03 June 2026

Building a skilled cybersecurity workforce for the public sector

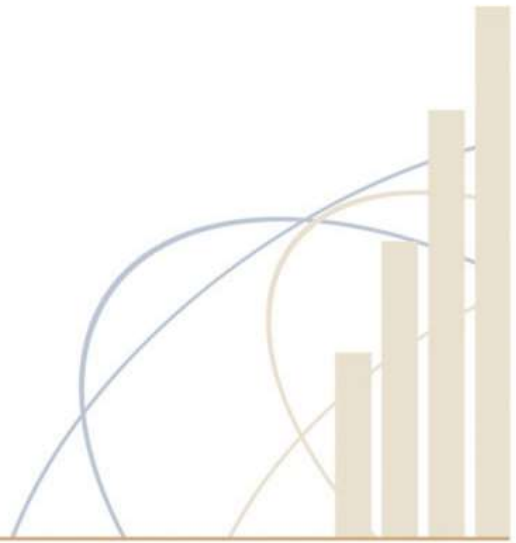
CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Kholofelo Halefose
Eskom

Opening Statement

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Technology can be bought, but skills must be built and that is where our biggest opportunity and risk lies.



Presentation Outline

- ❑ Cyberattacks in the Public Sector.
- ❑ Cybercrimes in Africa.
- ❑ Cybersecurity Skills Shortage.
- ❑ Upskilling & Reskilling.
- ❑ Bridging the gap between academia and industry.
- ❑ Women in Cybersecurity.
- ❑ Emerging Threats & Future Skills.
- ❑ Call for Action.

Cyberattacks in the Public Sector

- South Africa's public sector has emerged as a prime target for cybercriminals, following a wave of cyber-attacks on state-owned enterprises (SOEs) and government institutions.

"The public sector in South Africa has been increasingly targeted by cybercriminals, leading to a significant rise in cyberattacks. The Financial and Operational Impact of Cybercrime on the public sector is staggering, with R24 million stolen in a cyber-attack in May 2024, adding to the R300 million stolen over the past decade. The Council for Scientific and Industrial Research estimates that cybercrime costs the South African economy up to R2.2 billion annually" - telecomreviewafrica.com.

Impact of cyber-attacks in Public Sector

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

The current reality:

- ❑ Growing cyber threats targeting government and critical infrastructure.
- ❑ Limited pipeline of cybersecurity talent.
- ❑ Competition with private sector for skilled professionals.
- ❑ Legacy systems + rapid digital transformation = increased risk.

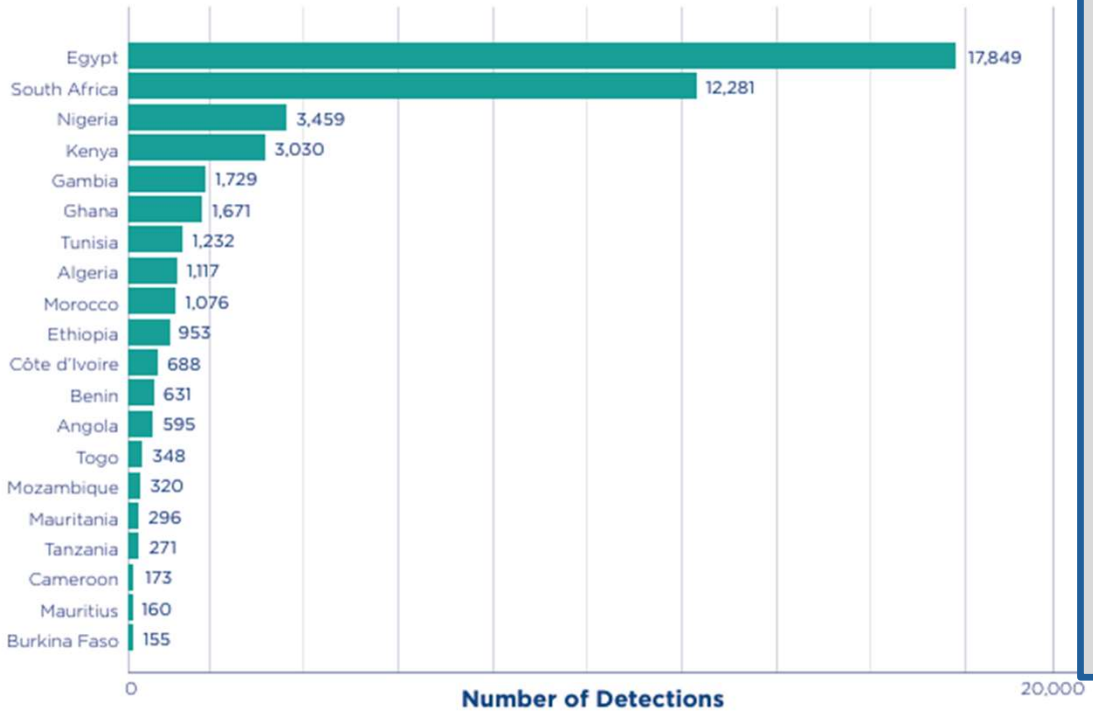
Impact on Public Services:

