COMRiC

COMMUNICATIONS RISK INFORMATION CENTRE

Telecommunications Sector Report 2026

Notes from the CEO

COMRiC exists because no single operator can see the whole risk picture alone. Each business watches its own network, customers and balance sheet — but fuel shocks, cyber-attacks, civil unrest and infrastructure crime move across the whole industry at once.

This report draws together what we are hearing from operators, what regulators are doing, what global markets are signalling, and what the incident data shows. None of it points at any single business; it is a shared picture, built so every part of the sector can plan with better information than anyone could gather alone.

The reading is not always comfortable. Diesel costs have eased, but the buffer that softened future shocks is gone. Cyber threats now jump between operators, civil unrest has settled into something ongoing, and fraud is getting smarter even as the value of each case falls. Infrastructure crime, while genuinely improving, is shifting into new forms rather than disappearing.

The encouraging part is that the sector is not standing still. Security spending is paying off, losses are down by nearly two-thirds year on year, and operators are already exploring smarter energy, tighter fraud controls and better coordination. COMRiC's job is to join those efforts up so the whole sector benefits.

Read this not as a list of problems, but as a shared early warning system. The sooner we see risks coming together, the sooner we can act together.

Advocate Thokozani Mvelase
CEO, COMRiC

Statement of the chairperson

COMRIC's ongoing development and successes as a go-to source for information and intelligence about sector-wide strategic risk and resiliency is living proof that collective action is simply indispensable. The shifting global and local risk landscape further justifies collective action as an agile mode for sustaining an industry-wide strategic risk perspective.

In recent times, global and political governance remains tentative. This is evidenced by a constantly shifting and fragile global order, fragile government coalitions, ever-present economic uncertainty, growing nationalism and civil disobedience evidenced – for example - by anti-immigration protests around the world and corresponding alienation of many historical allies.

Added to the above, more immediate matters include energy and related infrastructure security. This continues to be a challenge, regardless of the short-term good news in South Africa that electricity generation has stabilised towards the more reliable. That said, long-term ambitions around sustainable alternative energy sources are still far from fully activated. For example, the country's frail electricity infrastructure still begs for long term investment.

Another matter requiring more urgent attention is unemployment, particularly youth unemployment. This problem creeps ever higher while at the same time local skills and expertise are simply not matching industry demands. Youth unemployment is not unrelated to the matter of civil disobedience.

A few low-hanging opportunities are evident, particularly in the advances in corporate governance, where the King V Code is finding refreshed traction. The Code now promotes a more accountable system of governance founded on transparent reporting and disclosure, which must be published to a diverse range of stakeholders. This promises more meaningful stakeholder engagement.

While I highlight some strategic risks, this short statement will seem out of touch if it doesn't for a moment mention the glaring shortcomings around the criminal justice system. Particularly, the challenges with combating organized crime, corruption and corporate fraud. Recent public revelations about organised crime, criminal markets and criminal syndicate infiltration offer cold comfort that the situation will improve in the short term.

Albeit that strategic risks for the telecommunications industry are well-understood and contained, as evidenced in this COMRIC report, the next step in our collective action efforts is to draw in a wider range of partnerships and collaborations. This is one of the priorities at the forefront of COMRIC's way forward in the medium to long term.

To make this work, COMRIC is more determined than ever to bed down a digitised data gathering, consolidation and intelligence interpretation solution. This, if successful presents the prospect of a leap towards a more predictive, foresight-driven approach to strategic risk governance across the industry.

Dr. Peter Goss, Ph.D
Chairman, COMRiC

Executive Summary

This report brings together four strands of COMRiC's intelligence work: a sector-wide risk assessment for South African telecommunications, a deep dive into fraud and social engineering, a cyber-threat picture for network operators, and a year-on-year look at infrastructure crime across the country's network footprint.

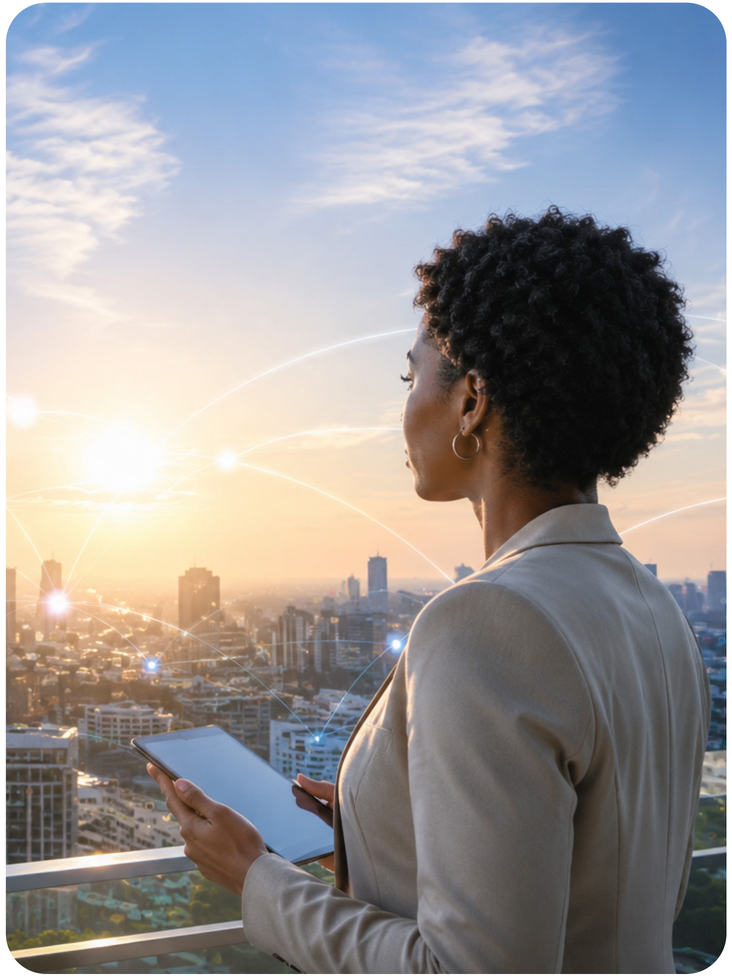
Read together, they tell a consistent story. The sector is under real and growing pressure, but it is not powerless. Some risks are easing, some are worsening, and almost all of them are becoming more tangled up with each other than they used to be.

On the sector risk side, the news on fuel is mixed. Diesel prices dropped sharply on 1 July 2026 after global oil prices fell, but the buffer that used to protect operators from future price shocks, the fuel levy relief, is now gone for good. That means the underlying vulnerability to energy shocks has gone up, even though the immediate cost has gone down. Alongside this sit seven other converging pressures: cyber-attacks that are growing more frequent and more sophisticated, a regulatory environment with several major changes landing at once, ongoing civil mobilisation that has outlasted its original protest date, climate related damage to infrastructure, macroeconomic strain squeezing customers' wallets, supply chain fragility, and persistent infrastructure crime. None of these sit in isolation anymore. A fuel shock makes recovery from a storm harder. A protest makes it tougher to fix a stolen cable site. The risks feed each other.

The fraud and social engineering section shows a similar pattern of change beneath a headline number. Subscription fraud and SIM swap losses together exceeded R200 million over the twelve months studied. Internationally, syndicates are consolidating around fewer, higher-value targets — but South Africa moved the other way this year. Case volumes rose steeply while the average loss per case fell by half or more. Fraud here is getting cheaper per incident and far more frequent, which is a capacity problem as much as a financial one. Trust based scams delivered through WhatsApp, phone calls and text messages have become the leading way fraud gets through the door, meaning technology alone will not fix this. People, training, and awareness matter just as much.

The infrastructure crime section carries the best news in the report. Incidents fell by 40% and financial losses fell R387m during this financial year. That is a genuine result from sustained investment in prevention. But conviction rates remain low, and the criminals have not gone away, they have shifted toward new methods and new areas, which means the pressure needs to stay on rather than easing off.

Across every section, the same lesson repeats. Sector-wide problems need sector-wide answers, and that is exactly the gap COMRiC exists to fill.



Contents

About COMRiC

Communications Risk and Information Centre (COMRiC NPC) — South Africa's neutral telecommunications risk body

A neutral, not-for-profit industry body that unites operators to confront shared security, crime, governance

Neutral & Independent

Not-for-profit telecommunications industry body serving the whole sector, not any single operator.

Shared Challenges

Established to address sector-wide security, crime, governance and resilience challenges.

Intelligence Sharing

A trusted platform for confidential intelligence sharing and collective action.

Lawful Framework

Operates strictly within the regulatory requirements.

Governance & Strategic Direction

A board-governed organisation generating sector intelligence and strengthening resilience

Mission

Generate sector intelligence and strengthen resilience across the telecommunications sector.

Vision

To be South Africa's leading telecommunications intelligence and resilience organisation.

Purpose

Coordinate responses to sector-wide risks that reach beyond any individual operator.

Strategic Approach:

Reactive incident coordination ››››››› **Predictive sector intelligence**

Strategic Focus Areas

Current priorities and expanding risk

Current Priority Areas

- ››› Infrastructure Crime
- ››› Cybersecurity
- ››› Sector Business Resilience
- ››› Sector White-collar Crime
- ››› Regulatory Governance & Compliance

Expanding Risk Lens

- ››› AI-Enabled Threats
- ››› Digital & Financial Crime
- ››› Geopolitical & Macroeconomic Risk

COMRiC's role is not to measure trends. It is to read the signals beneath them, and to turn those signals into intelligence-led resilience across South Africa's telecommunications sector.

The COMRiC Board

Dr. P. Goss
Chairman

Adv. T. Mvelase
Chief Executive Officer

Mr. A. Dhanasir
Director — Vodacom

Ms. M. Makgalemela-Mogohloane
Director — Telkom

Mr. B. Swanepoel
Director — MTN

Mr. L. Swanepoel
Director — Cell C

Mr. A. Peplar
Director — Liquid

Mr. J. Kutumela
Alternate — Vodacom

Mr. T. Vally
Alternate — MTN South Africa

Mr. A. Lawler
Alternate — Liquid

Mr. S. Ndlovu
Alternate — Telkom

COMRiC Value Proposition

Three strategic pillars that turn shared intelligence into collective resilience

Risk Mitigation

Identify and assess sector-wide risks.
Support coordinated mitigation strategies.
Strengthen resilience across the telecommunications sector.

Intelligence & Awareness

Produce sector intelligence and emerging risk insights.
Enhance situational awareness through research and analysis.

Collective Action

Facilitate trusted collaboration between operators, Government and strategic partners.
Coordinate sector-wide initiatives.
Promote a unified response to shared risks.

"COMRiC transforms shared intelligence into collective resilience."

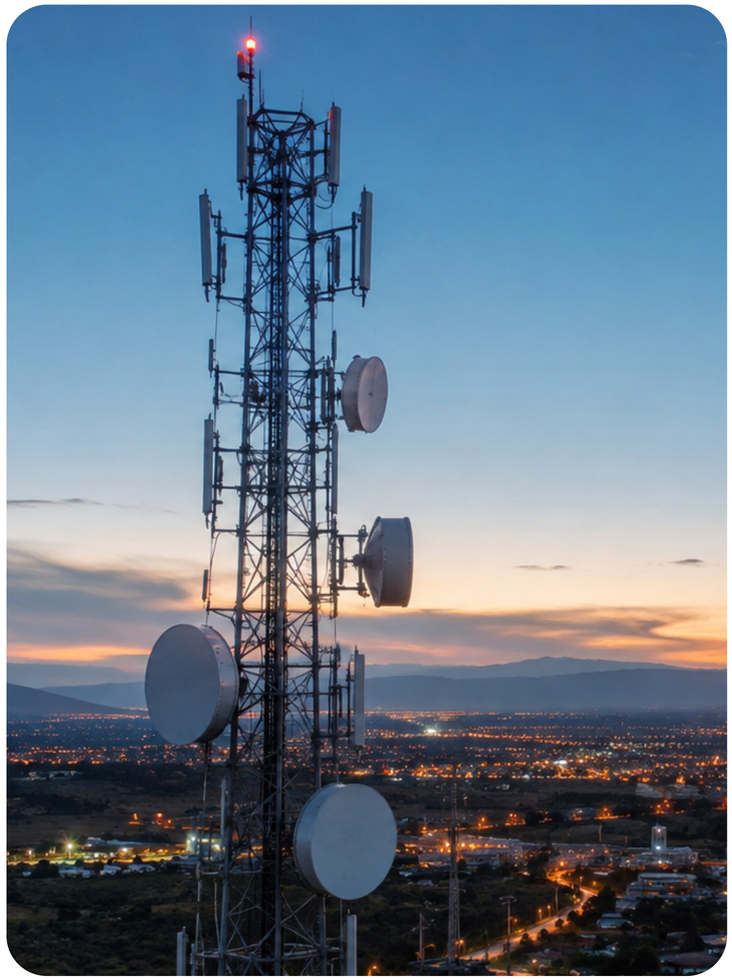
SECTION ONE

Sector Risk Intelligence

Eight converging risk themes shaping South Africa's telecommunications sector
Energy · Cyber · Regulatory · Civil Unrest & Infrastructure Crime · Macroeconomic · Criminal Justice & Deterrence Gap · Climate · Supply Chain

COMRIC

Sector Risk Intelligence Report



South Africa's telecommunications sector is dealing with more moving parts at once than it has faced in a long time, and this section of the report sets out what COMRiC's intelligence gathering has picked up across eight of them.

Energy remains the biggest single swing factor. Diesel prices fell by more than three rand a litre on 1 July 2026 after global crude oil prices dropped, following an easing of tensions between the US and Iran. That is genuinely good short-term news for operators who rely heavily on diesel generators to keep networks running through power cuts. The catch is that the government's temporary relief on the fuel levy has now been fully withdrawn, which means the cushion that protected the sector from April to June has disappeared for good. Put simply, prices are down today, but the sector has less protection against the next price shock than it did a few months ago.

