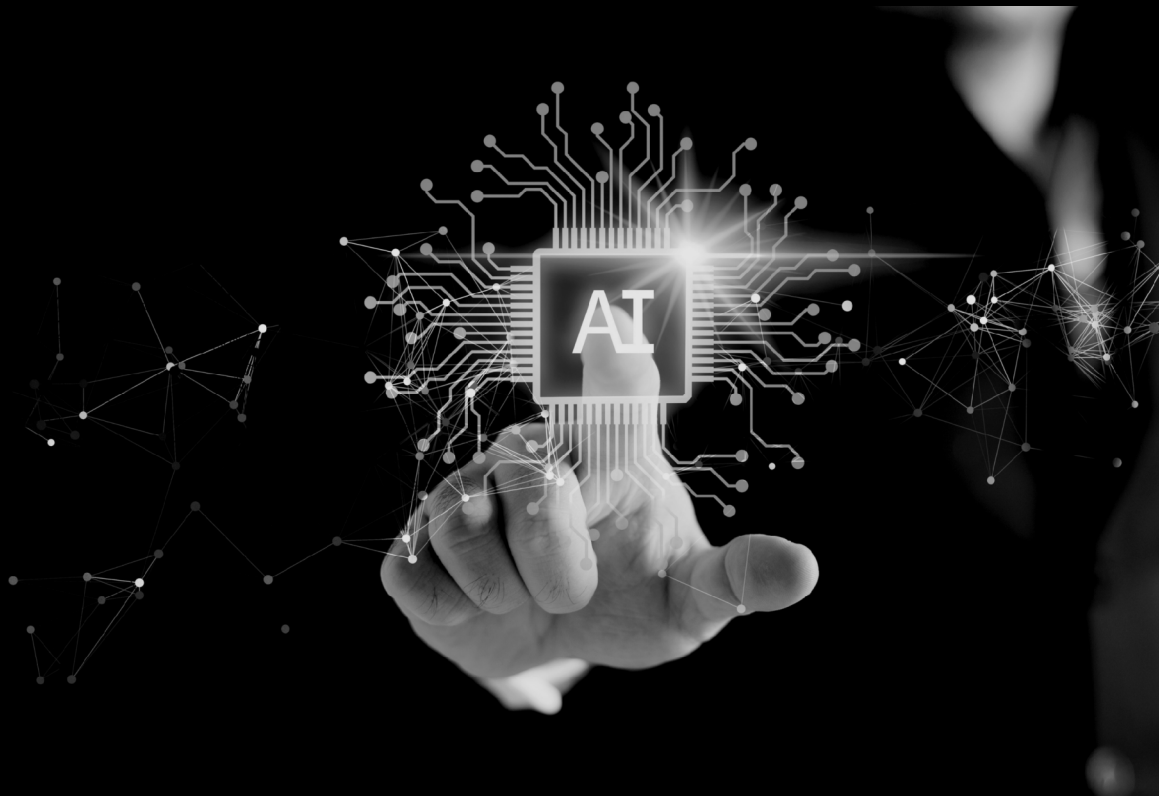




DATA PRIVACY | REGULATORY

Confidence is not capability (Part 1): What the data shows, and why POPIA is the foundation of cyber resilience

22 October 2026 17 min read

by Ahmore Burger-Smidt, Director and Head of Regulatory

A two-part series drawing on the Data Confidence & AI Readiness in Africa Report 2026

Introduction

Ransomware is no longer an IT outage. Today's attacks target backups first, exfiltrate personal information before encrypting it and use the threat of publication to extract payment. Running alongside that threat, artificial intelligence has moved from pilot projects into daily use in most large organisations, usually ahead of the controls meant to govern it. In South Africa, all of this takes place under a data protection regime that has been fully enforceable since 1 July 2021. The Protection of Personal Information Act 4 of 2013 (POPIA) is administered by an Information Regulator that has shown it will act when security safeguards fail.

