



Cybersecurity and Ransomware

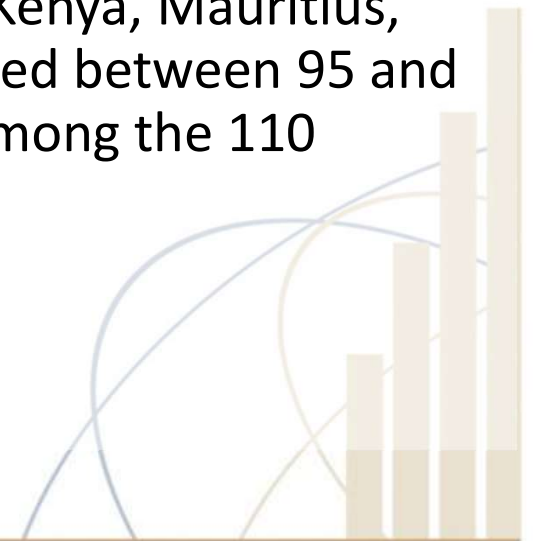


www.cigfaro.co.za

De Wit Coetsee
Independent Contractor Western Cape
Provincial Government
SAQA Recognised Professional Body

Statistics

- **South Africa**
 - South Africa ranks 14th globally in the **average cost of a data breach**, reaching nearly R50 million in 2024.
 - South Africa has made a significant leap in its cybersecurity standing, moving from 67th to 73rd in the global threat index. With a Normalised Risk Index of 37, it now ranks as **the third safest country in Africa**, showing notable improvements in its defences against rising cyber threats. Egypt and Zambia lead as the safest African countries in terms of malware threats, ranking 97th
- The African countries **leading in cybersecurity** are Ghana, Kenya, Mauritius, Rwanda, Tanzania, Egypt, and Morocco. These nations scored between 95 and 100 on the ITU's cybersecurity index. d 82nd respectively among the 110 countries surveyed in the Index.

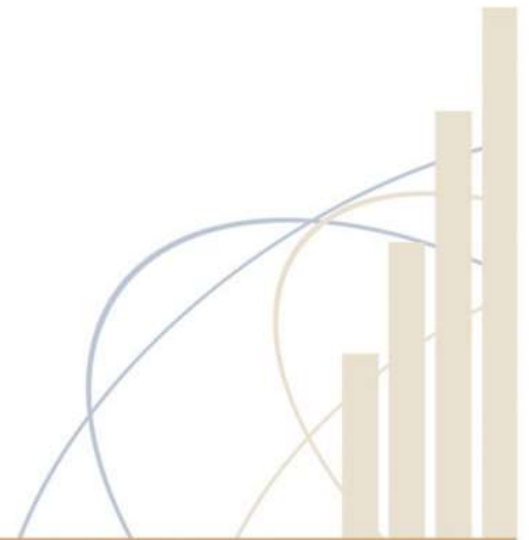


Municipal Vulnerability

- **Why?**
 - Vast amount of personal data, finances, and manage critical infrastructure
- **Types**
 - Including ransomware attacks, data breaches, phishing campaigns, and denial-of-service attacks
- **Targets**
 - Human and financial exploitation
 - Disrupt essential services like water and electricity supply, waste management, and tax collection
- **Trends**
 - Cyberattacks on South African municipalities appear to be increasing in frequency, mirroring the global trend
 - Ransomware attacks, where cybercriminals encrypt critical systems and demand a ransom for their release, are a significant concern for municipalities
 - Many municipalities struggle with limited budgets and a shortage of cybersecurity expertise, making them more vulnerable to attacks

What is Cybersecurity

Cybersecurity encompasses organisation-wide approach that includes strategy, processes, practices, and technologies to mitigate related threats to information, information systems, technology, and facilities.