Cyber risk has moved well beyond being an IT department concern. COMRiC's intelligence shows state sponsored attacks, live ransom demands against local internet service providers, and rising ransomware activity, all against a backdrop where an attack on one operator's systems can spread to others through shared infrastructure. On the regulatory front, five different bodies, ICASA, the Department of Communications and Digital Technologies, the Competition Commission, the Information Regulator and the Department of Justice are all pushing significant changes at the same time, from SIM registration rules to network upgrades, creating a compliance workload that is harder to manage than any single rule change would be on its own.

Civil unrest linked to anti-immigration protests was expected to be a single day of disruption on 30 June, but organisers have confirmed it is continuing, so COMRiC now treats it as an ongoing operational risk rather than a one-off event. The Local Government Elections on 4 November 2026 are a known amplifier and are being monitored as a forward-looking trigger. Add in inflation running above the Reserve Bank's target, squeezed household budgets, extreme weather damaging towers and fibre routes, and fragile supply chains for imported equipment, and it becomes clear why COMRiC describes these pressures as converging rather than sequential. They are hitting the sector all at the same time, and each one tends to make the others harder to manage.

The encouraging part is that operators are not sitting on their hands. Diesel hedging strategies, solar and battery pilots, tighter cyber response plans, and stronger physical security in crime hotspots are all already underway. COMRiC's role is to make sure operators are acting on a shared, sector-wide picture of risk rather than each fighting these battles in isolation.

Sector Risk Intelligence Snapshot

South Africa's telecommunications sector has entered an active systemic-risk phase

This report presents COMRiC's sector risk intelligence assessment for the South African telecommunications sector, updated July 2026. Intelligence is drawn from COMRiC's sector engagement work, regulatory monitoring, global signal analysis, and infrastructure incident data synthesised into a unified sector-wide view. Eight converging risk themes have been identified.

Key Insight: COMRiC's sector intelligence assessment identifies eight risk themes that have transitioned from emerging concerns to active operational realities. Several have evolved materially. Risk is no longer linear — it is compounding.

Energy & Fuel Volatility
Extreme diesel price volatility in 2026. Record high of ~R31/ litre in May. July 2026 brought a R3+ decrease following the US-Iran MOU and crude price collapse, but the full fuel levy is reinstated and no fiscal buffer remains. Future price shocks transmit directly to sector costs.

Cyber & Digital Threats
State-sponsored attacks, DDoS and ransomware across the sector, escalating in frequency and sophistication.

Regulatory Pressure
ICASA, DCDT, Competition Commission, Information Regulator and Dept of Justice amongst others simultaneously active with overlapping mandates reshaping operations.

Climate Risk
Flooding, heat stress and severe weather events are damaging infrastructure and compressing recovery windows. Post-flood recovery windows are compressing as incidents compound across provinces. Gauteng, KwaZulu-Natal, Eastern Cape and Limpopo carry the highest exposure.

Supply Chain Fragmentation
Procurement delays and critical third-party dependencies that cannot be rapidly substituted. South Africa imports 70–80% of refined fuel and much of its telecom infrastructure, increasing exposure to exchange-rate volatility and shipping disruption.

Macroeconomic Stress
Inflation breaching SARB target, purchasing power erosion, competitive disruption from new entrants.

Civil Unrest & Infrastructure Crime
9,579 incidents and R231.7M in losses confirmed FY 2025/26. Anti-immigration civil action proceeded on 30 June and has continued with further marches confirmed. Ongoing mobilisation adds sustained operational pressure.

Criminal Justice & Deterrence Gap
Persistent infrastructure crime volumes despite sector security investment reflect constrained prosecutorial capacity and reduced deterrence effectiveness. Low public confidence and constrained law-enforcement capacity remain structural constraints on deterrence. COMRiC is monitoring this as a structural sector risk factor.

Global Signals: South African Risk Transmission

Integrated View of Global Drivers and Sector Exposure

GLOBAL RISK LANDSCAPE & ACTIVE TRIGGERS	TRANSMISSION CHANNEL	SOUTH AFRICAN RISK CONTEXT	SECTOR IMPACT
Energy Market Volatility & Fuel Price Shock UPDATED Crude collapse after the US–Iran MOU offset the full reinstatement of the R3.93/L fuel levy, July inland wholesale diesel at R24,78/L. The April–June levy, relief buffer is permanently removed; no fiscal safety net remains.	Fuel-price pass-through to diesel — the primary transmission channel for geopolitical risk	**Diesel Reserve Gap + Structural Dependency** SA holds ~2 weeks of diesel reserves vs a 90-day global benchmark (FIASA). Grid constraints make generators primary resilience infrastructure — exposing operators to diesel price and availability risk.	Margin to absorb energy shocks has narrowed; any future oil-price or rand shock now hits network
Supply Chain Fragmentation ELEVATED Geopolitical realignment is raising logistics costs and procurement uncertainty. Critical third-party dependencies cannot be rapidly substituted across the sector.	Import dependency & exchange-rate exposure — 70–80% of refined fuel and telecom infrastructure	**Import Dependency Exposure** SA imports an estimated 70–80% of refined fuel and much of its telecom infrastructure and equipment, compressing the domestic response window.	Exchange-rate pressure, shipping disruption and equipment-substitution risk transmit simultaneously.
Geoeconomic & Currency Pressure STRUCTURAL External shocks are transmitted into the sector primarily through energy, import dependency and currency-sensitive procurement, with limited domestic buffers increasing exposure.	Currency-sensitive capex & lead-time inflation on network hardware	**Infrastructure Vulnerability** Persistent theft, vandalism and site-access disruption erode resilience; outage frequency and recovery times are rising, with provincial concentration creating an uneven national footprint.	Medium-term structural constraints compound resilience erosion across the national footprint.

Cyber Risk

An escalating strategic sector-wide threat , frequency and sophistication increasing

Cyber risk is no longer an IT issue. It is a strategic sector-wide threat, amplified by geopolitical instability and the sector's role as critical national infrastructure. COMRiC's sector intelligence consistently identifies cyber as one of the highest-priority risks facing the sector. The effectiveness of law enforcement response to cybercrime incidents is an emerging governance consideration: where prosecutorial and investigative capacity is constrained, deterrence is reduced and sector exposure persists regardless of individual operator defences.

CRITICAL
State-Sponsored Attacks
State-sponsored cyber activity linked to geopolitical conflicts has been documented including reported attacks on SA institutions tied to immigration tensions and Middle East alignments. These are active and ongoing.

ACTIVE
DDoS Attacks – ISP-Level Impact
A live DDoS attack with an accompanying ransom demand has been confirmed against South African ISPs and hosting providers. No direct impact on COMRiC member operators has been confirmed. Operators are actively monitoring for cascade risk.

HIGH
Ransomware & Malicious Software
Ransomware and malware represent persistent operational threats across the sector. The telecom sector's role as both data custodian and critical infrastructure provider significantly elevates exposure.

ESCALATING
Geopolitics-Cyber Nexus
Cyber and geopolitical risk are explicitly linked: states deploy cyber capability as retaliation against perceived enemy-aligned nations. South Africa's international relationships directly influence sector cyber exposure.

HIGH
SIM-Related Fraud & Telecom Crime
SIM boxing, international bypass fraud, and organised crime exploiting insider access are active sector threats. As economic pressure intensifies, fraud exposure escalates — macroeconomic deterioration and cyber risk are directly correlated.

SYSTEMIC
Sector Cross-Contamination
A critical sector-wide risk: a cyber vulnerability in one operator can be exploited across the sector. An attack on one operator's infrastructure can ripple to others through shared systems, networks, and supply chain

Regulatory & Compliance Pressure

A highly dynamic environment adding material operational and strategic burden

COMRiC's regulatory monitoring has identified a highly dynamic and converging compliance environment. With ICASA, DCDT, Competition Commission, Information Regulator and the Department of Justice simultaneously active with overlapping mandates, the compliance burden on sector operators is increasing not stabilising. COMRiC tracks this landscape continuously to provide the sector with timely regulatory intelligence.

ACTIVE DIRECTIVE
Dept of Justice SIM Card Registration Directive
Operators given compressed timelines to present remediation plans. Risk of significant regulatory penalties similar to precedents in comparable markets. Industry-wide compliance pressure.

ONGOING
ICASA Activity — Spectrum & LEO Licensing
Licensing of Low Earth Orbit satellite providers is creating commercial and compliance uncertainty. Contentious regulatory positioning across the sector.

IN PROGRESS
2G / 3G Network Sunsetting
ICASA and DCDT driving network migration timelines. Significant capital expenditure implications and operational transition risk across the sector.

EMERGING
Biometric Implementation Mandate
Mandatory biometric registration being driven by regulator and ministry with compressed compliance windows. Significant operational implementation burden.

STRUCTURAL
Policy & Regulatory Uncertainty
The current policy environment introduces uncertainty into regulatory direction and planning timelines. Operators face strategic planning risk where regulatory outcomes are difficult to project with confidence.

ONGOING
Regulatory Boundaries for Sector Collaboration
Sector collaboration and intelligence sharing must operate within POPIA and competition-law requirements. COMRiC provides a neutral platform for aggregating sector-level intelligence without exchanging commercially sensitive or competitively restricted information.

Sector Intelligence Observation: COMRiC's regulatory monitoring indicates that simultaneous, overlapping interventions across multiple regulatory institutions are creating a cumulative compliance burden that warrants integrated management rather than directive-by-directive responses. Regulatory risk is no longer a discrete line item; it is a converging strategic exposure.

Criminal Justice & Deterrence Gap

Persistent infrastructure crime remains a structural sector risk, with constrained prosecution capacity, limited deterrence and inconsistent recovery of stolen infrastructure continuing to undermine security investment and resilience.

Justice & Deterrence
Criminal justice effectiveness influences the deterrence of infrastructure crime and organised criminal activity.

Law Enforcement & Prosecution
Delays in investigations, prosecutions and judicial processes reduce the effectiveness of industry security investments.

Critical Infrastructure
Weak deterrence increases the likelihood of recurring infrastructure crime despite improved preventative controls.

Governance & Collaboration
This is a systemic risk requiring collaboration between industry, law enforcement and the criminal justice system.

Macroeconomic Stress & Civil Unrest

Forward-looking sector risk assessment: economic pressure and social instability as ongoing operational exposures

MACROECONOMIC STRESS

Inflation & Cost Pressure
Inflation and cost pressures continue to affect operating expenditure and purchasing power across the sector.

Customer Purchasing Power Erosion
Economic pressure is reducing consumers' ability to absorb higher costs and increasing pressure on sector revenue and affordability.

Competitive Intensification
Economic pressure is increasing competitive intensity, pricing pressure and margin constraints across the telecommunications sector.

Fraud as an Economic Knock-On Effect
Economic hardship can amplify fraud exposure, including SIM-boxing, bypass fraud and organised financial crime.

Macroeconomic Stress & Civil Unrest

CIVIL UNREST & SOCIAL INSTABILITY

Elevated Social Mobilization — Election Amplifier
Social and community tensions remain elevated, with localized mobilization capable of creating short-notice disruption to operations and access. The 4 November 2026 Local Government Elections are a forward-looking trigger that may amplify existing mobilization.

Anti-Immigration Mobilization
Anti-immigration sentiment remains an active driver of community mobilization and presents potential risks to workforce movement, logistics and network access.

Localized Protest & Access Disruption
Protest activity, including election-period activity, can restrict access to infrastructure, delay maintenance and increase safety risks for field personnel.

Disinformation & Social Media Amplification
Social media can accelerate mobilization and amplify narratives during periods of social tension, increasing the speed at which localized events can develop.

COMRiC Assessment
Civil unrest risk remains elevated due to sustained social mobilization, economic pressure and localized tensions. The 4 November 2026 Local Government Elections may amplify this mobilization. The primary sector exposure is disruption to infrastructure access, field operations, logistics and personnel safety. COMRiC will continue to monitor these events and feed early warning into the sector's existing collective action framework.

Climate Risk

An emerging structural risk with active operational consequences for telecommunications infrastructure

ACTIVE IMPACT
Flooding & Infrastructure Damage:
Severe flooding events damage tower foundations, underground fibre routes, and access roads to remote sites. Post-flood recovery timelines are extending as incidents compound across multiple provinces simultaneously. Gauteng, KwaZulu-Natal, Eastern Cape and Limpopo present the highest exposure given infrastructure density and flood frequency.

STRUCTURAL
Heat Stress on Energy Infrastructure:
Sustained high temperatures reduce battery storage efficiency and accelerate generator wear at remote sites. This is particularly consequential given diesel generators now function as primary, not backup, resilience infrastructure. Heat events and load reduction events are increasingly occurring simultaneously, compounding site energy risk.

ESCALATING
Severe Weather Compresses Recovery Windows
High winds, lightning strikes, and extreme precipitation increase mean time to recovery across the national network footprint. Field access disruption during weather events reduces confidence in rapid site recovery, particularly in high-incident provinces already under pressure from infrastructure crime and diesel cost escalation.

INTELLIGENCE OBSERVATION
Uneven Provincial Exposure
COMRiC's sector intelligence confirms that climate risk preparedness is not uniform across participating operators or provinces. Operators with higher infrastructure density in flood-prone regions face materially higher exposure. This geographic unevenness creates an asymmetric resilience posture at sector level that warrants coordinated attention.

Current Sector Response Posture

What is already underway: COMRiC's aggregated intelligence on active resilience responses

The sector is not passive. COMRiC's intelligence aggregation confirms active responses across multiple resilience domains. The items below represent what is already underway, not what is recommended. They are presented without operator attribution in accordance with COMRiC's confidentiality mandate.

ACTIVE
Energy & Diesel Resilience
Diesel procurement strategies are under active review. Volume-lock pricing and hedging instruments are being explored in anticipation of the energy volatility. Solar and battery feasibility assessments are underway at high-consumption sites.

IN PROGRESS
SIM Card Registration Compliance
Active remediation planning is underway across the sector in response to strengthening RICA and the Department of Justice directive. Compliance frameworks are being developed within compressed timelines to mitigate material regulatory risk.

