COMRiC

Communications Risk Information Centre

Telecommunications Sector Report 2025

Table of Contents

Overview

A Turning Point in Telco Crime Risk Intelligence

The COMRiC Sector Report 2025 marks five years of relentless effort to build South Africa's leading crime and risk intelligence body within the telecommunications industry. This inaugural edition offers a comprehensive overview of emerging threats, systemic vulnerabilities, and strategic responses shaping sector-wide resilience.

Telecommunications crime is no longer a siloed challenge. It touches everything from banking and energy to personal security and national infrastructure. South Africa's telco sector continues to face complex, layered threats, including SIM swap fraud, subscription and identity fraud, ransomware attacks, and infrastructure sabotage. The illicit use of sim boxes, synthetic identity creation, and criminal bypassing of SIM authentication processes present evolving dangers.

Despite this, momentum is building. AI-led prevention, biometric authentication, regulatory pressure, and cross-industry collaboration are showing measurable results. Between March 2024 and April 2025, reported

telecom fraud cases declined thanks to improved monitoring, real-time analytics, and stronger inter-agency response coordination. Mobile network operators processed 3,600 SIM swap requests between January and April 2025, of which only 3 percent were confirmed fraudulent following deeper authentication checks.

Other highlights include:

- Expansion of industry cooperation on fraud and subscription-related crimes.
- Calls for a National Cybersecurity Resilience Plan and sector-wide CSIRT
- Plan and sector-wide CSIRT.
- Advocacy for tighter RICA review and compliance including urgent regulation of OTT platforms like WhatsApp.
- Crackdowns on sim box usage and appeal to ICASA for enforcement action.
- COMRiC continues to serve as a bridge between private innovation and public accountability, enabling knowledge-sharing, strategic partnerships, and industry-wide advocacy.

The Mission

01.

Risk Mitigation

02.

Intelligence Generation and Awareness

03.

Collective Action and Collaboration

Our Governance Structures

Adv. Thokozani Mvelase joined the organisation in 2022 as the CEO of COMRiC. His tenure at COMRiC has been anchored in developing and implementing a structural plan that promotes growth and sustainability for the association. There have been markable developments, but the work is far from over. Adv. Mvelase is intentional about stakeholder engagement and purposefully positioning COMRiC as the telco association dedicated to crime prevention, risk and security matters. 2025 will see the rise of consumer education initiatives and a continued focus on the projects that move us closer to the goal of a crime free telecommunications industry.

While steering the ship rests on his shoulders, he is supported by a dynamic and capable board of directors, a dedicated internal team and all the member organisations of the association.

Our Board of Directors

COMRiC is governed by a Board of Directors, which is responsible for overseeing the implementation of the Strategic Priorities in pursuit of achieving its objectives.

The five years since COMRiC's formation as a vehicle for collective action on crime, risk intelligence, and resilience in the telecommunications industry have brought significant challenges to the fore.

Statement from the Chairman of the Board

Dr. Peter Goss
Chairman of the Board of COMRiC

We've seen escalating threats from digital transformation, particularly disruptive technologies like AI and their associated ethical and social risks. Infrastructure vulnerabilities whether from natural disasters, vandalism, or sabotage continue to expose critical weaknesses. Meanwhile, cybercrime remains a constant and evolving danger.

These risks play out against a backdrop of a fragile global economy and a volatile political landscape marked by civil unrest, growing disillusionment with traditional leadership, and increasing demands for meaningful change.
In South Africa, the call for inclusive economic growth grows louder. Youth unemployment continues to rise. And there is a mounting urgency to tackle deepening social and wealth inequalities.

The telecommunications industry is deeply embedded in this environment. It has responded admirably by establishing a robust technical framework for crime and security risk risk governance, and by building meaningful collective action partnerships.

Now, the focus must shift to higher-order goals influencing policy and engaging policymakers and regulators in ways that serve the broader interests of business, consumers, and civil society alike.

Looking ahead, COMRiC will draw civil society closer into its orbit of collective action. It will expand its partnerships beyond the founding five operators, engage with adjacent industries, and deepen collaboration with the public sector. This includes initiatives like Association of Comms and Technology (ACT), led by telecom CEOs, and partnerships with Business Leadership South Africa, Business Unity South Africa, Business Against Crime, and professional bodies such as the Institute of Risk Management South Africa.

The Board extends its appreciation to the five founding telecommunications operators Cell C, Liquid Intelligent Technologies, MTN, Telkom and Vodacom whose strategic foresight and leadership made COMRiC a reality and continue to shape its progress.

We remain confident and committed to the power of collective action not just as a tool for risk management, but as a vital lever for national resilience and sustainable progress.

The Board comprises of representatives of the founding member organisations and is chaired by an Independent Non-Executive. This brings multiple perspectives to bear in discussion and debate, ensuring robust oversight and strategic decision-making.