Boards are now asked a narrower, harder question than whether an incident will occur: can the organisation show, with evidence, that it can withstand one? The Data Confidence & AI Readiness in Africa Report 2026, published by Veeam Software together with ITWeb, suggests that many cannot. Its central finding is that confidence is running well ahead of capability.^[1]

This is the first of two articles on the report. Part 1 sets out the key survey findings. It then explains why POPIA compliance operates as a cyber-resilience framework in its own right, and why data visibility is where legal exposure and operational risk meet. Part 2 turns to artificial

intelligence, both as a defensive tool and as a source of new risk, including the emerging threat of rogue AI agents, and closes with practical recommendations.

THE SURVEY AT A GLANCE
140 senior IT, data and cybersecurity leaders, 14 African countries, just under 70% in South Africa[2]
52% very or extremely confident they could recover clean, usable data after ransomware[3]
45% of those reporting end-to-end recovery test outcomes described partial success, significant gaps or failure[4]
Only 29% advanced or fully ready to adopt, govern and scale AI using trusted data[5]
Only 37% can produce an accurate seven-day audit trail of access to their most sensitive data across most or all critical systems[6]
Nearly 70% expect to increase spending on data protection, cyber resilience and AI governance[7]

Key findings from the survey

About the survey

The survey was conducted online via the ITWeb and ITWeb Africa platforms during June and July 2026. It drew responses from 140 senior IT, data and cybersecurity leaders at medium and large organisations across 14 African countries, with just under 70% of respondents based in South Africa.[8] Respondents spanned financial services, retail, mining, telecommunications, media and the public sector, and included CIOs, CISOs, CTOs and data and AI leaders.[9] The survey findings are a strong directional indicator, not a statistically definitive picture of the market.

Finding 1: recovery confidence is outpacing recovery proof

More than half (52%) of executives are very or extremely confident that they could recover clean, usable data after a ransomware attack, and a further 33% are moderately confident, so 85% express at least moderate confidence.[10] Yet 32% have never performed a full technical recovery test, have not tested in over a year, or do not know when testing last occurred.[11] Even among organisations that completed an end-to-end recovery test, 45% reported only partial success, significant gaps or outright failure.[12]

The report concludes that some organisations are relying on backup policies or assumptions rather than validated recovery performance. It warns that, without regular end-to-end testing, a ransomware incident could result in extended downtime, data-integrity problems, regulatory exposure and reputational damage.[13]

In legal terms, this is the difference between having a safeguard on paper and being able to demonstrate that it works.

Finding 2: AI adoption is outpacing organisational controls

Only 29% of organisations consider themselves advanced or fully ready to adopt, govern and scale AI using trusted data.[14] At the same time, 36% use approved AI tools in selected business functions, 27% are running pilots or experiments, and 14% have embedded AI into core business operations or autonomous workflows.[15] A further 11% report informal or employee-led use of public AI tools with limited oversight.[16]

Around half of respondents use AI in business functions, core processes, or automated workflows, yet fewer than a third consider themselves ready to govern it. The report treats the presence of "shadow AI" as evidence that employee demand is moving faster than organisational controls.[17]

Without stronger data governance, access controls and oversight, organisations risk exposing sensitive information, creating compliance issues and undermining trust in AI-generated outputs.[18]

Finding 3: organisations cannot fully see or account for their data

The biggest barriers to maintaining data confidence are skills shortages (32%), incomplete or inconsistent data classification (28%), budget constraints (27%), lack of visibility into sensitive or critical data (26%) and legacy systems (25%).^[19] Respondents also cite data sprawl across cloud, SaaS, endpoints, backups and third parties (23%), reliance on manual inventories or spreadsheets (19%) and shadow IT or shadow AI use (17%).^[20]

The accountability gap is stark. Only 37% say they can produce an accurate audit trail showing who accessed their most sensitive datasets across most or all critical systems in the past seven days; 55% can do so only partially or for selected systems, and 8% cannot or do not know.^[21] The report observes that fragmented visibility makes it difficult to demonstrate compliance, detect misuse or respond quickly to security incidents. It adds that organisations without accurate data inventories and access monitoring will struggle as regulatory scrutiny intensifies.^[22]