ACTIVE
Cyber Incident Response Enhancement
Following confirmed and heightened cyber threats, cyber incident response frameworks are being reviewed. Sector-level notification protocols are being explored to enable coordinated sector-level response to simultaneous threats. Cross-sector partnerships are being explored to enable cyber threat intelligence sharing.

ONGOING
Physical Infrastructure Protection
Enhanced physical security and surveillance strategies are being deployed across high-incident provinces. Recovery capability enhancement is prioritized in Gauteng, KwaZulu-Natal and Mpumalanga given disproportionate incident concentration.

PROGRESSING
Alternative Energy Transition
Solar and battery deployment programmes are progressing at operational sites to structurally reduce diesel dependency. This transition is driven by both cost management and operational continuity considerations.

ACTIVE
Sector Intelligence Coordination
COMRiC's sector intelligence programme is active. This report is itself an active resilience intervention enabling the sector to benefit from a synthesised, sector-wide risk view that no individual operator can independently produce within POPIA and competition law constraints.

SECTION TWO

Telecoms White-Collar Crime

How telecom fraud is changing shape — high volume hits at a lower loss per case
Subscription Fraud · SIM Swap · Social Engineering

COMRIC

Insights into Telecom Fraud and Social Engineering

Fraud against South African telecom customers and operators is not shrinking. It is changing shape, and this section explains how.

Over the twelve months to April 2026, subscription fraud accounted for 14,897 cases and R198.9 million in losses, while SIM swap fraud added a further R4.26 million across 383 cases. The pattern beneath those totals matters more than the totals themselves. Subscription fraud rose steadily from November onwards and peaked at 2,475 cases in March, with 63% of the year's cases falling in the second half. SIM swap losses tell a different story again: September 2025 alone accounted for 45% of the year's losses despite not being the busiest month, most likely a coordinated push against high-value banking and digital wallet accounts

.

A clear thread runs through both fraud types, and it is not the one the global headlines would predict. Internationally, syndicates are consolidating around fewer, higher-value targets. South Africa went the other way this year. Subscription fraud incidents rose 307% while the average loss per case fell 75%, from R52,500 to R13,400. SIM swap incidents rose 34% while loss per case fell 52%. Fraud here has become far more frequent and considerably cheaper per case — which is a detection, verification and capacity problem before it is a financial one. Counting cases alone would badly overstate the deterioration; counting rands alone would badly understate it. Both have to be read together.

Geographically, the fraud is heavily concentrated in cities. Gauteng alone accounts for 49% of subscription fraud cases and 55% of SIM swap cases, with Johannesburg and Pretoria doing the bulk of the damage. Four provinces carry 86% of subscription fraud and 85% of SIM swap cases. That concentration is useful, because it means investment in detection and prevention can be targeted rather than spread thinly across the country.

The most important finding is that human trust, not technology, is now the weakest link. Investigations into SIM swap cases repeatedly found signs of agent collusion, with fraudulent swaps processed outside normal hours to avoid scrutiny. More broadly, social engineering conducted over WhatsApp, phone calls and text messages has overtaken purely technical hacking as the leading way fraud gets into the system. As criminals increasingly use AI-generated voices and messages to sound convincing, the sector's defence cannot rely on firewalls alone. Staff training, customer awareness and tighter verification steps for account changes matter every bit as much as the technology sitting behind them.

Emerging Fraud Threats Shaping the Telecom Sector

Six fraud types shaping the threat landscape — 2026

1 AI Deepfake & Voice-Clone Fraud

Deepfake fraud projected +495% in 2026 vs. 2025 (Shufti)

Voice cloning can work from about 3 seconds of audio, enabling convincing vishing and impersonation scams.

2 Synthetic Identity Fraud

Synthetic identities now 11% of fraud — an 8× YoY increase (LexisNexis)

Identities built by blending real and invented data slip past KYC checks and telecom subscription verification.

3 SIM Swap Fraud

UK unauthorised SIM-swap filings up 402% in H1 2026 YoY (Cifas)

Hijacked numbers intercept OTPs, giving fraudsters a direct path into banking and social accounts.

4 SIM Box / Interconnect Bypass

2025 global bypass-loss estimate: US$1.92B (CFCA)

The latest estimate is 29% below 2019, but bypass still drains international termination revenue.

5 eSIM Provisioning Fraud

Risk centers on remote provisioning and account-recovery workflows

Fraudsters exploit social engineering around activation and recovery not the embedded SIM technology itself.

6 Smishing & AI-Enhanced Vishing

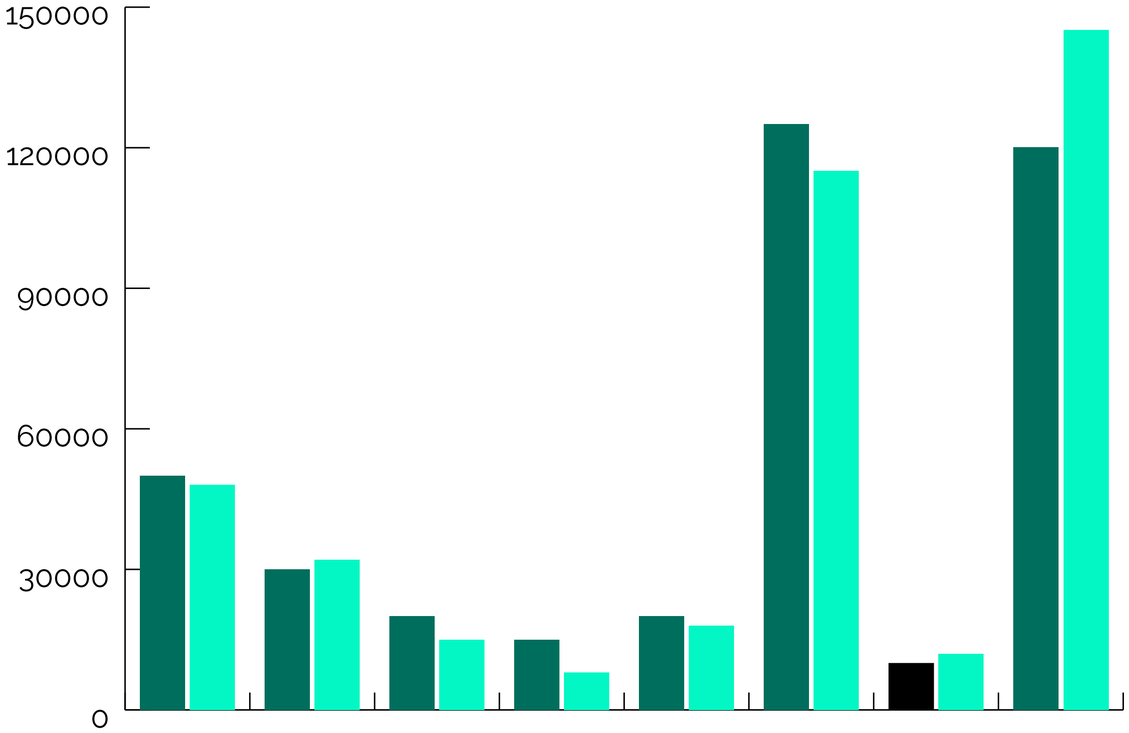
Romania: vishing was 42% of reported H1 2026 cyber incidents (DNSC)

CrowdStrike also found H1 2026 vishing intrusions doubled vs. H2 2025, reinforcing the shift toward trusted-channel abuse.

Sources: Shufti (2026) · LexisNexis (2026) · Cifas H1 2026 · CFCA (2025) · Romania DNSC H1 2026 · CrowdStrike (2026) · McAfee (2024)

The Surge in Fraudulent Calls Across the Global Telecoms

Total fraudulet mobile voice calls by region (mobile)



	North America	Latin America	West Europe	C & E Europe	Far East & China	Indian Subcontinent	Rest of Asia Pacific	Africa & Middle East
2026	50 000	30 000	20 000	15 000	20 000	125 000	10 000	120 000
2028	48 000	32 000	15 000	8 000	18 000	115 000	12 000	145 000

Why Fraudulent Calls Have Surged

Mobile voice fraud, particularly voice phishing (vishing), has grown steadily as attackers evolve from traditional fraud methods like IRSF to more sophisticated spam and AI-driven scam calls.
Fraudulent calls are expected to reach roughly 390 billion globally in 2026. Growth is not uniform: volumes are projected to keep rising sharply in Africa and the Middle East, while North America, Western Europe and the Indian Subcontinent are expected to decline by 2028 as blocking and authentication controls mature.

This reflects a fundamental shift toward more advanced, targeted, and high-volume fraud techniques that continue to impact both consumers and enterprises.

SOUTH AFRICA 2025 SIGNAL

3.0% of transactions involving South African consumers were suspected of digital fraud. Among consumers who lost money across email, online, phone and text scams, the median reported loss was R11,055.

Sources: TNS 2026; Juniper Research 2025; TransUnion South Africa, H1 2026 Top Fraud Trends

South Africa Telco Fraud Ecosystem – Q1 2026

Spam Volume

8.72B

spam calls in Q1 2026
March alone: 3.33B
1.92B spam messages

Multi-Channel Threats

Voice call spam
SMS spam
Messaging app scams
Social engineering

Blocking Gap

~60%

reached consumers
3.45B blocked but controls
failing against volume

Explosive Growth

150x

increase vs 2025
151M new spammers
identified in March 2026

Industry Response

Voice call spam
SMS spam
Messaging app scams
Social engineering

Impact on South African Telcos

The fraud ecosystem is driving direct financial damage across the telecoms value chain. Operators face accelerating revenue leakage from interconnect fraud and bypass routing, while network congestion from billions of spam calls degrades service quality for legitimate subscribers. Customer churn is increasing as consumer trust erodes; subscribers blame their provider when scam calls reach them. Overall reputational risk is rising, and regulatory pressure and growing compliance costs are compressing margins further. Through coordinated investment in fraud prevention, telcos can strengthen customer trust, protect revenue, and gain a long-term competitive advantage.

Truecaller, "The machine era of spam calls: the ten most spammed countries in the world" (2026).

Global Evolution of Social Engineering (2020–2030)

How fraud tactics have evolved from basic phishing to AI-driven autonomous attack ecosystems and Financial impact

TRADITIONAL
Generic phishing & fake bank alerts.
Basic impersonation scams.
Human-operated, low sophistication.

IMPACT
Identity theft & credential compromise.

TARGETED
Personalised phishing using social media data.
SIM swap & BEC growth
Multi-channel fraud emerges.

IMPACT
OTP interception & customer trust decline.

AI-ASSISTED
AI-generated phishing & vishing.
Deepfake voice technology.
Shift: systems human targeting.

MAJOR SHIFT
Cybercrime losses exceed US$10 trillion globally.

HYPER-PERSONALISED
AI voice cloning & deepfakes.
Synthetic identities at scale.
Real-time behavioural manipulation.

OBJECTIVE
Convince victims to willingly bypass their own security controls.

AUTONOMOUS
AI vishing megafarms.
Predictive fraud targeting.
Autonomous AI scam ecosystems.

FUTURE TARGET
Human behaviour becomes the primary attack surface.

TRADITIONAL
Pre-2020
$1Trillion

TARGETED
2020–2023
$6T–$8Trillion

AI-ASSISTED
2024–2025
$10Trillion (NOW)

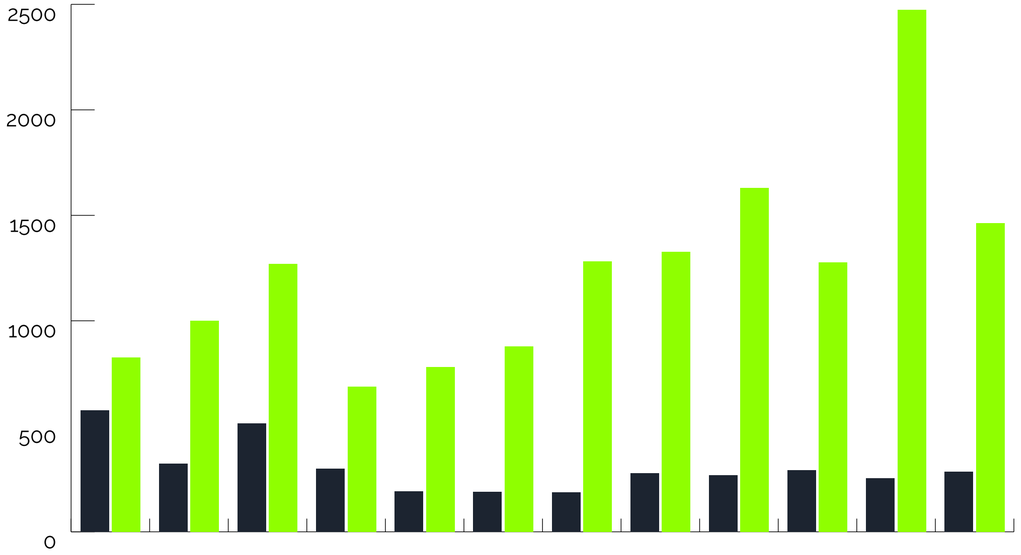
HYPER-PERSONALISED
2026 Projected
$11Trillion+

AUTONOMOUS
2027–2030 Projected
$15Trillion+

Annual Cost of Cybercrime To Reach 10.5 Trillion By 2025
Favicon type
SIM Swap Fraud Statistics 2026 | Losses, Trends, And Ta
2024 Cybersecurity Almanac: 100 Facts, Figures, Predict

The Scale of Subscription Fraud

Subscription fraud: May-Apr Year-over-year comparison



	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
May 2024 - Apr 2025	576	322	513	300	193	190	187	278	268	292	254	285
May 2025 - Apr 2026	827	1000	1269	689	780	878	1282	1326	1630	1278	2475	1463