Mr. Johan Van Graan
Chief Risk Officer (Vodacom SA)

Ms. Malebu Makgalemela Mogohloane
Group Executive (Telkom SA)

Mr. Anthony Peplar
Group Chief Assurance Officer (Liquid Intelligent Technologies)

Mr. Bradley Swanepoel
Chief Risk Officer (MTN SA)

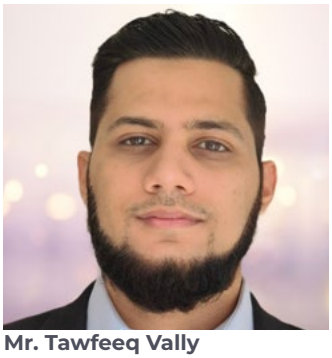
Mr. Lourens Swanepoel
Managing Executive: Forensic Services (Cell C)

Alternate Directors

Mr. Simile Ndlovu
Executive: Forensics & Corporate Insurance (Telkom)

Ms. Wilna Meiring
Managing Executive: Corporate Risk and Security Group Risk (Vodacom Group)

Mr. Andy Lawler
Enterprise Risk Manager South & East Africa Group Business Continuity Manager (Liquid Tech)



Mr. Tawfeeq Vally
General Manager - Risk Management and Internal Controls (MTN SA)

CEO's Message

This year marks five years since COMRiC's founding, and with that milestone comes this 2025 Sector Report, the first of our series' publications, aimed at tracking, interpreting, and influencing the national telecommunications risk landscape.

Our purpose from the outset was clear: to create a trusted, sector-led platform that could anticipate and disrupt criminal networks targeting South Africa's digital infrastructure. Five years on, that vision is not only intact but more essential than ever.

The scale of the threat is stark. In 2024 alone, telecom-linked fraud cost South Africa an estimated R5.3 billion, with nearly 60 percent of mobile banking fraud linked to SIM swap crimes. Infrastructure-related losses, driven by copper cable theft, battery vandalism, and sabotage, exceeded R7 billion across telecoms, energy, and logistics.

And yet, we are making progress. Industry-wide coordination, AI-enabled fraud analytics, and biometric SIM registration are beginning to shift the balance. In the last 12 months, we saw a measurable reduction in reported fraud cases. Network operators processed approximately 3,600 SIM swap requests in the last four months, of which only 3 percent proved fraudulent after authentication, a sign that fraud detection and prevention processes are maturing.

We are also intensifying focus on subscription fraud, where synthetic identities are used to gain unlawful access to telco customers , acquire devices, and exploit gaps in enforcement. This is not just a telecom issue. It is a national economic concern. The time has come to navigate the constraints of POPIA and competition law to allow targeted fraud data-sharing across sectors, including banking and retail.

Our legislative role is growing. Section 8 of RICA empowers the industry to support law enforcement in life-threatening cases. These powers have saved lives, but the RICA framework now requires a modernised approach, particularly to cover unregulated OTT services like WhatsApp, which continue to undercut SIM registration compliance.

We are also urging ICASA to enforce a ban on sim box modems, many of which are smuggled in without regulatory approval. These devices threaten network security, intercept messages, and bypass lawful surveillance systems. Their continued use undermines national efforts to protect digital infrastructure.

Looking ahead, COMRiC will roll out a national Consumer Awareness Programme and formalise a sector-wide Computer Security Incident Response Team to synchronise emergency response protocols. Our call to government is clear: we need a unified National Cybersecurity Resilience Plan. Anything less exposes our economy, society, and digital future to unacceptable risk.

South Africa's digital economy rests on the stability of its communications infrastructure. Without resilience, we risk economic disruption, failures in emergency response, and growing inequality. COMRiC is ready to lead and with stronger collaboration, shared intelligence, and bold regulatory support, we will secure what matters most.

Risk Shift Pattern 2025 vs 2024

The telecommunications sector continues to grapple with a multifaceted threat landscape. Ransomware attacks have spiked globally, but South Africa is responding with enhanced predictive analytics and AI-driven monitoring. SIM swap and synthetic identity fraud are now recognised as gateway threats to a broader web of crime, including mobile banking fraud, impersonation, and digital extortion. COMRiC's role in identifying threat patterns and facilitating coordinated action has helped industry actors detect and neutralise these risks faster than ever before.

Cybersecurity threats have evolved from phishing and malware into more targeted, AI-powered impersonation and manipulation campaigns. Unlike 2024, where incidents were primarily external, Q1 2025 saw a rise in employees falling for scams or misusing access that compromises user credentials.

Infrastructure vandalism and theft have become more sophisticated, with syndicates increasingly coordinating with insiders to carry out theft and damage. As a result, incidents in Q1 2025 showed a broader geographic spread and cross-sector impact.

Misinformation & disinformation threats have intensified in volume and speed. While 2024 saw isolated incidents, 2025 has introduced automated disinformation campaigns that exploit national narratives and create panic to the society.

Compliance risks are rising as new data regulations come into play. In 2024, risks were primarily centred on POPIA implementation. In 2025, concerns are expanding toward cross-border compliance and cloud-based jurisdictional conflicts.

Workforce-related risks are emerging more clearly in 2025. Burnout in cyber teams, skills shortages, and resistance to AI integration have become more prevalent compared to 2024.

Top Sector Risks

1

Cyber Insecurity
Cyberattacks, social engineering, and data breaches remain among the highest risks to national telecom operations.

2

Misinformation and Disinformation
Digital disinformation—especially during periods of unrest or elections—threatens network trust and societal stability.

3

Infrastructure Vandalism and Theft
Telecom infrastructure remains a frequent target of organised crime and civil unrest. COMRiC advocates for stronger legal protection of communication infrastructure.