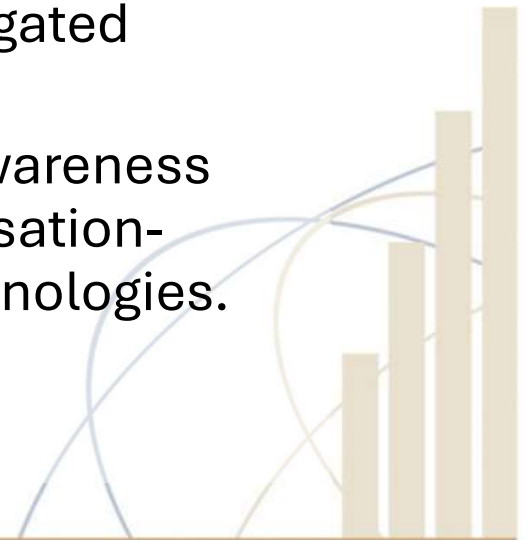
How Cybersecurity is Applied

- Whole-of-Organisation approach
 - All levels and individuals in the municipality have a role to play
 - It is a subset of the municipal governance system
 - Cybersecurity governance does not stand on its own
- Critical components of the municipality involved in cybersecurity



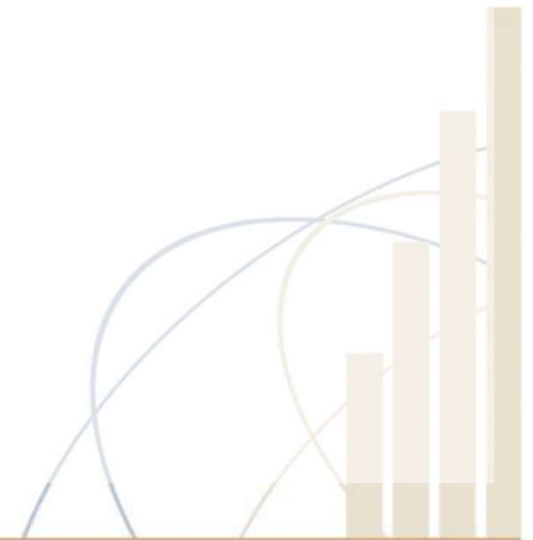
Attack Resilience

- No longer if, but when
- No longer when, but how many times per year
- Cyber threat resilience
 - The ability of the municipality to navigate security breaches and enable business continuity in accordance with business needs
 - The fluency with which incidents can be mitigated through muscle memory
 - The incremental improvement of recovery awareness (roles and responsibilities), methods (organisation-wide), incidence response strategy, and technologies.



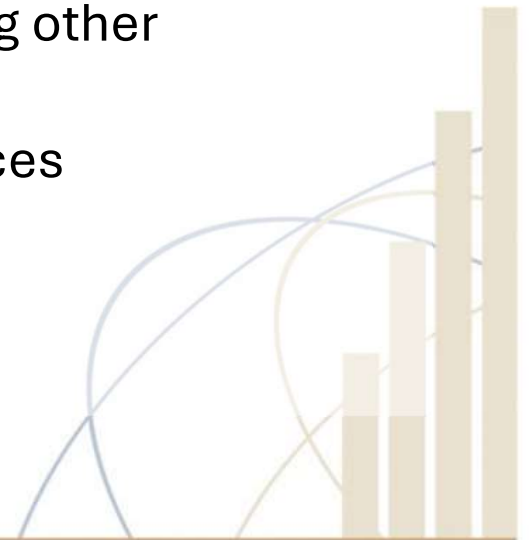
Strategic View

- Are we secure?
 - No longer a relevant
- Cascade of a need-to-know
 - In the event of a cybersecurity breach, can we recover as informed by business requirements?
 - Can you proof this?
 - Show-and-tell?



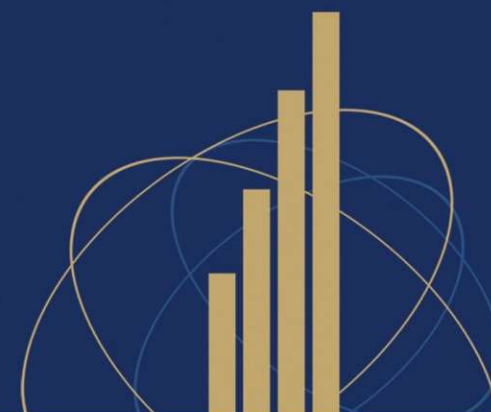
Pitfalls

- ICT and security is a cost center
- Cybersecurity is an ICT function problem
- Cybersecurity AI bright lights
- Fear mongering
- Responding due to breach instead of strategic approach
- All data is equal
- Ignoring complexity of human decision making
- Overemphasis of cybersecurity governance, ignoring other governance requirements
- Lack of business and ICT function skills and resources
- Underfunded security budget
- 3rd Party – service provider risk ignored





Thank You!



CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body