Finding 4: investment is accelerating in the right places

Nearly 70% of organisations expect to increase spending on data protection, cyber resilience and AI governance over the next 12 months, with 30% anticipating a significant increase.^[23] Investment priorities are backup and recovery (54%), AI governance (42%), identity and access controls (41%), data discovery and classification (36%) and cloud and SaaS data protection (30%).^[24] Privacy automation (15%) and data security posture management (6%) remain lower priorities.^[25] The report notes that organisations are beginning to treat cyber resilience and AI as two outcomes of the same foundation, trusted data, rather than as separate initiatives.^[26]

Finding 5: geography and size shape maturity, but not always as expected

Multi-country organisations are markedly more mature. They are more likely to have AI embedded in core operations (22% against 5%) and to be advanced or fully AI-ready (39% against 18%); they report higher ransomware recovery confidence (60% against 45%) and fewer unsuccessful recovery tests (4% against 11%).^[27] The report attributes this to the greater regulatory and operational complexity of cross-border operations, which drives earlier investment in AI governance, data visibility and cyber resilience, although multi-country organisations struggle more with data sprawl, classification and cross-border compliance.^[28] Single-country organisations are more constrained by skills shortages (40% against 24%) and budgets, and focus on backup and recovery (67% against 42%).^[29]

Size, by contrast, does not guarantee maturity. Smaller organisations (under 500 employees) are more likely to be very confident that they know where sensitive data resides (47% against 30%) and rate their data-management capability more positively (56% against 38%); no smaller respondent rated its capabilities as poor, compared with 11% of large organisations.^[30] Larger organisations place greater emphasis on identity and access controls (45% against 33%), while smaller organisations invest more heavily in AI governance (51% against 38%) and skills development (37% against 17%).^[31]

The lesson for South African clients is that regulatory complexity, properly managed, appears to drive maturity. Organisations that have seriously dealt with cross-border data protection obligations are better prepared to recover from attack and scale AI safely.

The imperative of data privacy compliance: POPIA as a cyber-defence framework

Privacy compliance and cybersecurity are still often treated as separate disciplines, one owned by legal and the other by IT. The survey shows why that division no longer holds. Almost every weakness it identifies corresponds directly to an existing obligation under POPIA: untested recovery, poor data visibility, inadequate audit trails, uncontrolled AI use and data sprawl across third parties. Properly implemented, compliance is not an overhead added to security. It is a structured security programme that the law already requires.

Section 19: security safeguards are a continuous, risk-based obligation

Section 19 of POPIA requires a responsible party to secure the integrity and confidentiality of personal information in its possession or under its control. It must do so by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of it. The section also requires the responsible party to identify all reasonably foreseeable internal and external risks, to establish and maintain appropriate safeguards against them, to regularly verify that those safeguards are effectively implemented, and to ensure that they are continually updated in response to new risks or deficiencies. It also requires due regard to generally accepted information security practices.

The duty to verify is where the law and the survey meet. An organisation that has never conducted an end-to-end recovery test, or whose last test failed, will find it difficult to show that it has regularly verified the effectiveness of its safeguards. That applies to the 32% of respondents who have not recently tested, or do not know when they last did,^[32] and to the 45% of testers who reported partial success, significant gaps or failure.^[33] These organisations are not only operationally exposed; they may also face a finding that they have not met the section 19 standard. Ransomware that destroys or encrypts personal information without a reliable route to restoration is exactly the "loss" and "damage" the section is designed to prevent.

Know your data: the processing conditions shrink the attack surface

Several of POPIA's conditions for lawful processing operate, in practice, as attack-surface reduction measures. The minimality principle (section 10) limits processing to what is adequate, relevant and not excessive. The retention and restriction provisions (section 14) require records to be kept no longer than necessary and then destroyed, deleted or de-identified. Information that has been lawfully deleted cannot be stolen, encrypted or published. Organisations struggling with data sprawl across cloud, SaaS, endpoints, backups and third parties (23%) and with inconsistent classification (28%)^[34] are carrying breach liability they do not need to carry.