4

Adverse Technological Advances (e.g. AI Misuse)
The rise of AI-powered attacks and surveillance risks demands proactive governance.

5

Hybrid Threats (Cyber-Physical-Political)
The convergence of cybercrime, civil unrest, and geopolitical instability requires unified contingency planning. COMRiC continues to engage NatJoints and NDMC to ensure the telecommunications is monitored and protected nationally

Pros and Cons of Current Sector Risk Trends

Pros:

- Greater awareness and investment in cybersecurity and business continuity.
- Stronger cross-sector collaboration, especially between telecoms, energy, and national security stakeholders.
- Innovation opportunities in AI-enabled risk detection, predictive maintenance, and fraud prevention.
- Movement toward harmonized compliance practices driven by regulatory developments.

Cons:

- High dependence on telecoms infrastructure makes the sector a top target for multi-layered attacks.
- Rapid tech evolution outpaces governance and legal frameworks.
- Fragmented vendor environments increase supply chain vulnerabilities.
- Skills gaps and staff burnout in cyber and operational risk functions.

COMRiC continues to help the sector navigate these trade-offs by providing tools, convening thought leaders, and driving forward-looking solutions.

Emerging Risks Monitored and Sector Impact Outlook

Emerging Risk	Short-term Impact	Medium-term Impact	Long-term Impact	COMRiC View
Deepfakes & Synthetic Fraud	Targeted scams against executives and customers; voice spoofing threats	Sector reputation damage and increased fraud risks	Normalization of digital impersonation unless countered	This risk threatens public trust and operational control. We recommend telecom-specific counter-disinformation protocols.
AI-Driven Labour Displacement	Initial workforce anxiety and resistance to automation	Need for strategic re-skilling and union engagement	Telecom operational restructuring and talent shortages	COMRiC supports responsible AI adoption and sector-wide skills planning.
Climate-Related Infrastructure Disruption	Isolated outages due to floods, storms, or heat waves	Insurance and redundancy cost increases; planning burden	Rising operational instability in high-risk regions	COMRiC supports climate risk integration into BCP and resilience maps.

Initiatives on Strategic Objectives

COMRiC's strategic pillars are focused on infrastructure crime, cybersecurity coordination, and regulatory transformation. A multi-agency approach is beginning to shift the dial with improved SIM swap authentication, better subscription fraud monitoring, and national forums that bring law enforcement, mobile operators, and civil society into the same room. Industry-led emergency drills and the planned CSIRT launch signal a maturing risk culture, but legislation must evolve to allow broader, lawful intelligence-sharing.

Network Infrastructure Theft and Vandalism

1

- COMRiC promotes community-based initiatives to encourage citizens to report suspicious activities around various telecom sites.
- Collaborate with SAPS, NPA and private security firms to dismantle syndicates and track stolen goods.
- Sitting in Joint initiatives on Crime & Corruption (JICC) – Participation in the NATJOINT Priority Committee

Cybersecurity Threats and Data Breaches

2

- COMRiC to establish CSIRT
- Work with cybersecurity agencies such as Cybersecurity Hub, CSIR and Information Regulator to strengthen industry-wide defences.

Telecommunications Sector Resilience

3

- Develop Business Continuity Framework and coordinate industry-wide emergency response.
- Participate & work with the National Disaster Management Center.

White collar crime prevention initiatives

4

- To include a coordinated effort to report and block numbers linked to scams and ensure that RICA information is updated.

Telkom

The telecommunication industry is one of the key industries that is critical for driving economic growth. The availability of telecommunication network is as important as the availability of electricity to drive economic and social activities. Collectively, network operators have vast critical infrastructure across the length and breadth of the country. The State President, Cyril Ramaphosa, previously mentioned that theft and damage to critical infrastructure constrains economic growth, investment, and job creation. Telkom alone has thousands of various types of critical infrastructure. This infrastructure came at a back of substantive capital investment by Telkom and other network operators.

Telkom and its peers have been on the receiving end of various types of crime and security incidents. These manifests as battery theft, theft, sabotage, or vandalism of infrastructure, and various types of subscription fraud. These crimes hamper the provision of essential network services to businesses and communities, and cause huge revenue loss, increase cost of doing business, and reputational damage for network operators. The crime directly impacts the efficient functioning of the economy, ineffective digital communication and negative customer experience to many consumers of network operators. The growth, sustainability and resilience of the industry is dependent on the network being constantly available. The infrastructure is central to the industry in offering quality network to customers.

Helen Keller once mentioned that “alone we can do little, together we can do so much”. It is for that reason that COMRIC was formed, after all as players in the telecommunication industry realised that individually we cannot win the coordinated and well organised onslaught by criminals’ syndicates. In its short existence, COMRIC has been instrumental in marshalling its members to deal with store robberies, sim-farming, and recently Telkom has engaged COMRIC to find ways of mitigating the perennial risk of sim-box fraud.

As Telkom, we are proud of being a member of COMRIC. Telkom is deriving immense value out of the COMRIC membership, especially the sharing of crime and risk information among members, Law Enforcement Agencies and Regulators. The insights that we receive by virtue of being a COMRIC member, is used to improve the internal controls and the fraud and security risk management practices of Telkom.

