



# Beyond Findings: Reclaiming Accountability and Restoring Public Confidence

---

## Cyber and IT Controls Under Scrutiny: Safeguarding Public Sector Systems

By: Dr. Zandy Dlamini



-  **01** South African Threat Landscape
-  **02** Public Sector Vulnerabilities
-  **03** Controls and Compliance Frameworks
-  **04** Case Studies and Challenges
-  **05** Best Practices and Future Solutions

## Agenda and Key Discussion Areas





# The South African Cyber Threat Landscape

## Growing Fraud and Breach Exposure

South Africa continues to experience one of the highest rates of suspected digital fraud on the continent. Government-related digital services remain attractive targets because of the volume and sensitivity of citizen information they process daily.

## Rising Data Breach

Regulators and legal analysts have reported significant growth in breach notifications, highlighting increasing exposure to phishing, ransomware, credential theft and data exfiltration incidents affecting public institutions.

## Monitoring and Preparedness Gaps

Many public entities still lack mature cyber monitoring capabilities. Limited continuous threat monitoring and delayed incident detection increase the likelihood of operational disruption and reputational damage.



# Why the Public Sector is Targeted

## Concentrated Citizen Information

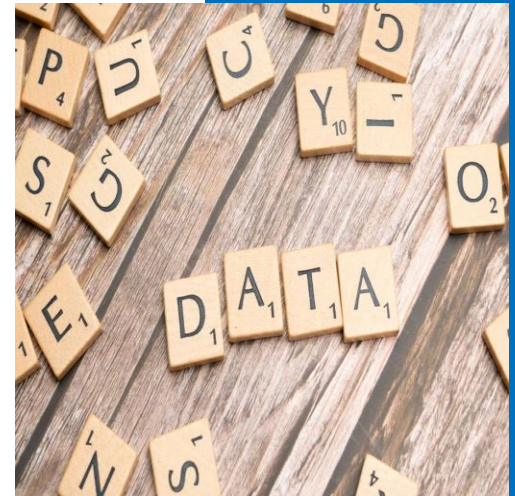
Departments and agencies maintain extensive records covering identity, taxation, social grants, healthcare and employment. These repositories provide significant value to cybercriminals and threat actors.

## Critical Infrastructure Dependence

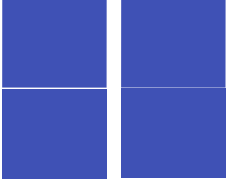
Disruptions to state-owned enterprises, municipalities and service delivery systems can create widespread economic and social consequences, increasing pressure on victims during cyber incidents.

## Legacy Systems and Procurement Delays

Outdated technologies, patching backlogs and lengthy procurement processes often create exploitable weaknesses and slow the adoption of modern security capabilities.



## Access Control Weaknesses



Excessive privileges, poor segregation of duties and dormant accounts remain frequent audit observations across agencies.

## Patch and Vulnerability Gaps

Delayed remediation and inadequate vulnerability management programs create recurring exposure and repeat findings.

## Monitoring Deficiencies

Limited logging, weak alerting and incomplete visibility hinder detection and response effectiveness.

# Common Audit Findings

# Core IT and Cyber Controls Frameworks

## **Access and Identity Management**

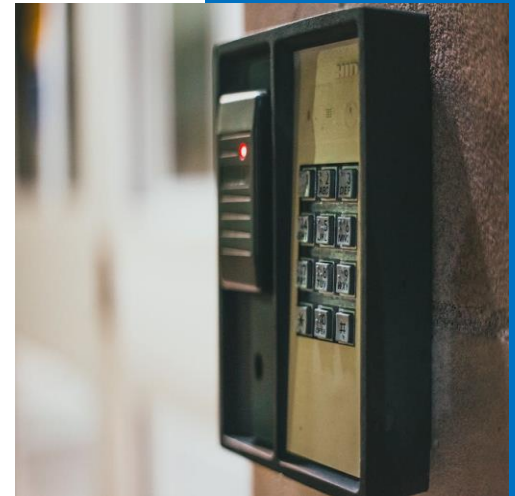
Strong user access governance, privileged account management and multi-factor authentication reduce the risk of credential compromise and unauthorized access to critical systems.

## **Patch and Vulnerability Management**

Continuous vulnerability assessment and disciplined patch management programs help eliminate known weaknesses before attackers can exploit them in public-facing environments.

## **Incident Response and Recovery**

Air-gapped backups, tested recovery procedures and rehearsed incident response plans strengthen resilience and reduce downtime during ransomware and data breach events.





## Regulatory and Compliance Pressures

### **POPIA Responsibilities**

POPIA requires reasonable technical and organisational measures to protect personal information. Breaches may trigger investigations, enforcement notices, penalties and reputational consequences for institutions and executives.