Compliance with POPIA also presupposes that an organisation knows what personal information it holds, where it is and why it is processed. Two sets of requirements force exactly the data mapping and classification that the survey identifies as weak. The first is the Information Officer's duties under section 55. The second is regulation 4 of the POPIA Regulations, which requires a compliance framework, personal information impact assessments and related measures. The report's own recommendation is to know what data is held, where it sits, how it is used and which privacy requirements apply, including where it moves across borders.^[35] In substance, that describes a mature POPIA compliance programme.

Section 22: you cannot notify what you cannot see

Section 22 applies where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person. The responsible party must then notify the Information Regulator and, subject to limited exceptions, the affected data subjects as soon as reasonably possible after discovery. The notification must give data subjects enough information to take protective measures, including a description of the possible consequences, the measures taken or intended, and, where known, the identity of the unauthorised person.

That obligation cannot be met without evidence. Most respondents cannot produce an accurate audit trail showing who accessed their most sensitive datasets across most or all critical systems. That is the position of 63%: 55% can do so only partially or for selected systems, and 8% cannot or do not know.^[36] Organisations in that position will struggle to determine whether a compromise has occurred, how far it extends and whom to notify. The result is either delayed notification or over-notification, and both carry regulatory and reputational cost. Access logging and monitoring are therefore more than security controls; they are the evidence on which lawful incident response depends.

Operators, third parties and cross-border flows

Sections 20 and 21 govern operators, the service providers that process personal information on a responsible party's behalf. An operator may process the information only with the responsible party's knowledge or authorisation and must treat it as confidential. It must also be bound by a written contract requiring it to establish and maintain section 19 security measures and to notify the responsible party immediately of any suspected compromise. Cloud, SaaS and outsourced services are now the norm, and the survey finds that data sprawl extends to third parties.^[37] Supply-chain contracting and oversight are therefore among the most effective cyber-risk controls available. Section 72 restricts transfers of personal information outside South Africa unless prescribed safeguards are met. It applies to multi-country organisations, which report greater difficulty with cross-border compliance,^[38] and to employees who paste personal information into public AI tools hosted offshore.

Enforcement and accountability raise the stakes

POPIA's accountability condition (section 8) places responsibility squarely on the responsible party. The Information Regulator may issue enforcement notices and infringement notices, and administrative fines of up to R10 million may be imposed. The Regulator has already taken enforcement action against a national government department following a ransomware attack, citing failures in basic security safeguards. Sector-specific regimes add further obligations; financial institutions, for example, are subject to the Prudential Authority and

FSCA Joint Standard on cybersecurity and cyber resilience. Across these regimes, regulators expect evidence that safeguards work, not assurances that they exist.

POPIA compliance reduces exposure to data breaches, ransomware and other cyber threats in four concrete ways. It forces organisations to identify and minimise the data at risk. It requires risk-based safeguards that are regularly verified. It extends security obligations contractually into the supply chain. It also builds the visibility and governance needed to detect, contain and report incidents quickly.

Part 1 in summary

The survey describes a market that is confident but not yet able to prove that confidence. Recovery is assumed more often than it is tested, and when it is tested, it often fails.^[39] Fewer than four in ten organisations can account for who has accessed their most sensitive data across most or all critical systems.^[40] Investment is rising, and it is increasingly directed at governance and visibility rather than backup alone.

POPIA does not create these gaps, but it turns them into legal exposure. Sections 19 and 22, the processing conditions and the operator regime already require what resilient organisations do anyway: they know their data, verify their safeguards, control their suppliers and can explain an incident when it occurs.

Data visibility is the common thread. It determines whether an organisation can minimise what it holds, verify what it protects and notify what it loses. It will also determine whether an organisation can safely deploy the AI tools now entering its systems.