Telkom is committed to ensure that COMRIC becomes a success. We work together with fellow members of COMRIC in sharing insights, and proactively tackling crime and security incidents that might derail the success of each member, and the broader industry. Through COMRIC, we want to work with other role players inside and outside the telecommunication industry, to find solutions to complex problems of crime that affects economic activity and flawless digital connection of South Africa.

2025 Developments for Telecommunications Sector

South Africa is currently undergoing a transformation, with several emerging activities happening that will disrupt the market in a positive direction.

Generative AI in Telecom – The adoption of GenAI is expected to unlock $6 billion to $9.6 billion annually in economic value for the telecom sector. AI-driven automation is improving network issue resolution, customer service, and aiding telcos with smart resolutions around infrastructure challenges.

Satellite Connectivity – The government is exploring regulations to allow Starlink and other satellite providers to operate without traditional BBBEE requirements. This could expand rural internet access and reshape competition in South Africa as we know. The government is looking at ways to provide companies looking to invest in South Africa with alternatives where they can either sell or surrender a 30% portion to previously disadvantaged persons in compliance of BBBEE.

Fiber Infrastructure Expansion – Despite advancements in satellite and mobile networks, fiber remains the backbone of South Africa's digital transformation. Investments in fiber-optic networks are crucial for supporting 5G and high-speed broadband.

Regulatory Shifts & Market Competition – New policies are being introduced to streamline licensing and improve regulatory certainty for telecom operators. These changes aim to attract investment and enhance service delivery.

Government-Led Digital Reforms – With the assistance of key players in the telco and ICT ecosystem, the state is launching a digital transformation roadmap to improve public service delivery and reduce data costs. This initiative seeks to integrate telecom advancements into broader economic reforms

Mitigation Strategies for Infrastructure Security

Enhanced Physical Security Measures	Collaboration with Law enforcement and Partners of COMRiC	Community Engagement
Infrastructure Security: Armed security, drone surveillance, and AI powered surveillance for monitoring of towers Tower Hardening: Reinforcing Infrastructure with tamper proof materials (e.g. concrete bunkers for batteries, anti –theft cable design)	Continued partnerships with SAPS, Hawks, Interpol and other law enforcement agencies to dismantle criminal syndicates. Collaboration with telco alliances, financial services sector and government to safeguard telco infrastructure	Awareness campaigns, partnerships with Community Police Forums and civil society groups.
Energy Resilience	**Legal and Regulatory Reforms**	**Technology Solutions**
Transitioning to solar/hybrid power solutions for towers to reduce reliance on theft prone batteries	Harsher penalties for infrastructure vandalism (e.g. Criminal Matters Amendment Act) Expediting permits for infrastructure deployment in high risk locations	Smart Sensors: IoT enabled devices to detect tampering. Blockchain: Tracking legitimate equipment sales to deter black market trade

Collaboration and Regulatory Engagement

Telecommunications resilience is no longer the telecom sector's job alone. Financial institutions, retailers, law enforcement, and regulators all have a stake to secure digital infrastructure. COMRiC continues to foster public-private collaboration models that cut across silos. We advocate for enabling legal frameworks to share actionable fraud intelligence while respecting privacy law, and we support harmonised regulation that addresses the rising use of OTT services and improperly RICA'd SIM cards.

Cross-sector collaboration is not only essential for mitigating current and emerging risks, but also for reinforcing the strategic role of the telecommunications sector within the national economic ecosystem. Telecommunications is an enabler of nearly all other sectors —Banking, Health, Logistics, Security, Education, and Government Services.

When telecom networks are disrupted due to vandalism, cyberattacks, or power outages, the entire value chain of the economy experiences delays, losses, and reputational harm. Therefore, a coordinated response involving telecom operators, regulators, energy providers, financial institutions, law enforcement, and technology partners ensures:

- Faster threat detection and response.
- Resilient infrastructure planning and mutual aid mechanisms.
- Regulatory clarity and innovation alignment.
- Reduced systemic risk exposure across interconnected sectors.

Potential Consequences

Should these risks materialize without collaboration, South Africa could face increased economic volatility, digital divide expansion, and impaired national security.
Conversely, if risks are successfully mitigated through collective action, the telecom sector can accelerate national goals such as digital transformation, inclusive growth, and regional competitiveness.

COMRiC champions these cross-sector partnerships by acting as a neutral convener, a knowledge-sharing platform, and an advocacy voice that aligns private-sector agility with public-sector accountability.

Defining Telco Infrastructure

Physical telecom infrastructure in South Africa refers to the foundational assets that enable communication networks to function. This includes:

- Fiber-optic networks – High-speed data transmission lines connecting urban and rural areas.
- Cell towers & base stations – Essential for mobile network coverage, supporting 4G and 5G connectivity.
- Copper cables - Remains a backbone for telecom systems, particularly in areas where fibre deployment is limited
- Submarine cables – International fibre-optic cables linking South Africa to global networks.
- Satellite infrastructure – Used for remote and rural connectivity where terrestrial networks are limited.
- Power & backup systems – Including generators and battery solutions to mitigate load shedding impacts.
- Data centres – with the prevalence of cloud-based telecom services, data centres have become a more strategic asset for operators.

The Importance of the Telecommunications Infrastructure

Telecommunications infrastructure is a key asset for South Africa, driving economic growth, digital inclusion, and national security.

