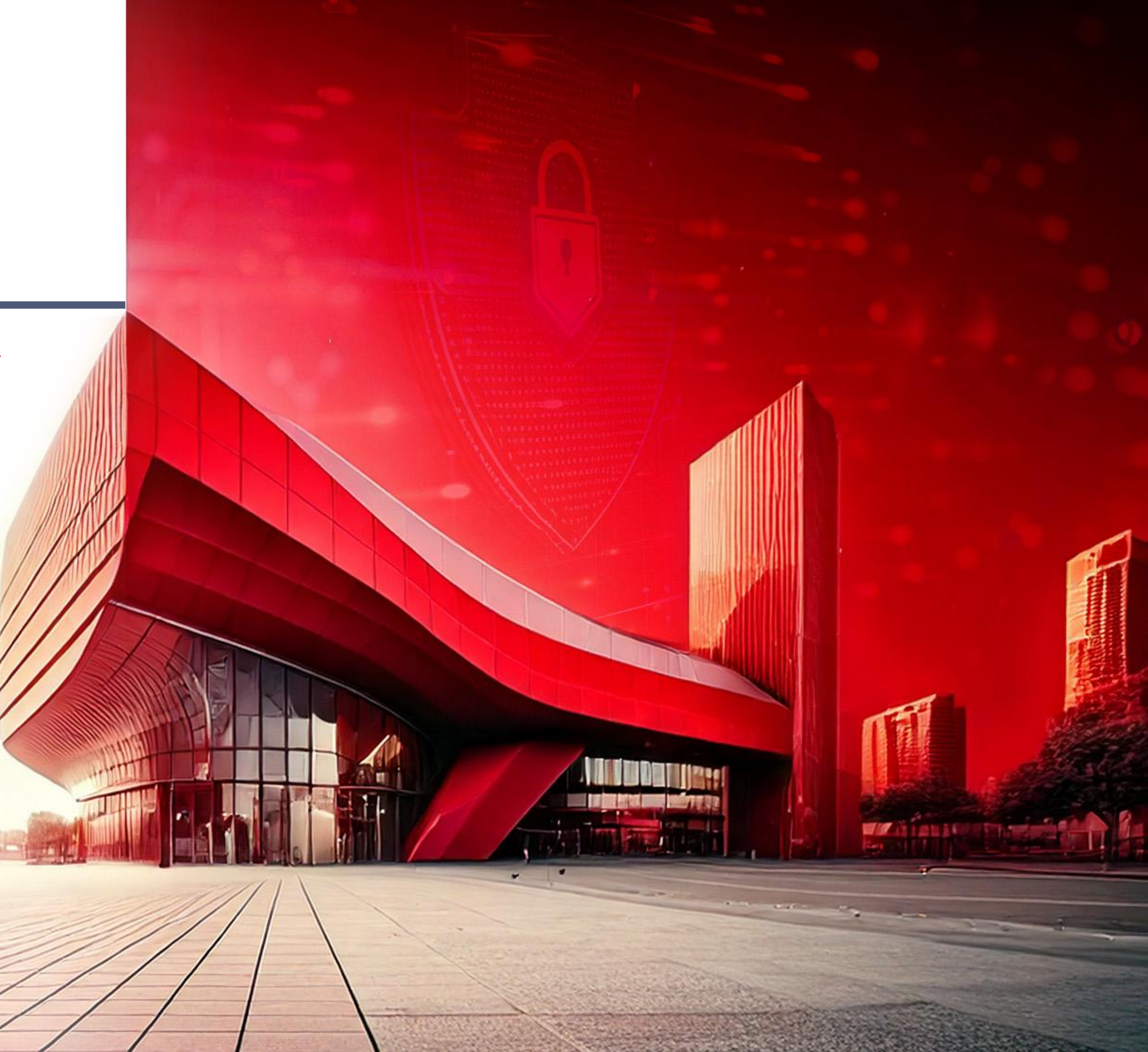
ACTUARIAL SOCIETY OF SOUTH AFRICA

Advancing Actuarial Excellence

# CYBERSECURITY

## A STRATEGIC RISK IN HEALTHCARE

May 2026



# 01

## CYBSERSECURITY’S NEW FRONTIERS

Speed, Scale and Ecosystems

ACTUARIAL SOCIETY OF SOUTH AFRICA

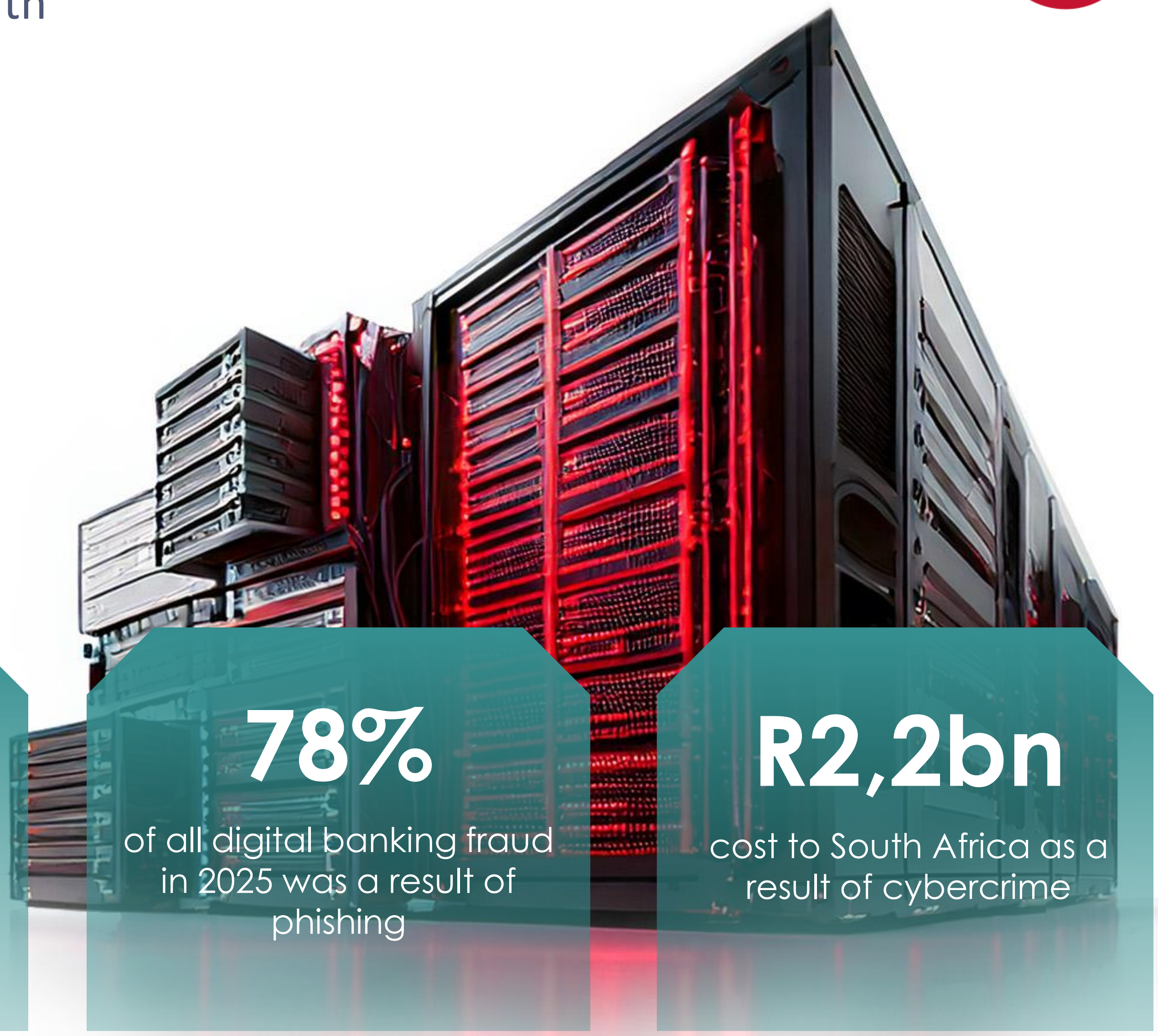
Advancing Actuarial Excellence

Educate • Develop • Uphold

# 01 Cybersecurity is a top global risk with South Africa amongst the most targeted

## South Africa is a high-value, high-frequency target…

**40%** of South African businesses experienced at least one ransomware attack in the last 12 months with an average cost of R49,5m