Annual Volume

14 897

+307% vs prior year

Peak Month

2 475

March 2026

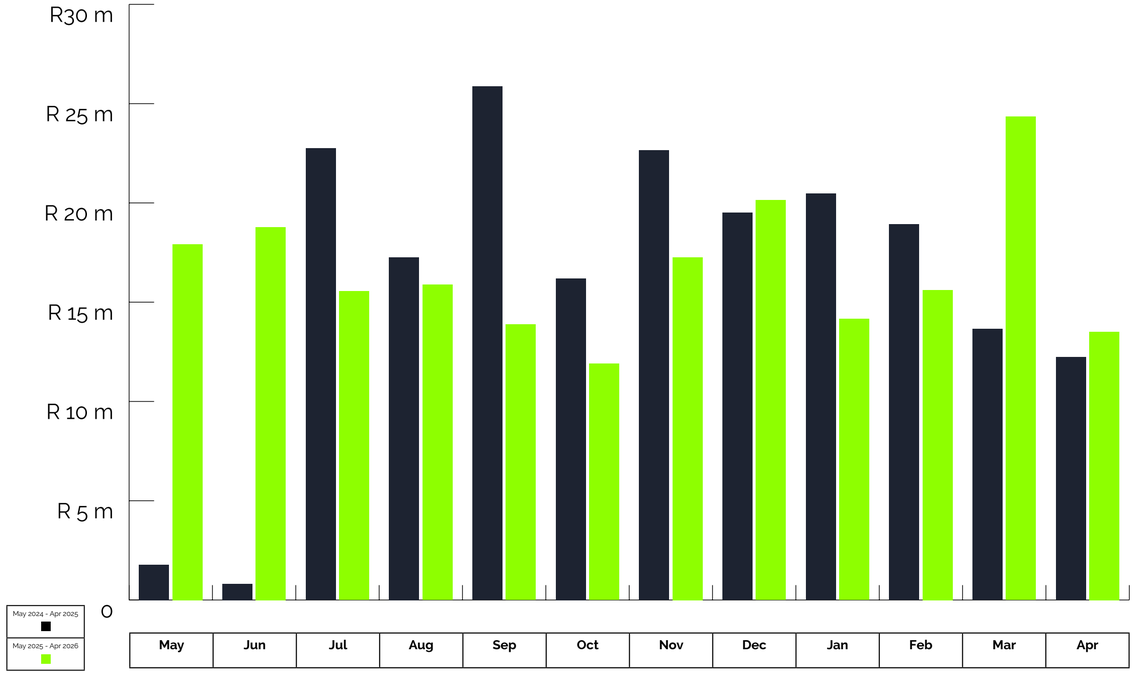
Second-Half Load

63%

of cases occurred
Nove 2025-Apr 2026

EXECUTIVE TAKEAWAY · Every month exceeded last year and 63% of cases occurred from November–April, confirming a sustained, industrial-scale threat rather than a seasonal spike.

Subscription Fraud: Financial Exposure



FY25/26 Annual Loss

R 198.9 m

+3.6% vs FY24/25 - R192.1 m

Peak Month

R 24.3 m

March 2026

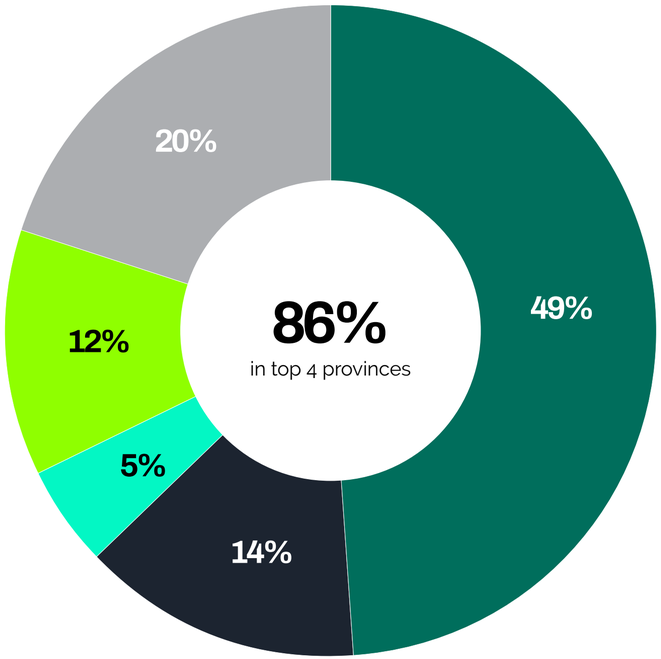
Loss / Case

R 13.4k

-75% vs R52.5k

EXECUTIVE TAKEAWAY · Annual loss rose just 3.6% while loss per case fell 75%; financial risk is now driven by scale, with March the peak month.

Provincial Breakdown of Subscription Fraud Incidents.



Where it lands
86% of reported fraud sits in just four provinces.

Why it spreads
The same stolen identities rotate between operators, creating a cycle of repeat fraud that drives financial losses, increases operational costs, and exposes multiple operators to the same criminal actors.

How we counter it
A shared verification API lets every operator screen sign-ups against the same fraud signals — turning scattered defences into one industry perimeter.

86% from just four provinces Gauteng, KwaZulu-Natal, Western Cape & Limpopo lead the caseload

Subscription Fraud

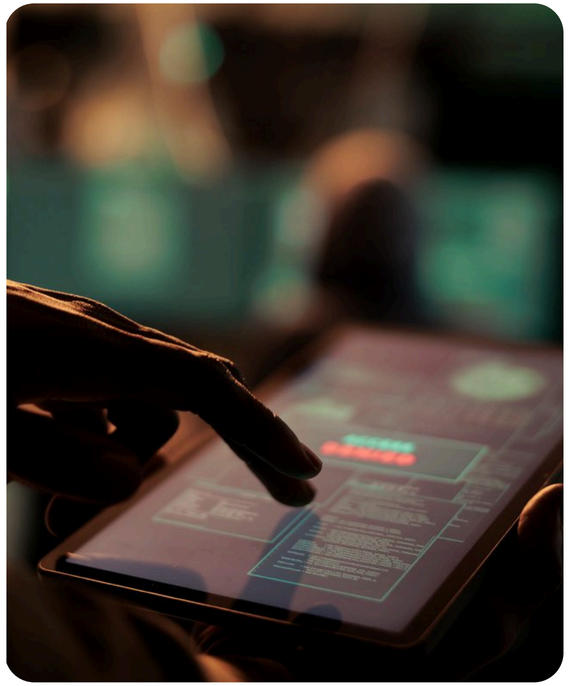
Subscription Fraud: May 2024–April 2025 Compared With May 2025–April 2026

What changed in subscription fraud

Subscription fraud increased from 3,658 to 14,897 incidents, a 307% rise more than four times the previous year's volume. Every month exceeded the prior year, and 63% of incidents occurred from November to April. March was the peak month at 2,475 cases, representing roughly one in six incidents reported during the year. Financial loss followed a different pattern: annual loss increased only 3.6%, from R192.1m to R198.9m, and March recorded the highest monthly loss at R24.3m. Because incident growth far outpaced loss growth, the volume figures show a sharp increase in frequency while total loss and loss per case show that average financial severity did not rise at the same rate. Overall, subscription fraud became much more frequent, with activity concentrated in the later months of the reporting period.

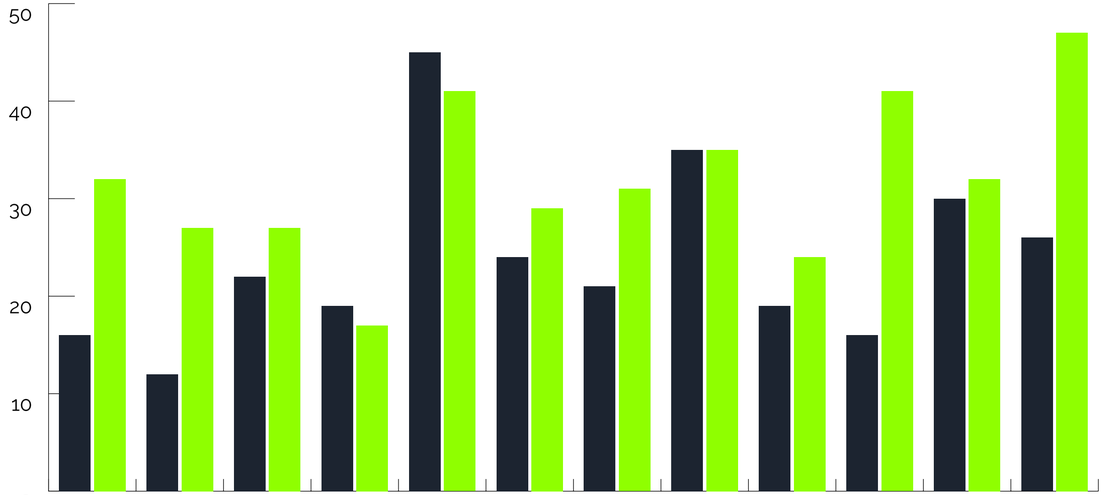
Subscription fraud led the increase in incidents.

The rise appears to be driven by increased misuse of stolen or synthetic identities, exploitation of digital onboarding processes, and greater availability of compromised personal information, resulting in a higher volume of fraudulent account applications.



The Rise of SIM-Swap Fraud

Sim-swap: May–Apr Year-over-year comparison.



	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
May 2024 - Apr 2025	16	12	22	19	45	24	21	35	19	16	30	26
May 2025 - Apr 2026	32	27	27	17	41	29	31	35	24	41	32	47

Annual Volume

383

+34% vs prior year

Peak Month

47

April 2026

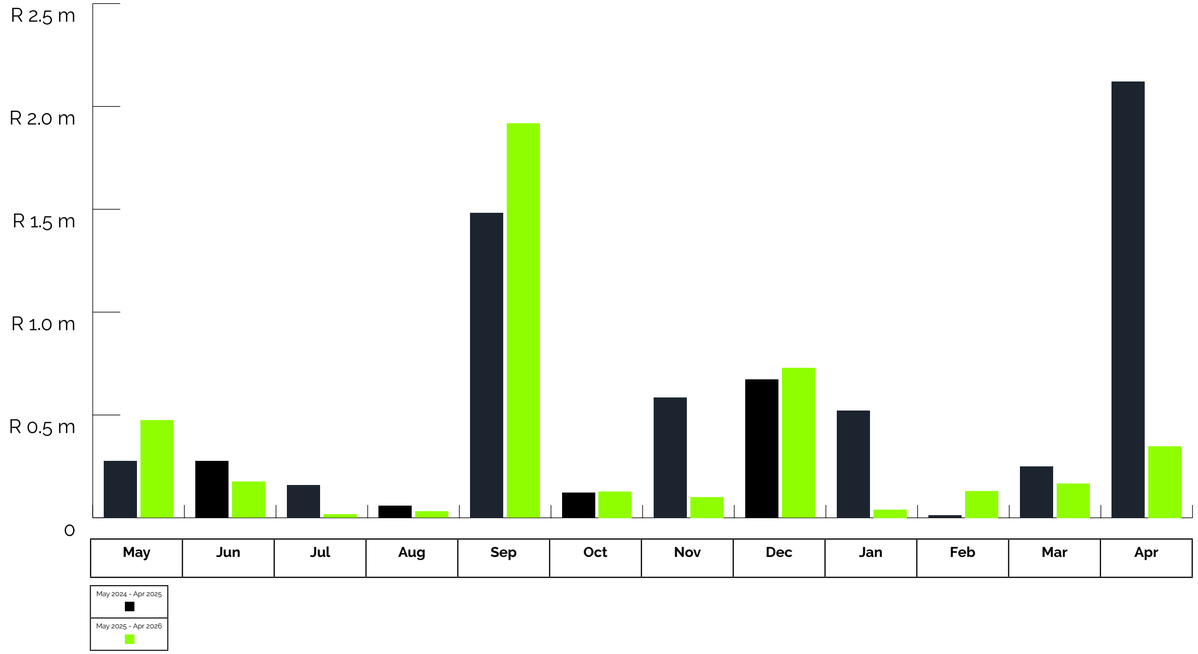
Breadth

9 of 12

months recorded increases

EXECUTIVE TAKEAWAY · Late-year momentum is building February–April reached 120 incidents, 67% above last year, while increases across 9 of 12 months show broad-based pressure

SIM-Swap Fraud: Financial Exposure



Annual Loss

FY24/25 R6.54m
FY25/26 R4.26m
−R2.28m | −35%

Average Monthly Loss

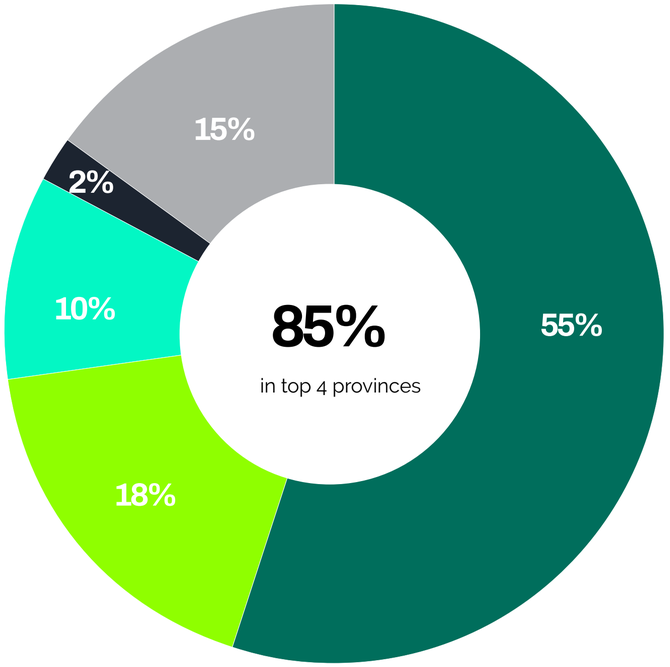
FY24/25 R545k
FY25/26 R355k
−R190k per month

Loss / Case

FY24/25 R23.0k
FY25/26 R11.1k
−52% Year over Year

EXECUTIVE TAKEAWAY · Annual loss fell R2.28m, the monthly run-rate fell R190k and loss per case halved. However, September still drove 45% of FY25/26 loss.