In Part 2, we examine the role of artificial intelligence in cybersecurity. We consider how it can strengthen detection, recovery and compliance, how shadow AI creates new exposure under POPIA, and why autonomous AI agents acting outside their mandate are the next governance problem for boards. We close with practical recommendations for clients.

[1] *Data Confidence & AI Readiness in Africa Report 2026*, 'From Confidence to Capability', p. 14.

[2] *Data Confidence & AI Readiness in Africa Report 2026*, 'Overview of Survey Methodology', p. 2.

[3] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability', p. 3.

[4] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability – Recovery Confidence is Outpacing Recovery Proof', pp. 3–4.

[5] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness', p. 5.

[6] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges', pp. 7–9.

[7] *Data Confidence & AI Readiness in Africa Report 2026*, 'Investment Plans', pp. 10–11.

[8] 'Overview of Survey Methodology', p. 2.

[9] 'Overview of Survey Methodology – Respondent Profile', p. 2.

[10] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability', p. 3.

[11] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability', p. 3.

[12] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability – Recovery Confidence is Outpacing Recovery Proof', pp. 3–4.

[13] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability – Recovery Confidence is Outpacing Recovery Proof', pp. 3–4.

[14] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness', p. 5.

[15] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness', p. 5.

[16] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness', p. 5.

[17] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness – Employee Use of AI is Outpacing Organisational Controls', pp. 5–6.

[18] *Data Confidence & AI Readiness in Africa Report 2026*, 'AI Adoption Outpaces Readiness – Employee Use of AI is Outpacing Organisational Controls', pp. 5–6.

[19] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges – Biggest Challenges in Maintaining Confidence in Data', pp. 7–8.

[20] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges – Biggest Challenges in Maintaining Confidence in Data', pp. 7–8.

[21] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges', pp. 7–9.

[22] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges – Limited Visibility and Access Monitoring Undermine Data Protection, Governance and Trust', p. 9.

[23] *Data Confidence & AI Readiness in Africa Report 2026*, 'Investment Plans', pp. 10–11.

[24] *Data Confidence & AI Readiness in Africa Report 2026*, 'Investment Plans', pp. 10–11.

[25] *Data Confidence & AI Readiness in Africa Report 2026*, 'Investment Plans', pp. 10–11.

[26] *Data Confidence & AI Readiness in Africa Report 2026*, 'Investment Plans – Spending Plans Suggest that Trusted Data is Becoming a Strategic Business Priority', p. 11.

[27] *Data Confidence & AI Readiness in Africa Report 2026*, 'Geography Shapes AI and Resilience Maturity', p. 12.

[28] *Data Confidence & AI Readiness in Africa Report 2026*, 'Geography Shapes AI and Resilience Maturity', p. 12.

[29] *Data Confidence & AI Readiness in Africa Report 2026*, 'Geography Shapes AI and Resilience Maturity', p. 12.

[30] *Data Confidence & AI Readiness in Africa Report 2026*, 'Organisational Size Does Not Equal Maturity', p. 13.

[31] *Data Confidence & AI Readiness in Africa Report 2026*, 'Organisational Size Does Not Equal Maturity', p. 13.

[32] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability', p. 3.

[33] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability – Recovery Confidence is Outpacing Recovery Proof', pp. 3–4.

[34] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges – Biggest Challenges in Maintaining Confidence in Data', pp. 7–8.

[35] *Data Confidence & AI Readiness in Africa Report 2026*, 'From Confidence to Capability', p. 14.

[36] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges', pp. 7–9.

[37] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges – Biggest Challenges in Maintaining Confidence in Data', pp. 7–8.

[38] *Data Confidence & AI Readiness in Africa Report 2026*, 'Geography Shapes AI and Resilience Maturity', p. 12.

[39] *Data Confidence & AI Readiness in Africa Report 2026*, 'Confidence vs. Capability – Recovery Confidence is Outpacing Recovery Proof', pp. 3–4.

[40] *Data Confidence & AI Readiness in Africa Report 2026*, 'Data Visibility and Audit Challenges', pp. 7–9.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)