**#1**
Cyber cited as top business risk across most industries

**Top 10**
Cyber remains one of the WEF's top 10 global risks in 2026 despite mounting geopolitical crises

**78%**
of all digital banking fraud in 2025 was a result of phishing

**R2,2bn**
cost to South Africa as a result of cybercrime

**Allianz Risk Barometer 2023; EY Banking CRO survey 2023; WEF Global Risk Report 2026; Africa Outlook 2026; Interpol 2026 Africa report; South African Banking Risk Information Centre

# 01 Cybersecurity is a top global risk with South Africa amongst the most targeted


### Standard Bank
**Data Breach**

March – April 2026


### Alexforbes
**Business Email Compromise**

April 2026

### TransUnion
**Repeat Data Breaches**

2022 - 2025

**SARB:**
"cyber attacks present a systemic danger to South Africa's financial stability"

"Cyber risk behaves like a systemic operational shock and amplifies single points of failure"

**Prudential Authority:**
"Joint Standards set the floor not the ceiling for cybersecurity and cyber resilience"

# 01 Cybersecurity is now about speed, scale and ecosystem trust

**01** Ransomware remains the dominant threat – but it has evolved

**02** AI is dramatically accelerating both attacks and defence

**03** Supply-chain and third-party attacks are primary scale vector

**04** Identity and cyber hygiene are the main attack surfaces

# 02 'SO WHAT' DOES THIS MEAN?

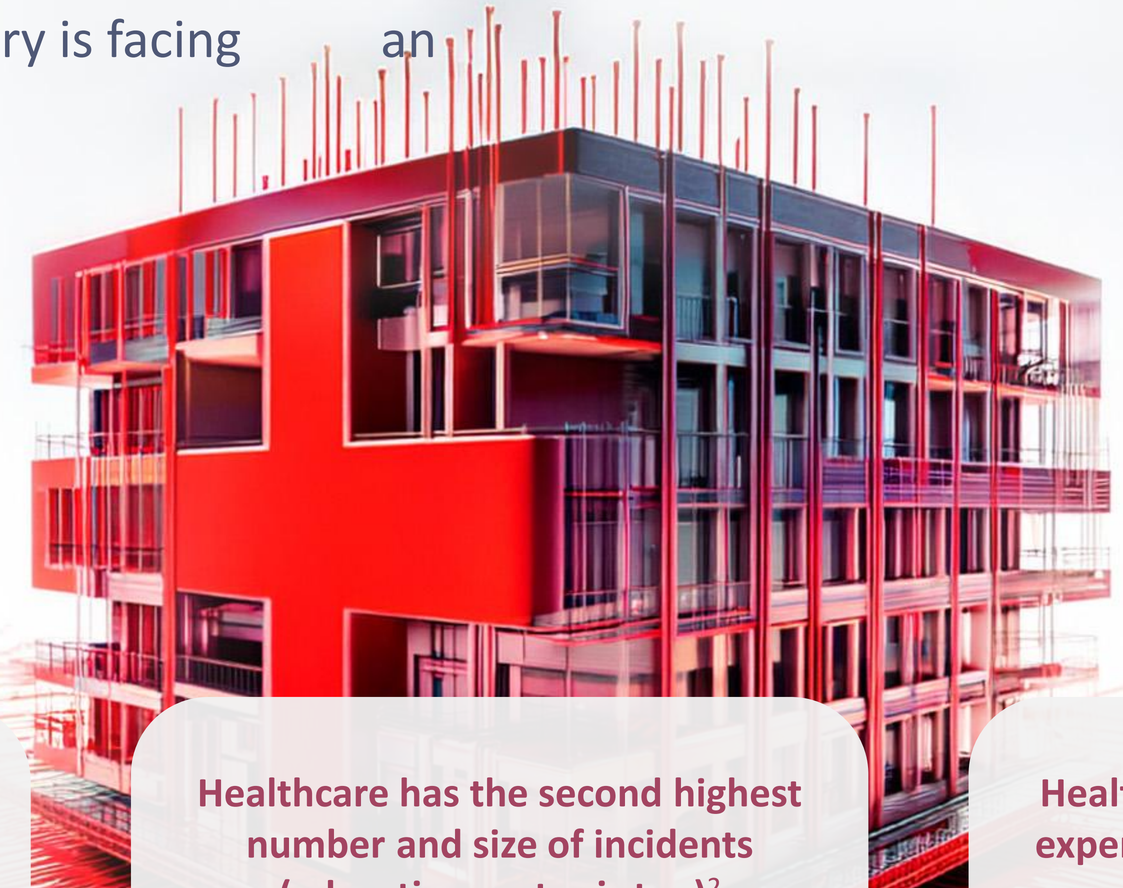
## Impact on the Healthcare Industry

ACTUARIAL SOCIETY OF SOUTH AFRICA

Advancing Actuarial Excellence

Educate • Develop • Uphold

# 02 The Healthcare industry is facing an onslaught



[1] IBM 2024 Cost of Data Breach Study
[2] Verizon Data Breach Investigations Report
[3] IT-Online

### Average cost of a healthcare data breach is highest of all industries

$10.93 million compared with $5.9 million for financial sector[1]

### Healthcare has the second highest number and size of incidents (education sector is top)[2]

1,378 incidents, 1,220 with confirmed data exposure per year
Personal data is the preferred target