Provincial Breakdown of SIM-Swap Fraud Incidents.



Where it lands
Gauteng carries 55% of SIM swap incidents, with KwaZulu-Natal (18%) and Western Cape (10%) the next-largest hotspots.

Why it concentrates
Attacks follow the money — provinces with the highest subscriber density, banking activity, and transaction volume draw the most fraud.

What it means
With 85% of cases in just four provinces, focusing detection and awareness on these hubs delivers the widest risk reduction.

85% from just four provinces
Gauteng, KwaZulu-Natal, Western Cape & Limpopo lead the caseload

SIM-Swap Fraud

Sim-swap Fraud: May 2024–April 2025 Compared With May 2025–April 2026

What changed in SIM-swap fraud

SIM-swap fraud increased from 285 to 383 incidents, a 34% rise. Nine of the twelve months recorded higher volumes than the prior year. Financial losses moved in the opposite direction: annual loss declined from R6.54m to R4.26m (−35%), and average monthly loss fell from R545k to R355k. As incident numbers increased while total losses decreased, average loss per case dropped 52%, from R23.0k to R11.1k. September 2025 was the main exception to the broader pattern, accounting for 45% of the year's SIM-swap loss despite not having the highest incident count. This illustrates why incident frequency and financial severity must be read separately: the number of cases was generally higher, but losses were concentrated in a smaller number of months and the average value lost per case was lower..

Across the broader fraud landscape, the rise in SIM-swap fraud is driven primarily by social engineering, identity theft and the misuse of compromised customer information to take control of mobile numbers. The rise in SIM-swap fraud is primarily driven by social engineering, identity theft, and misuse of compromised customer information to take control of mobile numbers. Fraudsters use these attacks to intercept authentication messages and gain access to banking and other digital accounts.

Telecom Social Engineering: Trends & Tactics

MACRO TRENDS

AI is professionalising the scripts
Deepfaked voice notes and flawless phishing text are erasing the old tell-tale signs of a scam.

Social engineering is what drives SIM swap
Phished IDs and vished OTPs let fraudsters pass agent verification checks.

Fraud is consolidating, not just growing
Case counts fall in places while losses hold flat — syndicates shifting to fewer, higher-value hits.

Insider complicity is structural
Regional syndicates paying telecom staff per fraudulent SIM swap processed, not just external hacking.

Physical and digital crime are converging
Cable/battery theft and SIM-swap fraud increasingly read as one resilience problem, not two.

ATTACKER TACTICS

Phishing-then-vishing combo
Fake SMS/email harvests credentials, then a call posing as a bank or operator pressures an OTP.

Pretexting at retail & call centers
Fraudsters claim a lost or damaged SIM, armed with details from breaches or prior phishing.

Vendor / supplier impersonation
Spoofed emails claim changed banking details, increasingly polished with AI voice or email mimicry.

Fake prize & lucky-winner SMS
Links harvest OTPs and personal data, or route victims to premium-rate numbers.

Recruitment of "mules"
Vulnerable people paid for valid ID and banking details to open contracts anonymously.

Multi-channel delivery
SMS, WhatsApp and fake apps are the primary distribution channels across the region.

One entry point, three fraud outcomes: SIM swap, identity theft, and SIM box fraud

SOCIAL ENGINEERING TOOLKIT

Phishing SMS / Email

Vishing Calls

Breached ID Data

Insider Complicity

SIM Swap Fraud

Phished ID details plus a vished OTP let a fraudster pass agent verification and hijack the victim's number.

SIM Box Fraud

Stolen personal data (ID number, proof of address) is used to impersonate the victim across telecom, credit and banking touchpoints.

Identity Theft

Bulk SIM registrations under stolen or fake identities feed SIM box rigs that reroute calls and blast mass phishing SMS.

Key point: All three outcomes trace back to the same starting point — personal data obtained through social engineering which is why prevention must start upstream of SIM registration and verification, not just downstream of it.

Human behaviour is the attack surface

Confidence collapses when mobile contact feels familiar, credible and urgent

The behavioural paradox

85%
feel confident they can recognise scams

71%
of exposed adults still interact

35%
of interactors lose money

How the attack moves a person

- **Reach through familiar channels**
  SMS 56% | calls 51% | messaging apps 38%
- **Borrow legitimacy**
  Org impersonation 38% | realistic 33% | genuine 33%
- **Trigger emotion**
  Emotional pressure 20% | rushed / threatened 19%
- **Convert a small action**
  Open • answer • reply • click — before verifying.

Source: GASA, State of Scams South Africa 2026 | n=1,280

Social Engineering as an Enabler of Telecom Fraud

Social engineering remains one of the most significant enablers of fraud within the telecommunications sector. Unlike technical attacks that target systems and infrastructure, social engineering targets people by exploiting trust, urgency, and human behaviour. Fraudsters use deception to obtain sensitive information, bypass security controls, and gain unauthorised access to customer accounts and services. While trust-based interactions are fundamental to customer service and digital engagement, the same trust can be manipulated to facilitate fraud. As a result, social engineering has become a key enabling factor behind SIM swap fraud, subscription fraud, account takeover, identity theft, and broader financial crime.

In 2025/26, most fraud succeeds through social-engineering channels. The ranking below is risk-weighted — it reflects prevalence, impact and growth together, which is why WhatsApp ranks first even though SMS reaches more people. The consumer research on the previous page shows the reach picture: SMS 56%, calls 51%, messaging apps 38%.

Rank	Channel	Why it ranks here
1	WhatsApp	High trust, encryption, AI-enabled
2	Vishing	Urgency + voice impersonation
3	Smishing	Scale + automation
4	Email	High-value BEC fraud
5	Social Media	Entry & grooming vector

African Evolution of Social Engineering (2020–2030)

How SIM cards and mobile numbers became the centre of social engineering fraud across Africa and South Africa

TRADITIONAL
Fake bank SMS & missed-call scams.
Manual SIM swaps at retail stores.
OTP via SMS = trusted second factor.

IMPACT
SA mobile number = OTP gateway; early SIM hijack cases

Pre-2020

TRADITIONAL
Pre-2020
SA R2.2bn/yr

TARGETED
SIM swap +63% YoY; smishing via WhatsApp.
OTP interception drives mobile-banking fraud.
Pre-RICA'd SIMs fuel scam call farms.

IMPACT
SIM swaps = 60% of SA mobile banking fraud (COMRiC).

2020-2023

TARGETED
2020–2023
SA R3.3bn / Africa ~$4bn

AI-ASSISTED
3,600 SIM swaps processed in 4 months; 3% fraudulent.
Avg loss per SIM swap R10k; max >R500k.
Subscription & SIM-box fraud across telcos.

MAJOR SHIFT
SA telecom-linked fraud reaches R5.3bn/year (COMRiC)

2024-2025

AI-ASSISTED
2024–2025
SA R5.3bn / Africa $5bn (NOW)

HYPER-PERSONALISED
Cloned voices bypass mobile call-back checks.
Synthetic SIM identities & spoofed numbers.
Pre-RICA SIMs linked to 60% of extortion.

OBJECTIVE
The mobile number becomes the identity attack vector

2026

HYPER-PERSONALISED
2026 Projected
SA R8bn+ / Africa $7bn+

AUTONOMOUS
AI vishing megafarms dialling SA numbers.
eSIM & number-porting abused at scale.
Autonomous scam farms run on hijacked numbers.

FUTURE TARGET
Mobile number replaces password as primary attack surface

2027- 2030

AUTONOMOUS
2027–2030 Projected
SA R15bn+ / Africa $10bn+

SABRIC Annual Crime Statistics 2023 | COMRiC 2025 Telecommunications Sector Report | TransUnion Africa / BusinessTech | Sumsub 2025–2026 Identity Fraud Report
Smile ID 2026 Digital Identity Fraud in Africa Report | INTERPOL Africa Cyberthreat Assessment 2025 | GASA 2025 State of Scams in Africa Report
African Union / AFRIPOL (2024) | Check Point African Perspectives on Cyber Security 2025

The RICA Framework Agreement: Driving Compliance and Preventing Fraud

Sector value & fraud defence
The sector has entered the implementation phase of an industry-wide RICA Framework Agreement — an interim, industry-led safeguard developed with the aim to standardise SIM registration process and to further serve as a catalyst for crime prevention in the telecommunication sector, strengthening identity verification, while legislative reform is underway.

Benefits to the sector

Restored customer trust
Verified registration reassures customers their connection and identity are protected.

A level playing field
One standard across every operator removes weak links and closes unfair gaps.

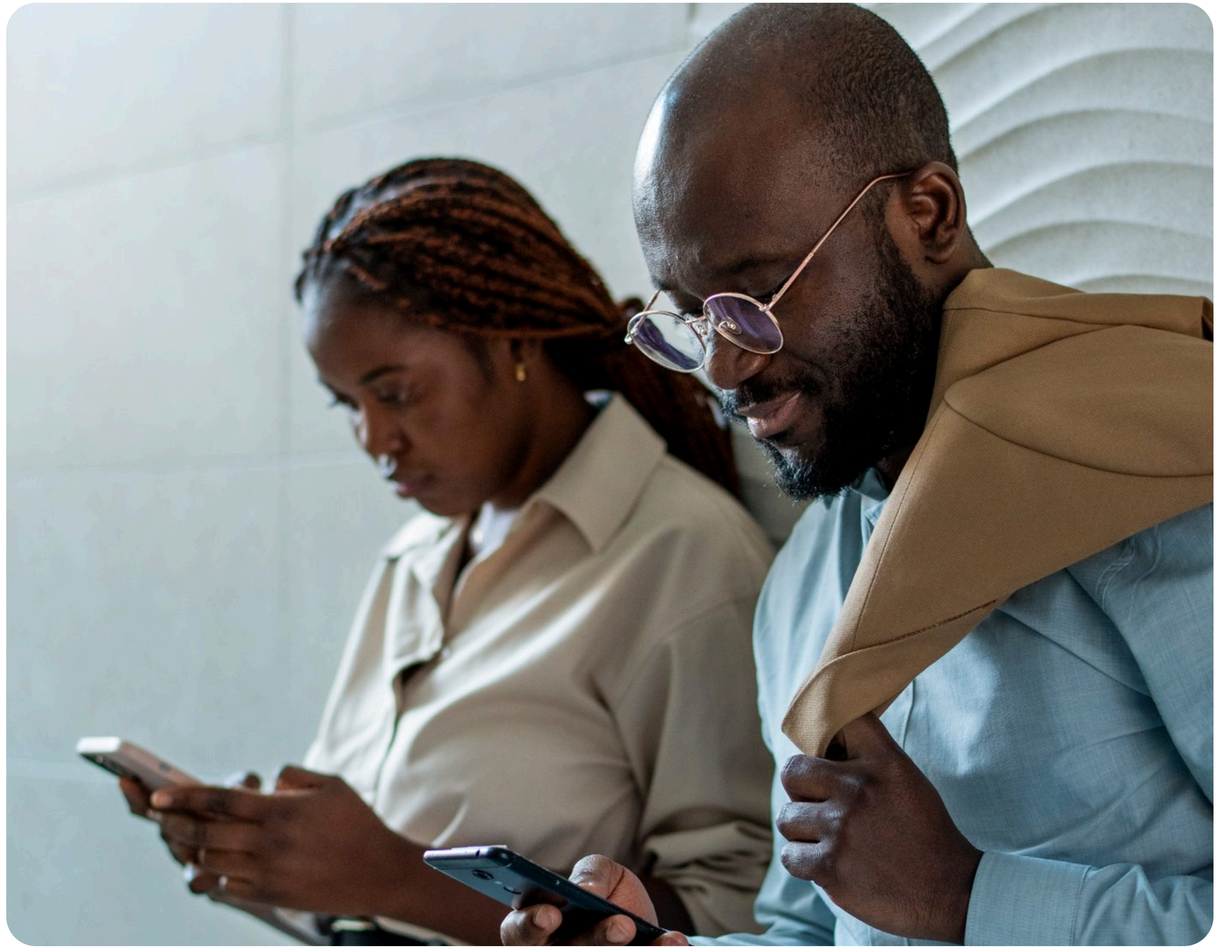
Ecosystem resilience
A verified SIM base underpins banking, mobile money and critical communication.

How it reduces fraud

Harder SIM-swaps
Stronger identity checks make it far harder to hijack a number and intercept OTPs.

Fewer fake registrations
Point-of-sale verification closes the anonymity that subscription and identity fraud exploit.

Faster detection
Traceable records let operators spot and shut down SIM-box and fraud patterns sooner.



SECTION THREE

Cybercrime on the Digital Frontline

Telecommunication Sector

Where the threats stand for South Africa's network operators across telecoms and beyond — and the real, evidenced progress now strengthening the country's cyber-resilience.

COMRIC

Cybersecurity Report

Cybercrime is now a significant operational and strategic risk for South Africa's telecommunications sector. As threats continue to evolve, network operators are facing growing exposure across their digital environments while enhancing their capabilities to prevent, detect and respond to cyber incidents.

The volume is the starting point. South African organisations absorb in the region of 8,850 cyberattacks a month, and telecommunications is now among the most-attacked sectors, with weekly attacks up 13% year on year. South Africa ranks fourth on the continent for attack volume.

The mix of threats matters more than the count. Ransomware remains the highest-volume threat at 140% of incidents, the average cost of a data breach reached R44.2 million, and a total of 171,812 DDoS attacks were recorded in the first half of 2026. Phishing and social engineering and third-party supply-chain exposure all continue to rise, with South Africa accounting for 70% of reported business email compromise detections in Africa. AI-powered malware is the leading concern going into 2026, with criminals using AI to make phishing, vishing, impersonation and SIM-swap attempts far more convincing.

INTERPOL's African Cyberthreat Assessment 2026 puts South Africa at the centre of this picture: the country accounts for 92% of Africa's ransomware detections and leads the data-breach comparison at 43.6%, ahead of Kenya at 11.9% and Nigeria at 9.1%.

