02 June 2026

Keynote address: Securing the Digital State:
Advancing Cyber Resilience in the Public Sector

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Mathabo Nakene-Mginqi
University of South Africa

www.cigfaro.co.za

SAQA Recognised Professional Body

KEYNOTE ADDRESS

Securing the Digital State

Advancing cyber resilience in the public sector

Securing the digital state is not, at its heart, a technology problem — it is a leadership problem.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Mathabo Nakene-Mginqi · University of South Africa · 02 June 2026

FROM STRATEGY TO EXECUTION

The leadership discipline

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

A repeatable chain — each step earns the next. Done in order, the gap between where you are and where you want to be becomes your roadmap.

01

Anchor the strategy

Tie every security objective to an institutional objective it protects or enables.

02

Build the plan

Translate targets into sequenced, resourced, owned interventions.

03

Choose the standards

Hold yourself accountable — for us, ISO 27001 and the NIST framework.

04

Assess maturity

Score honestly, 0–5, across the six NIST functions to set a baseline.

05

Derive the roadmap

The distance from today to target, sequenced by risk and dependency.

06

Execute, item by item

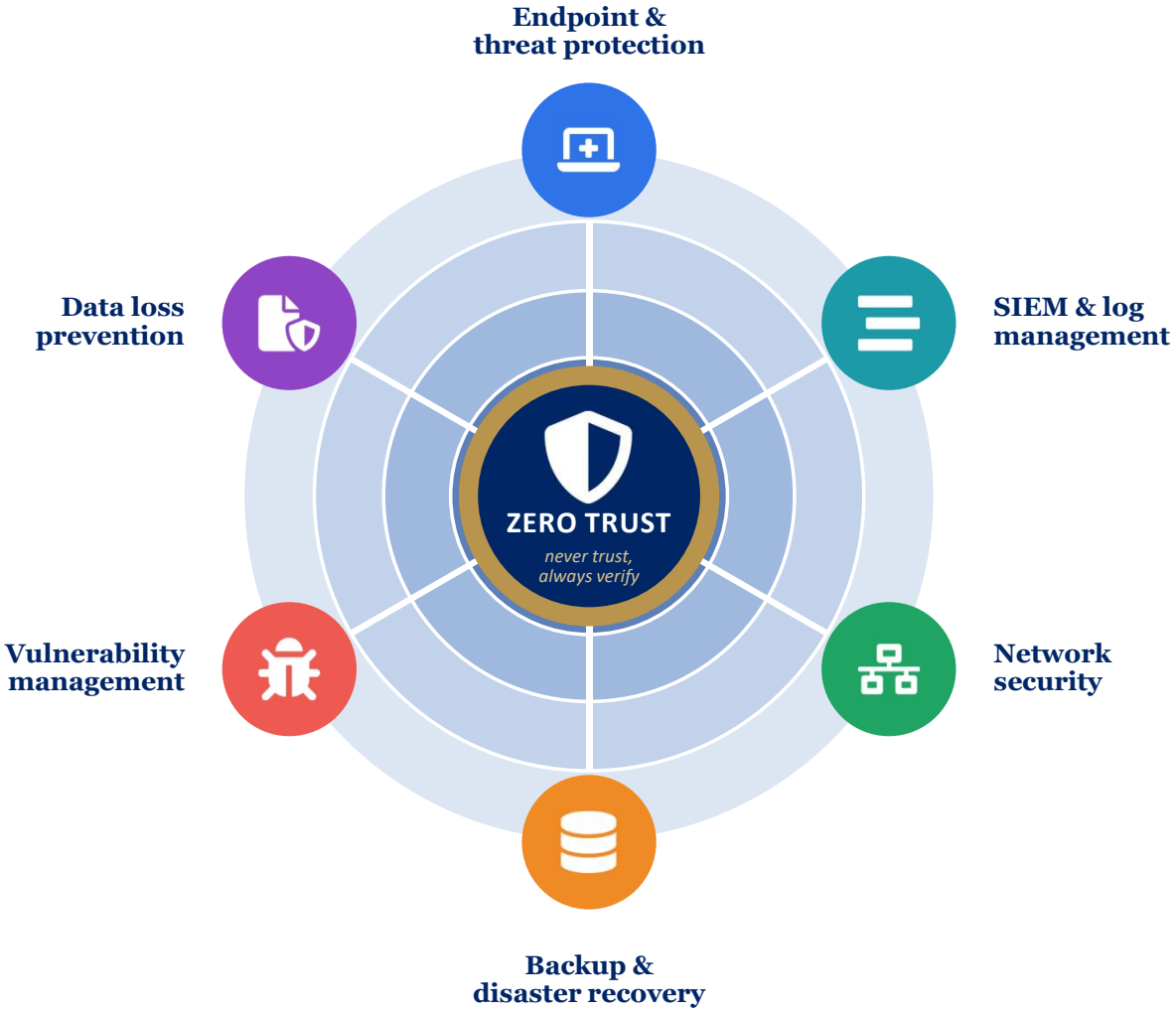
Close one control gap, then the next — and monitor what is already done.