- ❑ Disruption of essential services (health, education, utilities).
- ❑ Operational downtime and delayed service delivery.
- ❑ Significant financial impact and recovery costs.
- ❑ Loss of public trust and confidence.

Cybercrime in Africa

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

In 2024, INTERPOL member countries identified ransomware as one of the most prevalent cyberthreats across the African continent, posing a growing risk to governments, businesses, and critical services.



Challenges in Combating Cybercrime in Africa

The most common limitations include:

- ❑ **Training needs: 95% reported inadequate, inconsistent, or donor dependent training.**
- ❑ Resource constraints: 95% of countries.
- ❑ Access to specialized tools: 95% of countries.
- ❑ **Technical skill gaps: 74% of countries.**
- ❑ Infrastructure gaps: 72% of countries.
- ❑ Operational barriers: 58% face bureaucratic, legal, or institutional obstacles to efficient investigations.

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Building a skilled cybersecurity workforce for the Public Sector

Let us not just respond to cyber threats , let us build the capability to stay ahead of them

Cybersecurity Skills Shortage

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Data Point	Source
The global cybersecurity workforce gap stands at 4.8 million unfilled positions, a 19% year-on-year increase.	*ISC2 Cybersecurity Workforce Study, 2024*
55% of cybersecurity teams globally are understaffed. 65% of organisations have unfilled cybersecurity positions.	*ISACA State of Cybersecurity, 2025*
63% of respondents based in sub-Saharan Africa reported their organizations is lacking the talent and skills required to meet their current cybersecurity objectives (globally 50%).	*WEF Global Cybersecurity Outlook, 2026*
Women represent approximately 20–25% of the global cybersecurity workforce. In the under-30 cohort, this rises to 26%.	*ISC2 Women in Cybersecurity, 2024*
Adaptability is now the #1 qualification factor for cybersecurity hires (61%), ahead of prior experience (60%). Soft skills are the top skills gap (59%).	*ISACA State of Cybersecurity, 2025*
Only 29% of enterprises trained non-security staff to move into security roles in 2025, down from 41% the prior year, despite 46% of current cyber staff having transitioned from non-security roles.	*ISACA State of Cybersecurity, 2025*

Upskilling & Reskilling

- ❑ Continuous professional development.
- ❑ Cross-skilling IT and OT professionals.
- ❑ Certification programmes (aligned to NIST, ISO, etc.).
- ❑ Practical simulations and labs.

Upskilling & Reskilling (continues)

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Early-Career Pivoter - *Typical Job Requirements*

What Employers Ask For	What It Means
Cybersecurity Certificate, e.g., Security+ or ISC2 CC / Diploma in IT / BSc Computer Science	Entry-level cybersecurity certification showing foundational knowledge
Networking Basics	Understanding how computers and networks communicate
SIEM Exposure	Ability to use security monitoring tools such as Splunk or Microsoft Sentinel
Problem-Solving Skills	Ability to investigate and respond to security issues
Communication Skills	Writing reports, explaining incidents, and working with teams
Willingness to Learn	Employers value curiosity and continuous learning
Basic Cloud Knowledge	Understanding platforms like AWS or Microsoft Azure
Hands-On Practice	TryHackMe, Hack The Box, or home lab experience

Upskilling & Reskilling (continues)

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Available Self-learning Training