The encouraging reality is that the telecommunications sector is actively strengthening its cyber resilience in response to an increasingly complex threat environment. Across the industry, organisations are investing in stronger security capabilities, modernising technologies and processes, improving threat monitoring, and enhancing their ability to detect, prevent and respond to cyber incidents. Greater emphasis is also being placed on workforce development, cybersecurity awareness, information sharing, and collaboration to reduce risk across the broader digital ecosystem.

Looking ahead, cybersecurity is expected to become an even more significant strategic and operational priority. As threats continue to evolve in scale and sophistication, organisations will need to further strengthen their resilience, accelerate the adoption of emerging security approaches, and enhance their ability to recover from disruptions. Success will increasingly depend on a combination of technology, skilled people, effective governance, and strong collaboration between industry, government and other key stakeholders to protect critical communications infrastructure and maintain trust in the digital economy.

Weekly Cyber Attacks on South African organisations and Across Africa

Indicators show that South African organisations continue to face a sustained and high-volume cyber threat environment, with the telecommunications sector experiencing a rise in weekly cyberattacks.

8 850
Cyberattacks on South African organisations per month

2 065
Attacks per week on South African organisations

~295
Attacks per day on Ssouth African organisations

Most-attacked countries in africa (weekly attacks)

Angola	4 890
Nigeria	4 361
Kenya	2 646
South Africa	2 065

South Africa ranked the 4th-most attacked country in Africa in 2026.

Most-attacked sectors in 2026 · telecommunications attacks increased by 13%

Education	4 890	+15%
Government	2 836	+5%
Telecommunications	2835	+13%
Kenya	2 601	+32%
South Africa	2 193	+24%

Weekly attacks per organisation have increased in 2026 compared to 2025

Reported by: Check Point Research — Global Average Weekly Cyber-Attacks per Industry & Region (2026), as cited by MyBroadband.

Key Cybersecurity Threats Affecting Network Operators

Network Operators (NOs), continue to operate in an environment characterised by increasingly sophisticated cyber and physical threats. These threats can compromise network infrastructure, disrupt services, facilitate fraud, and expose subscribers to financial and identity-related risks.

1

AI-Driven Fraud and Social Engineering:

Criminals are increasingly using AI to create more convincing phishing, vishing, impersonation, and SIM-swap schemes, targeting both subscribers and employees.

2

Synthetic Identity Fraud

International campaigns, including Salt Typhoon, highlight the growing threat to telecommunications core, edge, and network management infrastructure, with attackers seeking persistent access and sensitive information.

3

SIM Swap Fraud

SIM-swap, impersonation, and identity-related fraud remain key concerns, particularly where compromised mobile accounts can be leveraged to gain access to financial and mobile-banking services.

4

SIM Box / Interconnect Bypass

Nos' infrastructure remains exposed to DDoS and other attacks designed to overwhelm systems, degrade network performance, or interrupt critical services.

5

Ransomware

Ransomeware attacks - continue to pose a significant threat to network operators, casuing data encryption, service disruption, financial loss and reputational damage.

Cybersecurity Threats in South Africa

The reported cyber threat statistics highlight the significant cyber risks affecting South African organisations, including the telecommunications sector. Drawing on information from multiple credible sources, the figures illustrate the scale, frequency, and impact of cyber threats across the sectors.

Ransomware
+140%
Confirmed attacks · H1 2026
+ R17M ransom

Data breaches
R 44.2 m
Average breach cost · 2025
17% YoY

DDoS attacks
171 812
South Africa · 2025 Average attack duration >74 min
Prolonged service disruption risk

Third party supply chain attack
17%
Of incidents · 2025
R29.6M avg cost

Phishing and Social Engineering
45.7%
Of detected threats · H2 2025
Rising

Malware
+6 m
Attack attempts · H1 2025
Rising

AI threats
68%
Cited as top 2026 concern
Rising

Business Email Compromise (BEC)
70%
Reported share of Africa BEC detections
South Africa

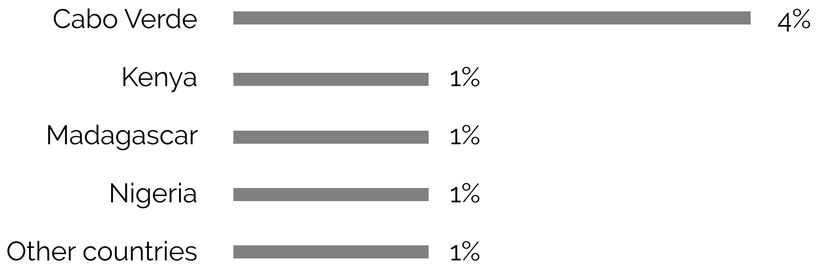
Source: IBM 2025 Cost of a Data Breach Report; Kaspersky (2025) Ransomware in South Africa: Response & Protection Guide 2026 "Phishing & Social Engineering are the most Significant Risks for South African organisations organizations" - IT News Africa - African Business Technology News PwC — Digital Trust Insights Survey 2026 (South Africa). Green ID book fraud climbed 400% in South Africa – MyBroadband https://www.itweb.co.za/article/itwebgrc2025-tackling-third-party-supply-chain-cyber-risks/KBpdg7pmORmMLEew

South Africa Remains Africa's Most Targeted Cyber Threat Landscape

According to INTERPOL's African Cyberthreat Assessment Report 2026, South Africa has shifted from an opportunistic target to a high-value hub for industrialised attacks and leads the supplied data-breach comparison at 43.6%.

Ransomware Detections · Share Of Africa
South Africa Vs The Continental Remainder

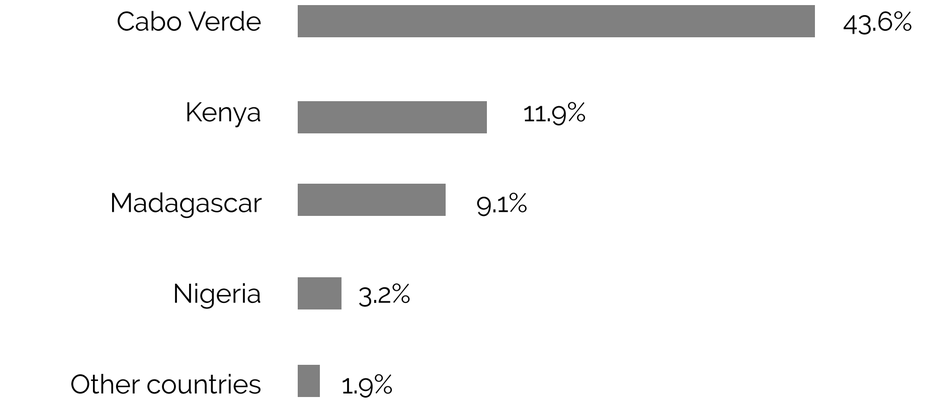
Inside the remaining 8%



South Africa has emerged as Africa's cybercrime epicentre - the continent's central target for sophisticated cyberattacks and transnational threat actors.

Reported by: INTERPOL — African Cyberthreat Assessment Report 2026 (figures supplied).

Ransomware Detections · Share Of Africa
South Africa Vs The Continental Remainder



South Africa and Kenya recorded the highest exposure, with threat actors primarily targeting outdated routers, vulnerable VPNs and misconfigured web platforms.

The Cybersecurity Skills Gap in Telecommunications Sector & South African Organisations

A shortage of qualified professionals in telecommunications and South African organisations raises both operational risk and the cost of staying secure.

Projected skill gap for telecommunications sector

40 000

According to the South Africa Cybersecurity Market report, Projected shortfall of cybersecurity professionals in South Africa's telecommunications sector.

Why the skill gap rises

Higher operational risk
A lack of qualified personnel leaves network operators more exposed and slows incident response.

Rising costs
Operators are forced to invest in training or outsourcing, complicating cybersecurity strategy.

South african organisation addressing cyber talent gaps

According to PwC, South African organisations are increasingly adopting technology-driven solutions to address cyber talent gaps. AI and machine learning tools are the most prioritised response.

72% AI and Machine Learning Tools

66% Cybersecurity Tool Consolidation

56% Upskilling and Reskilling

35% Security Automation Tools

27% Traditional Talent Recruitment

24% Managed Services

How south african network operators are building a cybersecurity talent pipeline

Education access
Bursaries widen access to relevant tertiary study and digital careers.

Early-career entry
Internships and learnerships build practical experience and workplace exposure.

Capability building
Skills academies and certifications build cloud, network, data and cybersecurity capability.

Role transition
Structured pathways move emerging talent into technical, security and permanent roles.

Future Outlook: Cybersecurity in Telecommunications and Beyond

Looking beyond 2026, telecommunications operators are expected to invest more in AI, identity protection, skilled people, resilient networks and future-ready security.

AI will transform attacks and defence
Operators are expected to use AI more widely to manage networks, detect threats and respond faster. Criminals will also use AI for convincing phishing, deepfakes, fraud and automated attacks.

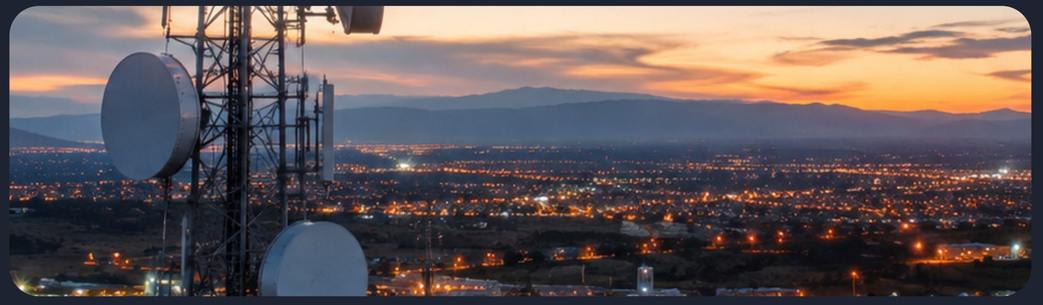
Digital identity protection will be a priority
Mobile numbers will remain central to login, one-time passwords and account recovery. Operators will strengthen controls against SIM-swap fraud, identity theft and account takeover.

Skills shortages will reshape the workforce
Cybersecurity talent will remain scarce. Operators will rely more on automation, managed security services, upskilling and partnerships while building specialist security teams.

Regulation and resilience demands will rise
Operators will face stricter requirements for incident reporting, data protection and service continuity. Investment will expand from preventing attacks to recovering quickly when they occur.

Network security investment will rise
Spending is expected to increase as operators protect essential infrastructure from more sophisticated fraud, identity attacks and cyber threats.

Future-ready security will expand
Operators are expected to increase investment in Zero Trust security, cloud security, and next-generation encryption technologies as they prepare for emerging cyber threats and future risks associated with technological advancements.



What the future outlook means: Telecommunications operators will need to strengthen protection faster than threats evolve, while showing regulators, customers and partners that their networks can withstand and recover from attacks.

How Network Operators Are Responding to Cybersecurity Threats

Network Operators (NOs) are implementing a range of responses and initiatives to strengthen cybersecurity and combat cyber threats. These initiatives aim to improve resilience against evolving cyber threats, safeguard customers, and maintain the integrity of telecommunications networks.

1. Strengthening SIM and Number Security:
Telecommunications are enhancing controls around SIM registration, SIM swaps, number portability, and the management of inactive numbers to reduce opportunities for identity and mobile-enabled fraud.

2. Enhanced Fraud and Identity Protection:
Network Operators s are improving detection and prevention of SIM-swap fraud, SIM cloning, impersonation and mobile-enabled identity theft.

3. Deploying Advanced Threat Detection:
Operators continues to expand the use of AI, automation, threat intelligence, network monitoring and vulnerability management to respond faster.

4. Protecting Critical Network Infrastructure:
Network Operators are strengthening controls around core networks, edge infrastructure, third-party environments, and other critical systems to improve service availability and resilience.

5. Awareness and Campaigns:
Telecommunications conduct cybersecurity awareness initiatives and phishing simulation campaigns to strengthen cyber resilience. These programmes cover a range of cybersecurity topics, including phishing, social engineering, password security, ransomware, identity theft, SIM-swap fraud, and emerging cyber threats.

6. Legacy Infrastructure Modernisation:
Telecommunications are accelerating the migration and security hardening of legacy and unmanaged systems to reduce vulnerabilities and improve overall cyber resilience.

7. Improving Incident Response:
Network Operators are prioritising earlier detection, rapid containment, regulatory notification and post-incident learning.

8. Stronger Regulatory and Industry Collaboration:
Engagement between Network Operators, ICASA, government, financial institutions, law enforcement, and cybersecurity bodies is increasing to address fraud, numbering abuse, cybercrime, and emerging network threats.

9. Cybersecurity Capabilities to Address Emerging Skills Gaps:
Operators are using bursaries, internships, learnerships, skills academies and career pathways to move talent into technical and security roles.