### Healthcare organisations in Africa experienced a 38% YoY increase in cyber attacks[3]

3,575 cyber attacks per week in 2024
Africa recorded the highest average weekly attacks globally

# 02 The Healthcare industry is facing an onslaught

**NHLS**

**Ransomware Attack**

2024 - 2025

**Lancet Laboratories**

**POPIA Breaches**

2024 - 2025


**Mediclinic**

**Cyber Extortion**

2025

**Civil Claims:**
“there is an emerging liability inflation risk linked to maturing of class actions and civil claims”

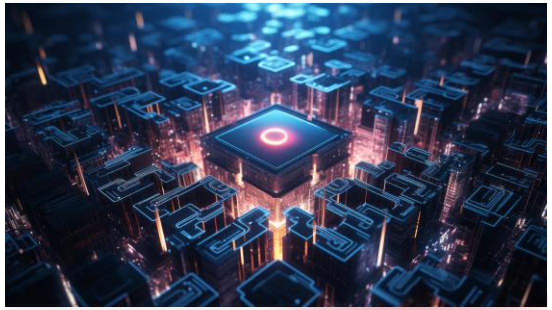
**Information Regulator:**
“There is no low risk breach under POPIA”

**Regulators:**
SA has world class regulations and laws but they still lag the pace of change

# 02 And the Healthcare industry is uniquely exposed

| | |
|---|---|
| High-value, highly sensitive data | Care delivery disruption |
| Complex service delivery | Data compromise |
| System constraints | Financial shock |
| Always-on operations | Trust impact |

# 02 Which has actuarial implications



**Capital**

Cyber risk creates volatility & accumulation risk

**Pricing**

Cyber costs increasingly embedded

**Sustainability**

Cyber risk erodes trust & system viability

**Resilience**

Cyber events are stress tests of healthcare system

# 03 'NOW WHAT' SHOULD WE DO?

## Responding Effectively and Responsibly

ACTUARIAL SOCIETY OF SOUTH AFRICA

Advancing Actuarial Excellence

Educate • Develop • Uphold

# 03 What should we do: responding responsibly

| | | |
| --- | --- | --- |
| 01 | **Recognise cyber risk as an enterprise and system risk** | Move cyber risk out of the “IT register” and into enterprise risk management |
| 02 | **Define what “resilience” means in business terms** | Stop asking “Are we secure?” instead ask “What level of disruption can we tolerate?” |
| 03 | **Incorporate cyber risk into capital, pricing and stress testing** | Make cyber risk financially visible |
| 04 | **Strengthen response readiness not just prevention** | Prepared response reduces harm more reliably than perfect protection |