Economic Growth & Digital Transformation	Connectivity & Social Development	Security & National Resilience	Bridging the Digital Divide
The digital economy contributes between 2% and 19% of South Africa's GDP	78.6% of South Africans have some form of internet access, primarily through mobile networks	COMRiC collaborates with stakeholders to protect the sectors infrastructure.	Investments in broadband, mobile networks, and satellite communications are essential for rural connectivity.
A 10% increase in broadband penetration correlates with a 1.38% GDP growth in developing countries.	20.3% of schools have an internet connection suitable for digital learning.	Telecommunications infrastructure is vital for disaster response, emergency services, and national security.	Reliable internet underpins innovation hubs and start-ups. Our telco's drive over 90% mobile penetration through fixed line adoption lags.
The government aims for universal access to affordable, high-speed internet, with a focus on connecting homes and schools.	The telecommunications infrastructure will be critical in supporting e-voting systems, ensuring secure and transparent elections.	The resilience of the network during increased power shortages demonstrated the investment by the sector and the importance of protecting the infrastructure from day zero.	Submarine cables: SA serves as Africa's gateway via cables (SAT -3, WACS, SEACOM), linking the contingent global markets and reducing latency.

Key Threats to Sector Infrastructure – South Africa

South Africa's communications infrastructure faces persistent physical threats. The Q4 police statistics suggest a seasonal dip in incidents, but experts warn this may reflect displacement rather than resolution. Copper theft remains strongly correlated with global commodity prices, while lithium battery theft surged during load shedding. Criminal syndicates are growing more organised. COMRiC's analysis calls for integrated tower security strategies, community-based reporting, and the inclusion of tower operators in sectoral security planning.

Theft and Vandalism

- Copper Cable Theft: Driven by high scrap metal prices. Criminals target copper cables, fibre-optic lines and backup batteries – leading to network outages and costly repairs.
- Impact: Telco's lose millions a year replacing stolen and damaged infrastructure
- Hotspots: Informal settlements, remote areas, unguarded infrastructure

Infrastructure and Sabotage

- Acts of sabotage during civil unrest such as tower burnings, cable cutting – which leads to service disruptions.
- e.g. 2021 riots where over 100 cell towers were damaged impacting KZN & GP.
- Criminals will often sabotage infrastructure by cutting cables they thought were copper and leaving wires damaged and exposed

Energy Instability

- Load shedding: Eskom's power cuts push telcos to rely on back up batteries and generators, which are also targets of theft
- Battery Theft: an average of 215 batteries are stolen monthly from cell towers, thus compromising network resilience during outages.

Illegal Connections

- Unauthorised fibre jacking and illegal cable connection lead to network congestion, service degradation and safety hazards.

Organised Crime Syndicates

- Sophisticated criminal networks export stolen telecom equipment (e.g. copper, batteries) to neighbouring countries.
- Scrap metal dealers buy stolen materials which encourages theft.

Environmental Risks

- Floods, fires and extreme weather damage exposed infrastructure, particularly in rural and informal areas.

Key Threats to Sector Infrastructure – Globally

Cybersecurity Risks: Telecom networks are prime targets for cyberattacks, including ransomware, Distributed Denial of Service (DDoS) attacks, and insider threats.

Supply Chain Vulnerabilities: The reliance on third parties for hardware, software and cloud services can expose the sector to breaches, service disruptions and ultimately weak security.

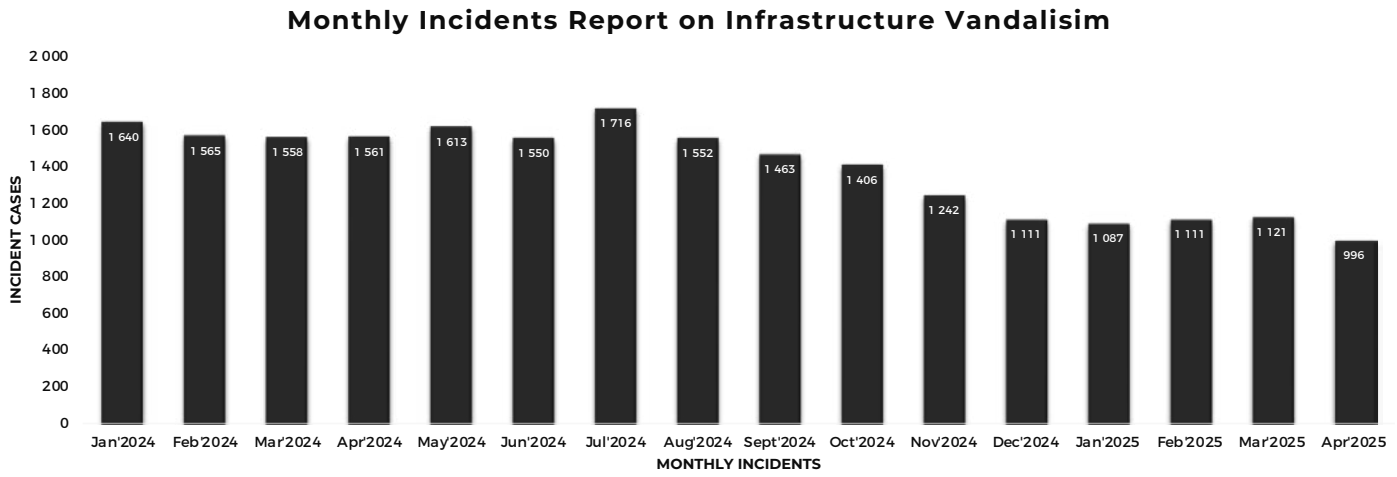
Geo Political Tensions: International conflict and trade restrictions impact telco infrastructure, notably submarine cable networks. Governments all over the world have started introducing legislation to protect their critical infrastructure from foreign attack.