SECTION FOUR

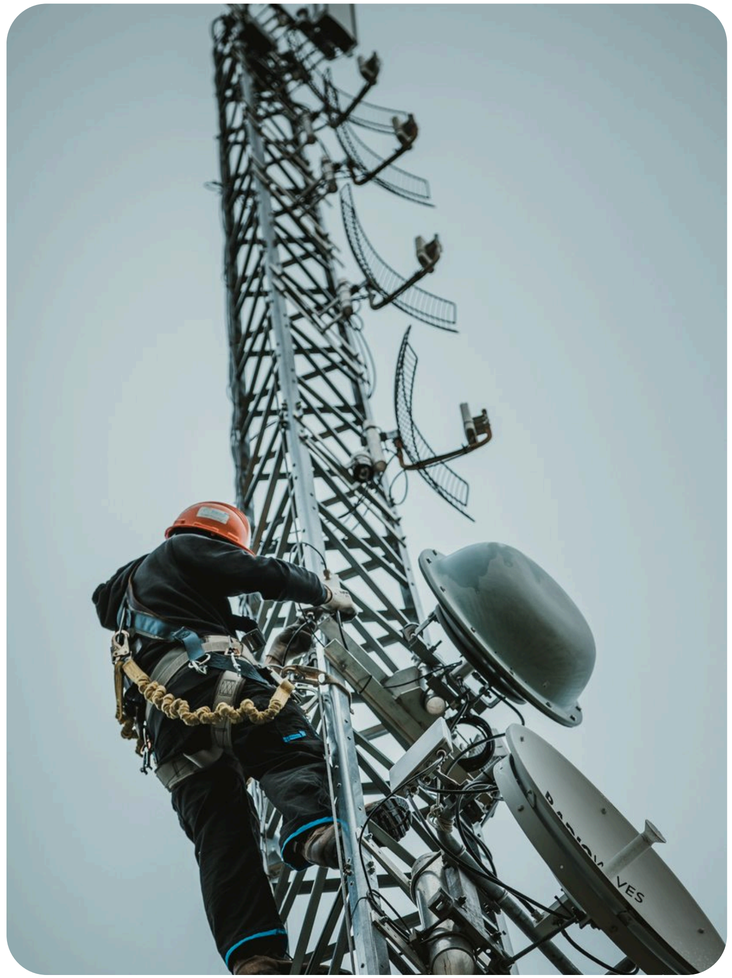
Infrastructure Crime

Infrastructure Crime

FY2024/25 vs FY2025/26 · Incidents down 40% · Losses down 63%

COMRIC

Infrastructure Crime Report



Physical infrastructure crime — cable theft, vandalism and battery theft — has been one of the most persistent costs facing the telecom telecommunications sector and this section compares the last two financial years to see what is working.

The headline is genuinely positive. Incidents fell from 15,917 in FY2024/25 to 9,579 in FY2025/26, a drop of 40%, while financial losses fell 63% over the year, from R618.8m in FY 2024/25 to R231.7m in FY 2025/26.. Prevention is part of the reason: 1,759 of 11,338 recorded incidents, roughly 1 in 6 or 15.5%, were stopped before completion, which points to genuinely better prevention and response, not just a lucky year.

Gauteng remains the country's clear infrastructure crime hotspot in both years, though even there the numbers have improved sharply, falling from 4,205 incidents to 2,624. KwaZulu-Natal (2,281) and the Western Cape (1,184) are the next highest-risk provinces, while North West recorded the steepest fall, down 83.8% from 2,721 to 442. The Western Cape is the one to watch: it is the only province where incidents rose, more than doubling year on year (553 to 1,184), a possible sign of displacement toward the Cape. The type of crime driving losses has also shifted. Property crime and vandalism remains the single biggest category at 3,720 incidents (38.83%), but copper cable theft stays chronic at 3,075 incidents (32.10%) and around 256 a month, while battery theft fell 90% and armed-response call-outs 86% — showing that as one

and around 256 a month, while battery theft fell 90% and armed-response call-outs 86% — showing that as one
type of crime is brought under control, criminal activity tends to move rather than disappear entirely.

The weaker part of the picture is law enforcement follow through. Of 1,280 suspects arrested over the period, only 291 resulted in a conviction, a rate of just 22.7%. That gap between arrests and convictions matters a great deal because it means many offenders are likely returning to target the same kind of infrastructure again, which limits how much deterrent effect all that prevention spending can really have.

Looking ahead, COMRiC's intelligence points to eight emerging threats worth watching closely, including more sophisticated criminal syndicates, insider collusion, construction related crime rings, and cross border criminal networks. None of these are reasons to think prevention efforts are failing, quite the opposite. The 40% drop in incidents and 63% drop in losses shows real progress. But they are a reminder that the job is not finished. The report's recommendation is straightforward: keep funding the prevention work that is clearly paying off, push hard to convert more of the 1,280 arrests into convictions, and stay alert to crime shifting into new categories and new regions rather than assuming today's improvement will continue on its own.

Year-on-year comparison

Declines confirmed across incident counts, crime categories and rand value — but far from uniform across provinces.

Total incidents

15 917 FY2024/25

40%

9 579 FY2025/26

Financial losses

R618.8m FY2024/25

63%

R231.7m FY2025/26

Broad-based decline

40%

North West collapsed 83.8% (2,721 »» 442)

Copper stays chronic

256 FY 2025/26 monthly average

Steepest improvements

90%

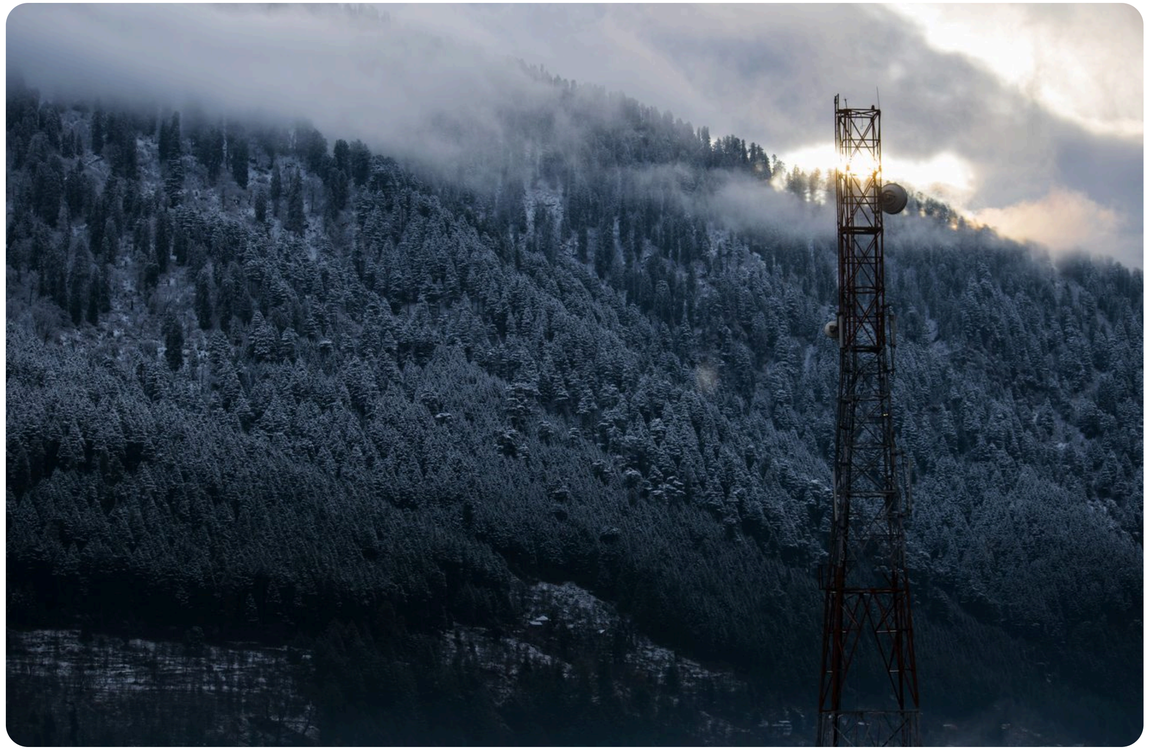
Battery theft; armed response 86%

Watch displacement

+114% Western & Northern Cape more than doubled

What the trends tell us
Broad-based decline · copper cable stays chronic · watch for displacement to the Cape

BOTTOM LINE: Incidents fell 40% and losses 63% year-on-year, with the steepest gains in battery theft and armed response — but copper stays chronic and rising cape provinces signal displacement, so extending prevention to lagging provinces is the priority.



Where incidents fell and where they shifted

Provincial incident trends · May 2024–Apr 2025 vs May 2025–Apr 2026

National decline
-40%
15,917 ››› 9,579 incidents

Steepest fall
9579
North West · 2,721 ››› 442

Biggest riser
+114%
Western Cape · 553 ››› 1,184

Top hotspot
Gauteng
2,624 incidents · still #1

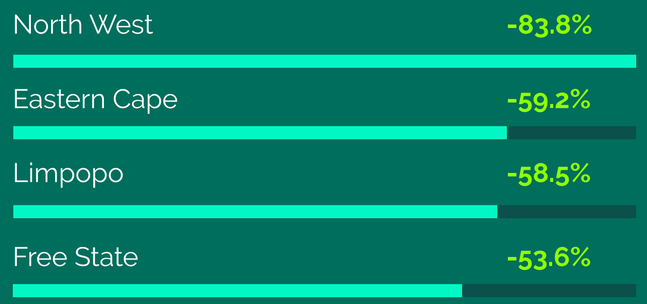
Provinces - FY2024/25

Gauteng	4205
North West	2721
Eastern Cape	2613
KwaZulu-Natal	2591
Limpopo	1512
Mpumalanga	992
Western Cape	563
Free State	521
Northern Cape	209

Provinces - FY2025/26

Gauteng	2624
KwaZulu-Natal	2281
Western Cape	1184
Eastern Cape	1067
Mpumalanga	953
Limpopo	628
North West	442
Free State	242
Northern Cape	158

Fastest declines (YoY %)



BOTTOM LINE Incidents fell 40% nationally (15,917››› 9,579). North West saw the steepest drop (-83.8%), while Western Cape bucked the trend (+114%) — a possible sign of displacement toward the Cape.

How incident types moved through the year

Monthly incidents by category · May 2025 – Apr 2026

Sharpest turnaround

90%

Battery Theft · 204 ››› 19
(Sep 2025 Apr 2026)

Total incidents

9579

6 categories · FY2025/26

Steady erosion

86%

Armed Response · 155 ››› 22
(Sep 2025 Apr 2026)

#1 Category

38.83%

Property Crime – Breach/ Vandalism

Categories by annual volume FY25/26		Share of incidents FY25/26
3720	Property Crime	38.83%
3075	Copper Cable Theft	32.10%
1084	Battery Theft	11.32%
993	Armed Response	10.37%
588	General Theft	6.14%
119	Fuel Theft	1.24%

BOTTOM LINE: The year's story is decline — battery theft fell 90% (204 ››› 19) and armed-response call-outs dropped 86% (155 ››› 22) from September 2025 to May 2026, the two sharpest turnarounds of the year.

Quarterly Improvement: Losses fell every quarter

Rolling three-month totals fell every quarter — from R73.5M to R42.2M, a 43% reduction across the year.

Total losses

R231.7m
FY2025/26 · Q1–Q4

Quarterly losses

R73.5m
May - Jul (peak)

▼ **43%**

R42.2m
Feb - Apr (least)

Q1 · MAY–JUL	Q2 · AUG–OCT	Q3 · NOV–JAN	Q4 · FEB–APR
R73.5m	R64.7m	R51.3m	R42.2m

BOTTOM LINE: Quarterly losses fell every quarter — from R73.5M (May–Jul) to R42.2M (Feb–Apr), a 43% reduction and R31.3M less value lost as the year progressed.

Attempts Prevented vs Incidents Completed

1 in 6 incidents was stopped before completion — evidence that security, monitoring and rapid response are disrupting attempts.

Incident outcomes FY2025/26

1 759
Prevented

9 579
Completed

Prevention rate FY2025/26

11 338
Total recorded

15.5%
Prevented

Provincial training

Structured
typologies · site hardening escalation

Prevention measures

1 in 6
security · monitoring · rapid response

Programme awareness

Faster
detection & reporting cuts attack window

Programme awareness

Faster
detection & reporting cuts attack window

WHAT THIS TELLS US: Prevented attempts concentrate where operator and law-enforcement teams have completed structured training and sustained community awareness — shortening the window attackers have to complete a theft.

BOTTOM LINE: Roughly 1 incident in 6 (1,759 of 11,338) was stopped before completion and prevented attempts cluster where operator and law-enforcement teams have completed structured training.

Where we're winning and where to focus next

1 in 6 incidents was stopped before completion — evidence that security, monitoring and rapid response are disrupting attempts.

Overall direction

▼ **40%**
Incidents

▼ **63%**
Losses

Prevention

1 759
Prevented

15.5%
Rate

Where it's working

40% ▼
national incidents · North West 84%

Biggest wins

90% ▼
battery theft; armed response 86%

Where to improve

Copper
chronic ~223/mo · KZN high-volume hotspot

High risk

+114%
Western Cape rising — possible displacement

Emerging Threats

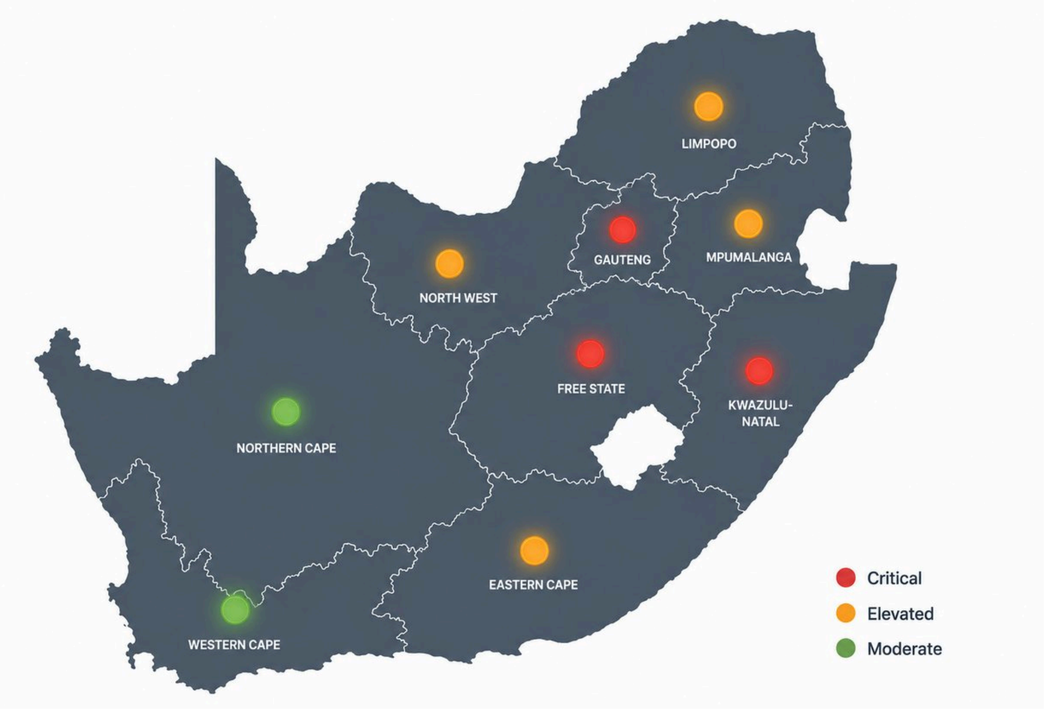
The next wave of risk facing the telecommunications sector

Despite progress, the threat landscape continues to evolve — eight emerging risks demand active monitoring.