BUILDING RESILIENCE DELIBERATELY

A layered software ecosystem

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

No single tool makes you secure. Resilience is built by layering defences under one principle — zero trust — then using AI to turn the data they generate into focused action.



Defence in depth — layers wrapped around a zero-trust core, each covering what the others cannot.

AI-DRIVEN PRIORITISATION

A layered ecosystem generates more alerts, logs and signals than any team could read. AI cuts through the noise to find what matters.

Hone in on the 20%

of interventions with the highest strategic impact — focus, not overload.

LEADERSHIP & STAKEHOLDER ENGAGEMENT

The multi-factor authentication story

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Identity was our single largest source of incidents. The right control was obvious — and contested.

The problem

Compromised credentials — identity-based attacks, our biggest exposure.

The pushback

Sustained pressure from executive peers to delay, dilute, or roll MFA back. It was lonely to hold the line.

The decision

A correct control that is hard for the customer is a reason to make it easier — never to abandon it.

THE RESULT

90%+

reduction in identity & access management incidents

From my most contested decision to one of our most decisive wins — held by engaging stakeholders again and again, not just once.

WHAT YOU MUST KEEP EXERCISING

Three leadership muscles

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Not projects you complete — muscles you build, test and strengthen for as long as you hold the role.

01

Stakeholder engagement

- Security is no longer 'IT's problem' — own it across the institution.
- Keep engaging after the decision, not only at launch.
- The day you stop is the day hard-won decisions unravel.

ENGAGE AGAIN AND AGAIN

02

Intentional education & awareness

- Tailored to your maturity roadmap and the student mindset.
- Back-to-basics or sophisticated — always responsive.
- Five adoption strategies; ~80% of ransomware now uses AI.

MAKE IT EASY TO DO RIGHT

03

Communication via governance

- Regular, honest reporting through Senate and structures.
- Challenges, interventions, and what to watch — by the numbers.
- People support what they understand.

BUILD TRUST BEFORE YOU NEED IT

All three are leadership — not technology. They are the scarce resource only we can supply.

FROM THE INSTITUTION TO THE NATION

Cyber sovereignty: a strategic imperative

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

As AI moves into identity, tax, grants, health, policing, energy and finance, the leadership question scales up to the nation.

THE SOVEREIGN CONTROL DOMAINS

01

Cryptographic control

Sovereign key custody for national-critical workloads. If we cannot hold the keys, our sovereignty is conditional.

02

Operational visibility

Telemetry, security logs, audit rights and model-behaviour insight — or oversight is merely decorative.

03

Strategic exit

Portability, recovery and exit rights. If a workload cannot move, dependency is built into the architecture.

Sovereign cybersecurity creates control — *and choosing to build it is a test of leadership.*

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body