# 03 **Ecosystem:** Act responsibly across the value chain

### Share

Cyber risk is a shared responsibility that cannot stop at organisational boundaries

Encourage sector-level collaboration and information sharing

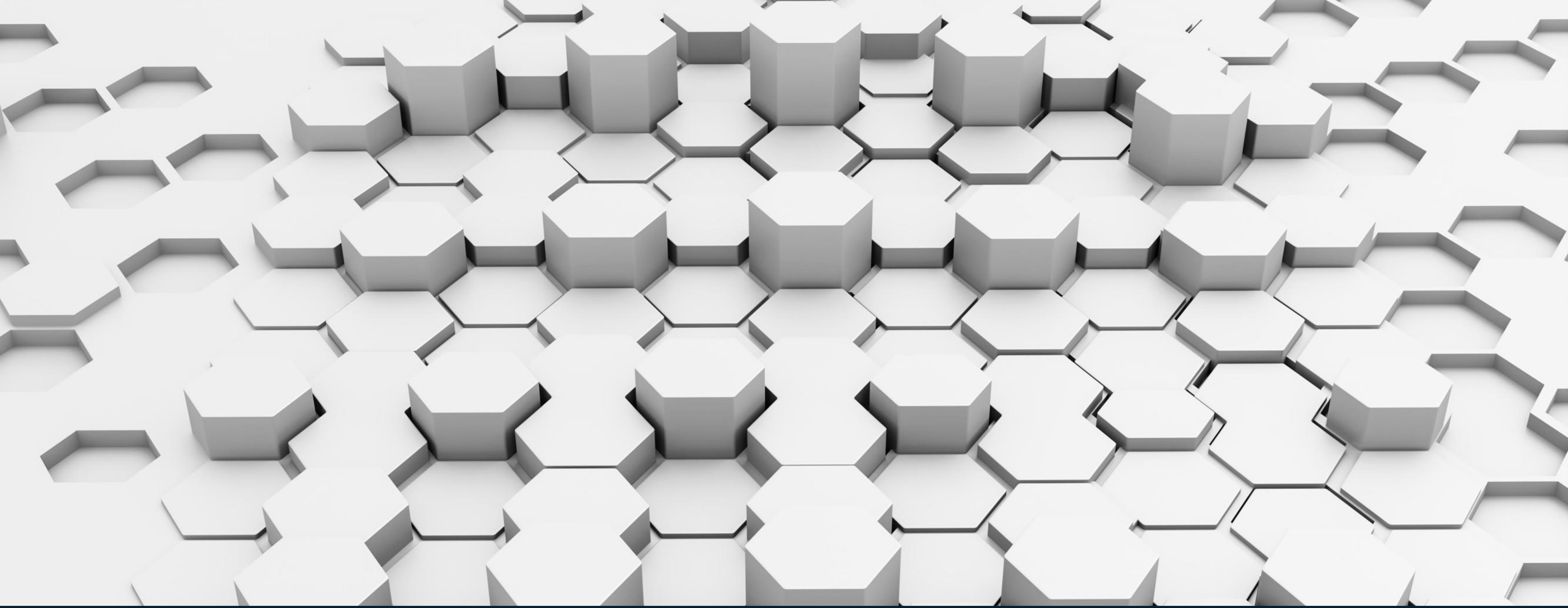
### Evidence

Require evidence of cyber resilience (not just policies) from all ecosystem players across the full healthcare value chain

### Coordinate

A fragmented response creates fragility

Sector resilience depends on a coordinated response across the value chain



# Thank you

ACTUARIAL SOCIETY
OF SOUTH AFRICA

Advancing Actuarial Excellence

Educate • Develop • Uphold