Physical Infrastructure Sabotage: Attack on undersea cables, power grids and telecom hubs can disrupt global connectivity. Defence mechanisms around such assets have increased.

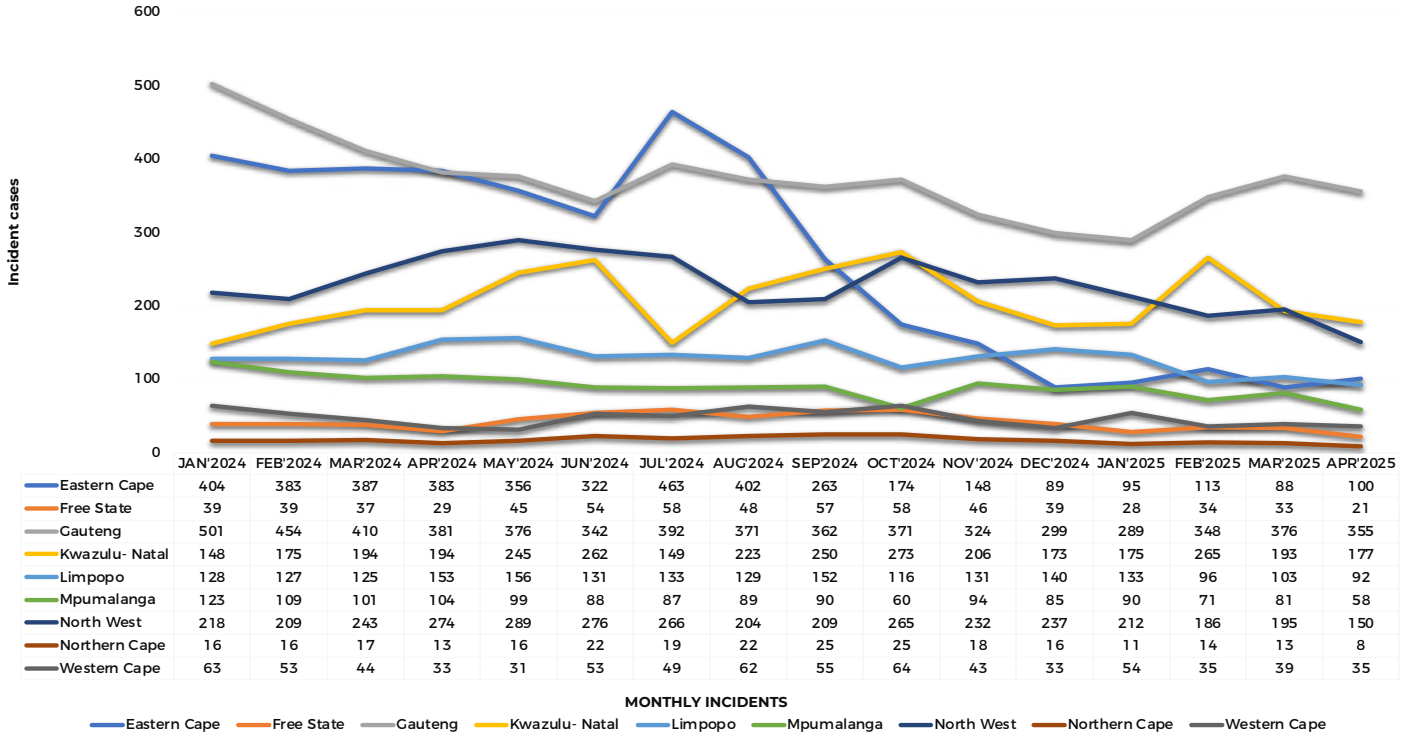
Cloud & IoT Security Challenges: The rise of cloud-based telecom services and IoT devices introduces new attack surfaces. Weak security protocols can lead to data breaches and service outages.

Global copper price: With the market experiencing a shortage in copper, there has been an observed increase in the price for copper. Making illicit copper trade a lucrative market for criminals.