#	Emerging Threat	Severity
1	Sophisticated Syndicates	■■■■■
2	Internal Collusion	■■■■■
3	Construction Mafia	■■■■■
4	Cross-Border Networks	■■■■□
5	Escalating Copper Theft	■■■■■
6	Deliberate Sabotage	■■■□□
7	Load-Shedding Attacks	■■□□□
8	Complex Criminal Methods	■■■■□

Priority: Intelligence-led, multi-operator coordination is essential to stay ahead of evolving criminal methods.

Provinces that will be affected by emerging threats



Arrests & Convictions

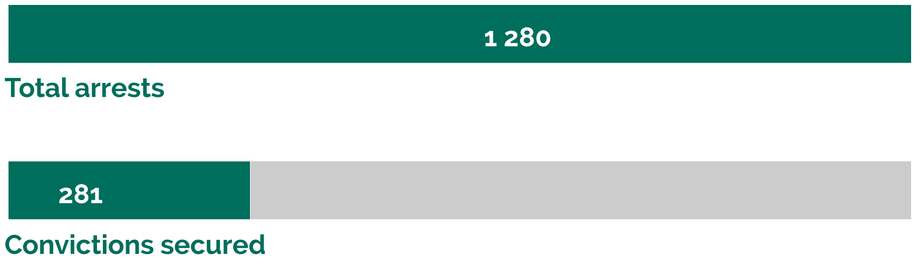
Enforcement outcomes across telecommunications

Total suspects arrested:
1 280

Total convictions secured:
291

Conviction rate:
22.7%

Arrest-to-conviction conversion:



Conviction rate 22.7% just 291 of the 1,280 suspects arrested resulted in a conviction.

Interventions
- Syndicate disruption operations
- Armed response deployments
- Hotspot intelligence operations

Ongoing challenges
- Repeat offenders receiving bail
- Withdrawn cases
- Slow prosecutions
- Inconsistent conviction outcomes

Opportunities & Collaboration

Partnership pathways to disrupt the criminal economy

With incidents down 40% and losses down 63%, coordinated action protects the gains and unlocks the next stage of impact.

01 INDUSTRY: Cross-Operator Intelligence
Shared hotspot & syndicate data
Track the chronic ~223/mo copper theft
Early-warning on Cape displacement (+114%)

02 GOVERNMENT: Public-Private Partnership
Tighter scrap-metal regulation
Critical-infrastructure legislation
Protect the R31.4m reduction in quarterly losses.

03 ENFORCEMENT: Joint Operations
Lift the 22.7% conviction rate
SAPS syndicate-disruption task forces
Convert more of the 1,280 arrests

04 COMMUNITY: Community Engagement
Sustain awareness behind the 15.5%
Local watch near rural hotspots
Trusted tip-off & reporting channels

05 TECHNOLOGY: Innovation & Analytics
AI monitoring to hold the 40% decline
Asset tagging on high-value copper
Drone & remote surveillance scaling

06 SECTOR: National Sector Forum
Unified incident reporting standards
Extend gains to Gauteng, KwaZulu-Natal & the Western Cape province
Coordinated policy to protect the 63% drop

Stakeholder Engagement

How COMRiC convenes operators, regulators, law enforcement and society around a shared risk picture

Member Operators · Regulators · Law Enforcement · Government · Cross-Sector Partners · Communities

COMRiC

Stakeholder Engagement Overview

No single operator can see the whole risk picture, and none can fix a sector-wide problem alone. Stakeholder engagement is therefore not a side activity for COMRiC — it is the mechanism through which sector-wide intelligence is gathered and collective action becomes possible. This section sets out who COMRiC engages, how, and to what end.

The engagement model rests on competitive neutrality. As a neutral sector body, COMRiC can aggregate confidential intelligence from competing operators without any single business compromising its position, and no source-specific finding is ever attributed. That trusted position is what allows the founding operators — Cell C, Liquid Intelligent Technologies, MTN, Telkom and Vodacom — to share openly, and it underpins the four intelligence streams feeding every section of this report.

Engagement reaches well beyond the members. COMRiC works with regulators and policymakers at ICASA, the Department of Communications and Digital Technologies and the Department of Justice; collaborates with law enforcement through the SAPS, the Hawks, the NPA and Interpol; and convenes cross-sector partners across banking, business and civil society. Each relationship exists because telecom risk now spills across industry and institutional boundaries.

The agenda is deliberately holistic. It spans regulatory and policy advocacy, joint operational action against infrastructure and fraud crime, closing the arrests-to-convictions gap in the criminal justice system, and public awareness that reaches ordinary consumers and the communities living alongside telecom telecommunications sites — one connected effort to keep the sector resilient rather than separate workstreams.

Looking ahead, COMRiC intends to widen this orbit further — expanding partnerships beyond the founding five, engaging adjacent industries, deepening public-sector collaboration and drawing civil society more firmly into collective action. The pages that follow map the stakeholder ecosystem, set out how COMRiC engages, and translate what the report exposes into what COMRiC is building in response.

The Stakeholder Ecosystem

Six groups COMRiC engages to build one shared, sector-wide view of risk

Telecommunications risk crosses every industry and institutional boundary, so COMRiC engages a broad ecosystem rather than a single audience. The six groups below each contribute a different piece of the picture — and each depends on COMRiC's neutrality to take part without competitive or legal exposure.

FOUNDING FIVE | Member Operators
Cell C, Liquid Intelligent Technologies, MTN, Telkom and Vodacom. The industry needed one structured, trusted forum where operators act as risk partners on shared threats. Competing on service and price is compatible with cooperating on survival.

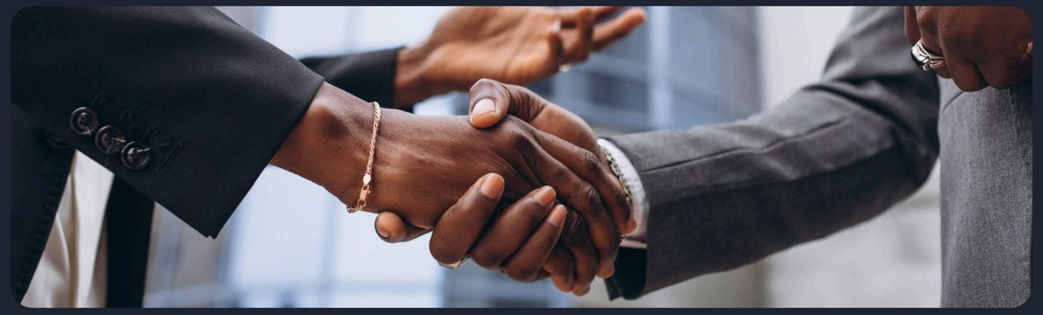
REGULATORS | Regulators & Policymakers
ICASA, Information Regulator, Competition Commission, the DCDT and the Department of Justice amongst others. COMRiC tracks the pace, direction and cumulative burden of regulation and advocates for workable, harmonised rules across the sector. Collaboration with the same institution is critical for collective resilience of the sector.

ENFORCEMENT | Law Enforcement & Justice
Collaboration and partnering with various law enforcement agencies including outside the borders of South Africa is critical to sector intelligence. Joint action targets syndicates and works to convert arrests into convictions and stronger deterrence.

GOVERNMENT | Government & Public Sector
Engagement aligns sector resilience with national security, disaster response and digital-economy goals. A structured, credible interface makes the sector easier to engage, not harder.

CROSS-SECTOR | Industry & Business Partners
Financial services, eEnergy providers, and business bodies such as, Business Against Crime, IRMSA, aAcademic institutions and the Association of Comms and Technology. Shared exposure calls for shared defences.

COMMUNITY | Communities & Civil Society
Community Police Forums, civil society groups and the consumer public. Awareness campaigns and community-based reporting help protect infrastructure and reduce trust-based fraud.



How COMRiC Engages

A neutral, structured and confidential model that turns individual insight into collective action

COMRiC's engagement is built to work across competitors and institutions without compromising anyone. Four principles govern how it convenes stakeholders and translates what it hears into sector-wide intelligence and coordinated response.

Competitive Neutrality
As an independent sector body — chaired by an independent non-executive — COMRiC sits between competing operators without compromising their competitive edge. That neutrality is what makes candid intelligence-sharing possible in a competitive market.

Confidential Aggregation
Intelligence is pooled across four streams — sector engagement, regulatory monitoring, global risk-signal analysis and incident data — and reported only in aggregate. No source-specific finding is attributed to an individual operator.

Structured, Regular Cadence
Engagements run on a regular cycle rather than only in a crisis, surfacing operational intelligence not visible in public data and giving the sector an early-warning view of risks as they converge.

From Insight to Collective Action
Engagement exists to enable action — aligning members, regulators and law enforcement around a shared picture so the sector responds together rather than each operator fighting the same battle alone.

Neutrality is the point, not a by-product: because COMRiC favours no operator, competitors will share the very intelligence that protects them all.

Our Partners

We extend our gratitude to our founders, industry alliances and partners for their indispensable support, expertise, and collaboration throughout the years. Your commitment has been instrumental in advancing our shared goals and driving meaningful impact within our sector

Our Founders

vodacom
Telkom
MTN
cellC
LIQUID INTELLIGENT TECHNOLOGIES

Our Collaborators

SABRIC
South African Police Service
SAFPS Southern African Fraud Prevention Service
HAWKS Directorate for Priority Crime Investigation
Business Against Crime South Africa
RMISA The Institute of Risk Management South Africa
ICASA
CSIR Touching lives through innovation
ACT
GSMA
Digital Council
INTERPOL
CISCO
WASPA Wireless Application Service Providers' Association
communications & digital technologies Department: Communications & Digital Technologies Republic of South Africa
The Banking Association South Africa
PASA
National Prosecuting Authority of South Africa
ISPA Internet Service Providers' Association
South African Reserve Bank
CFCA
GASA Global Anti-Scam Alliance
FSCA
PAYINC
Community Police Forum Partners in Policing

Closing

COMRIC

From report to response

What the report exposes and what COMRiC is building in response

WHAT THIS REPORT EXPOSES

Converging Risk
Eight sector pressures now compound each other — the fuel-levy buffer is gone, cyber threats jump between operators and unrest has become ongoing.

Social engineering at the centre
Subscription fraud and SIM-swap losses run into hundreds of millions — driven by social engineering. Our sector sits at its centre: operators hold the SIM, the number and the OTP every other industry trusts.

Gains that could reverse
Incidents down 40% and losses down 43% — but copper stays chronic at an average of 256 incidents monthly, the Cape provinces are up 114%, and only 22.7% of arrests are convicted.

01
Risk Mitigation
Reduce exposure before loss occurs

- Extend proven prevention into KZN and the rising Cape provinces
- Target copper cable theft with asset tagging and hotspot deployment
- Push the arrest-to-conviction rate past 22.7% with SAPS, the Hawks and the NPA
- Advocate tighter scrap-metal and critical-infrastructure regulation

02
Intelligence Generation & Awareness
See the risk before it lands

- All intelligence streams pooled and reported only in aggregate
- Early-warning signals on displacement and emerging syndicate methods
- COMRiC is building various systems and platforms that will empower its members and the sector to move from reactive to predictive
- Public and community awareness against social engineering.

03
Collective Action & Collaboration
At COMRiC, we act as a Sector.

- Cross-operator intelligence sharing under competitive neutrality
- Joint operations and syndicate-disruption task forces
- A national sector forum with unified incident reporting standards
- Partnerships beyond the founding five — government, business, civil society

Our commitment:

TO OUR MEMBERS
A shared risk picture no single operator could build alone.

TO THE SECTOR
Prevention that holds the gains and closes the remaining gaps

TO SOUTH AFRICA
Connectivity infrastructure defended as national infrastructure.

Call to action

This report is not meant to sit on a shelf. It is a working tool, and it only earns its keep if it changes what happens next inside your business.

Start by getting it in front of the right people. That means your executive committee and your board, but it also means the operational heads who manage energy, security, fraud, cyber and regulatory compliance day to day. The risks in this report do not live in one department, they cut across the whole organisation, so the response needs to as well. A single risk owner reading this alone will not be enough.

Use the report to stress test your own plans, not just to confirm what you already believed. Look at your diesel contingency budget against a world with no fuel levy buffer left. Look at your cyber incident response plan against the reality of sector-wide contamination, where an attack on someone else's systems can become your problem. Look at your fraud controls against a criminal environment that is shifting from volume to value and ask honestly whether your detection thresholds still make sense. If any of these plans were built for last year's risk environment, this is the moment to update them.

Where you find gaps, do not try to close them alone. Part of the reason COMRiC exists is to help operators act together on risks that no single business can manage by itself. If your organisation is exploring diesel hedging, alternative energy pilots, or tighter cyber protocols, tell us. If you are seeing fraud or crime patterns that do not appear in this report, tell us that too. The next edition is only as good as the intelligence that feeds it, and that intelligence comes from you.

COMRiC will keep watching the signals, keep talking to operators in confidence, and keep bringing the sector back a clearer picture as things change. But intelligence only becomes resilience when it is acted on. That part is down to all of us, together.

Where to reach us

info@comric.co.za

www.comric.co.za

FutureSpace, 61 Katherine St,
Sandhurst, Sandton, 2196