---

### **Cybercrimes Act Requirements**

The Cybercrimes Act defines offences related to unauthorized access, extortion and unlawful interception while strengthening reporting and investigative frameworks across South Africa.

---

### **PFMA and Governance Accountability**

The PFMA and related governance requirements treat digital assets as critical resources. Failure to safeguard systems and information can result in findings, misconduct allegations and audit scrutiny.

---

## **Case Study: South African Bureau of Standards**

### **Major Ransomware Incident**

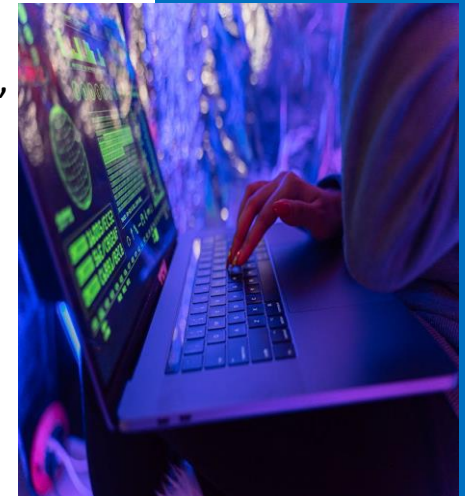
A ransomware attack severely disrupted operations, affecting systems, business continuity and organizational effectiveness. The event highlighted weaknesses in resilience and preparedness.

### **Operational Consequences**

Extended service interruptions, manual processes and financial impacts demonstrated how cyber incidents can rapidly evolve into governance and service delivery crises.

### **Executive Accountability**

Investigations emphasized the importance of acting on audit findings and security recommendations. Ignored control weaknesses can eventually translate into leadership and governance scrutiny.







## Case Study: Stats SA and Gauteng Province

### Public-Facing System Exposure

Recruitment and citizen-facing platforms remain common entry points for attackers seeking access to sensitive information and broader government networks.

### Data Exfiltration Risks

Modern attackers increasingly focus on stealing information for extortion and public disclosure rather than only encrypting systems, creating regulatory and reputational risks.

### Lessons for Government

Strong data classification, segmentation, monitoring and rapid isolation procedures are essential to contain incidents and protect citizen information assets.

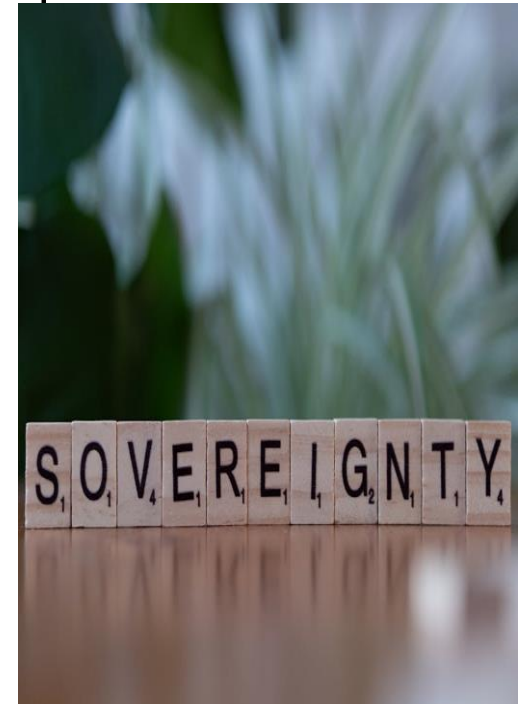


## Key Challenges Facing Government

### Skills, Budget and Governance Constraints

Public institutions face persistent shortages of cybersecurity talent, fragmented governance structures and competing budget priorities. These challenges reduce the effectiveness of security programs and slow the implementation of modern controls. Without sustained executive sponsorship, cybersecurity initiatives often become compliance exercises rather than operational capabilities.

Closing the gap requires integrated governance, workforce development, measurable accountability and continuous testing of controls and recovery processes.



## Best Practices for Public Sector Leaders

- 01 Act on Audit Findings Immediately
- 02 Adopt Zero Trust Principles
- 03 Stay Informed About Emerging Threats
- 04 Run Cyber Awareness Drills
- 05 Implement Continuous Monitoring

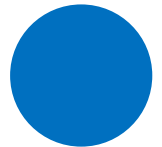


## Cybersecurity as Governance

# Call to Action

### **What should public sector leaders do next?**

Cybersecurity must be treated as a governance, accountability and service delivery priority. Leaders should invest in resilience, verify control effectiveness and ensure that protection of citizen data receives the same attention as protection of public funds.





BY 2030 ETHEKWINI WILL BE AFRICA'S MOST LIVEABLE CITY