Reported Infrastructure Theft and Damage at Base Stations

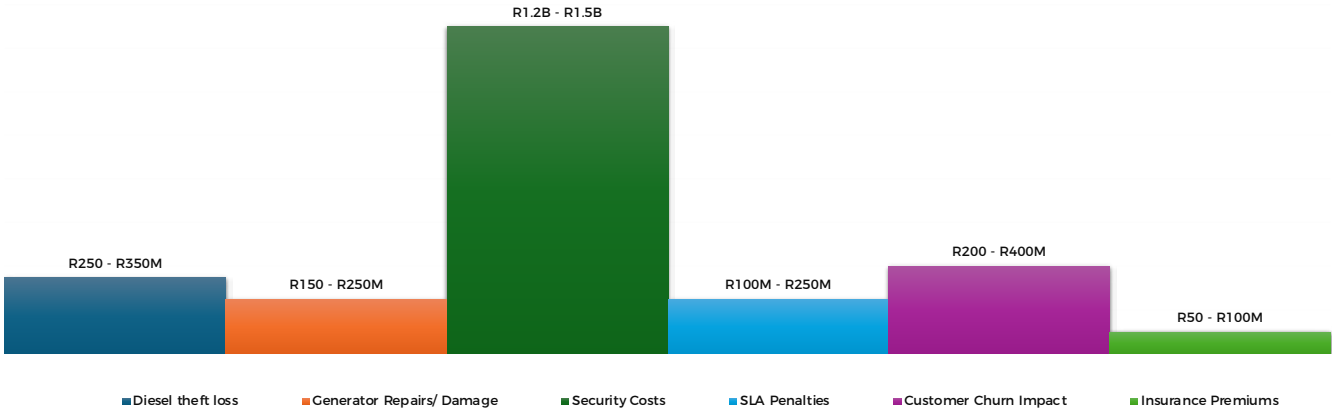


Monthly Provincial Trends



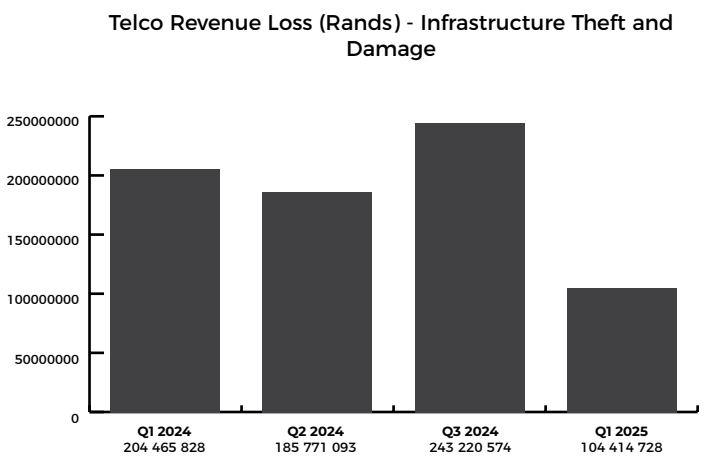
	JAN'2024	FEB'2024	MAR'2024	APR'2024	MAY'2024	JUN'2024	JUL'2024	AUG'2024	SEP'2024	OCT'2024	NOV'2024	DEC'2024	JAN'2025	FEB'2025	MAR'2025	APR'2025
Eastern Cape	404	383	387	383	356	322	463	402	263	174	148	89	95	113	88	100
Free State	39	39	37	29	45	54	58	48	57	58	46	39	28	34	33	21
Gauteng	501	454	410	381	376	342	392	371	362	371	324	299	289	348	376	355
Kwazulu- Natal	148	175	194	194	245	262	149	223	250	273	206	173	175	265	193	177
Limpopo	128	127	125	153	156	131	133	129	152	116	131	140	133	96	103	92
Mpumalanga	123	109	101	104	99	88	87	89	90	60	94	85	90	71	81	58
North West	218	209	243	274	289	276	266	204	209	265	232	237	212	186	195	150
Northern Cape	16	16	17	13	16	22	19	22	25	25	18	16	11	14	13	8
Western Cape	63	53	44	33	31	53	49	62	55	64	43	33	54	35	39	35

Diesel Theft Impact - Mar 2024 - Mar 2025



Category of cost	Estimated Financial impact
Diesel Theft Loss	R250 – R350 million
Generator Repairs / Damage	R150 – R250 million
Security Costs	R1.2 billion – R1.5 billion
SLA Penalties	R100 million – R250 million
Customer Churn Impact	R200 – R 400 million
Insurance Premiums	R50 – R100 million

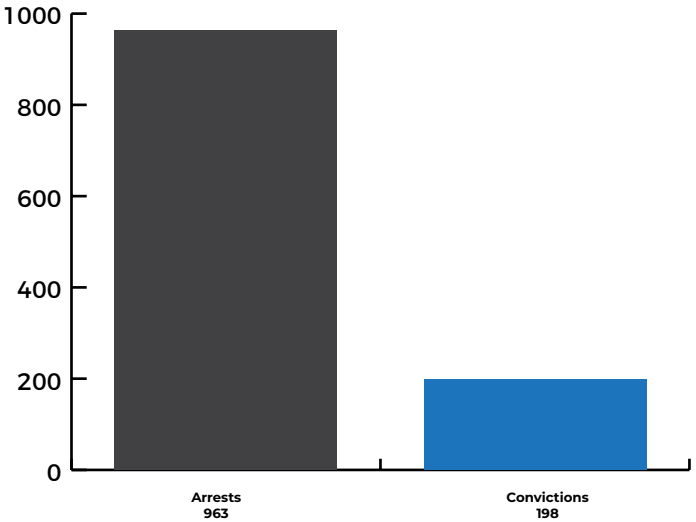
Financial Impact Overview



Revenue losses per quarter can be attributed to the following factors:

- Theft: copper cables, fibre cables, batteries, diesel, poles, pillar joints etc.
- The cost of replacing and repairing damaged/ stolen assets at base stations
- Sabotage incidents

Arrests vs Convictions: '24



In 2024 there were 963 arrests and 198 cases were finalised. The convictions are not directly linked to the arrests for that year. While arrests are frequent, securing convictions remains a complex process. The sector has made a firm effort to work closely with law enforcement agencies both nationally and internationally.