Provider	Certification	Cost	Skills Covered
Cisco	Introduction to Cybersecurity	Free	Cyber basics, threats, networking
ISC2	Certified in Cybersecurity (CC)	Free training + sometimes free exam	Security fundamentals
Microsoft	SC-900 Security Fundamentals	Free learning	Cloud security basics
Fortinet Training Institute	NSE 1–3	Free	Network security fundamentals
AWS	AWS Cloud Practitioner Essentials	Free learning	Cloud fundamentals
Google	Google Cloud Cybersecurity Certificate	Free trial / Financial aid	Cloud security, SIEM, threat management
Microsoft Learn Sandbox	Hands-On Practical Skills	Free	Azure security, Defender, Sentinel, cloud governance
Splunk Boss of the SOC (BOTS)	Hands-On Practical Skills	Free	SIEM investigations and SOC operations
Kali Linux / Home Lab Projects	Hands-On Practical Skills	Free	Penetration testing and vulnerability assessments

Skilling up - Certifications

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Early-Career Pivoter

Certification	Provider	Career Path
CompTIA Security+	CompTIA	General Cybersecurity
SC-200 Security Operations Analyst	Microsoft	SOC Analyst
Certified Ethical Hacker (CEH)	EC-Council	Ethical Hacking
Splunk Core User	Splunk	SIEM / SOC
AWS Certified Security – Specialty	AWS	Cloud Security

Bridging the gap between academia and industry

- Integrate cybersecurity into school and university curricula.
- Strengthen partnerships with academia.
- Graduate programmes & internships.
- Public sector bursaries and scholarships.

Bridging the gap between academia and industry (Initiatives)

Women in Cybersecurity

- Increase participation of women in cybersecurity.
- Mentorship and sponsorship programmes.
- Inclusive policies and environments.
- Role models and visibility.

Women in Cybersecurity (Initiatives)

Increase participation of women in cybersecurity

Why this matters:

- Increase participation of women in cybersecurity.
- This programme helps close the gap through skills, mentorship, and access.
- It positions you for global opportunities and leadership.

Participants can choose from four specialised tracks:

- Policy & Diplomacy.
- Incident Response.
- Criminal Justice.
- Cyber & AI.

"Women constitute only about 24% of the cybersecurity workforce in 2024 and are underrepresented in international negotiations on cyber issues".

Women in Cybersecurity (Initiatives)

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

CYBERSECURITY CAREER ROADMAP & SELF-ASSESSMENT TOOLKIT

- A 12-Month Career Pathway for Women Entering, Advancing In, and Building Cybersecurity Teams.

https://womeninit.org.za/

Emerging Threats & Future Skills

- AI-driven cyberattacks.
- Quantum computing impact on cryptography.
- OT/IT convergence risks.
- Digital sovereignty and data governance.

Call to Action

- ❑ Invest in skills development programmes.
- ❑ Strengthen collaboration across sectors.
- ❑ Build inclusive and diverse talent pipelines.
- ❑ Elevate cybersecurity to strategic priority.

"We must invest in people as much as we invest in technology."

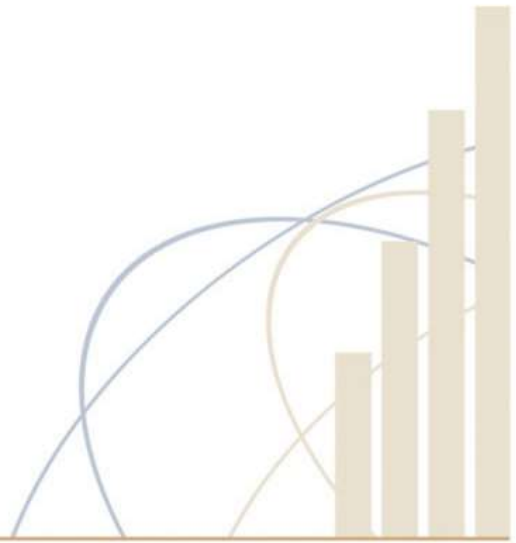
Cybersecure Culture

- **Leadership Commitment**:
  - Strong executive and board-level ownership driving cybersecurity as a strategic priority.
- **Continuous Awareness & Training**:
  - Ongoing, role-based education to build sustainable cyber capabilities.
- **Shared Responsibility**:
  - Cybersecurity is everyone's responsibility—not confined to IT alone.
- **Cyber Hygiene**:
  - Individuals must practice basic cybersecurity hygiene as a fundamental life skill, both professionally and personally.

Closing Statement

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Cybersecurity is a shared responsibility and collaboration is our strongest defence.



Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body