The arrests made were predominantly for copper cable theft and vandalism.

Monitoring Copper Cable Theft

The black market circulation of copper in South Africa:

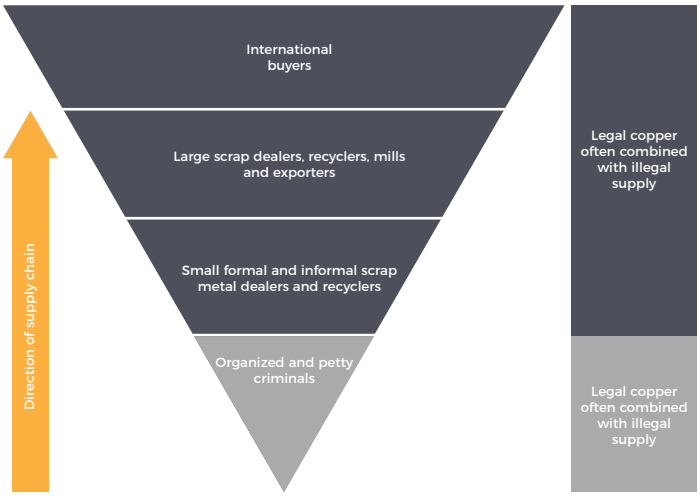
Copper stolen by thieves

Sold to informal and formal scrap metal dealers and recyclers, where it is processed

Local copper market, both formal and informal

Exported to other countries

International buyers market:



International Buyers Market - reference: https://globalinitiative.net

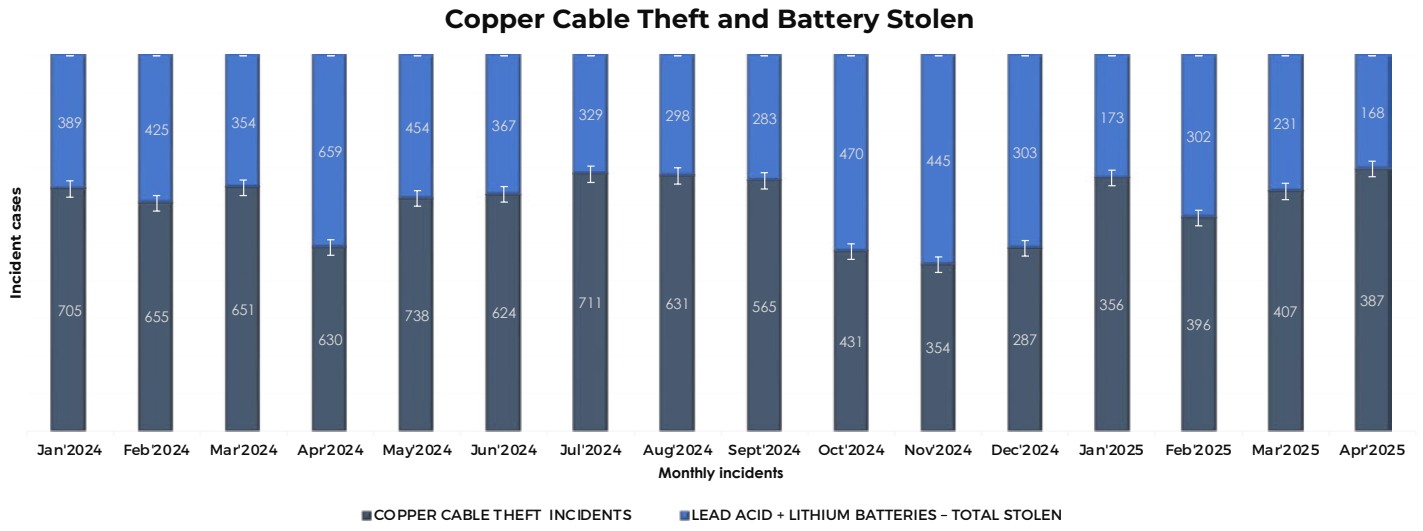
Copper Cables | Lithium Battery Theft

- **Scale & Frequency:** Copper theft has historically been a major issue, costing South Africa R5–7 billion annually. Criminal syndicates target telecom, rail, and power infrastructure.
- **Impact:** Disrupts telecom networks, electricity grids, and transport systems. Stolen copper is often smuggled and resold in illicit markets.
- **Mitigation:** Increased security measures, stricter sentencing, and alternative materials (like aluminium) are being explored.

Recent stats indicate that the **Telco sector saw a 30 - 40% decline in copper and battery theft** incidents due to improved security measures. However, site vandalism remains a challenge, suggesting criminals are shifting tactics.

- **Scale & Frequency:** During power outages we noticed an increase in battery theft, however socio-economic issues contribute to the level of crime.
- **Impact:** Causes mobile network outages, affecting emergency services, business operations and may cause network congestions. This also impacts the quality of connectivity.
- **Mitigation:** Operators are investing in tamper-proof enclosures, GPS tracking, and AI-driven monitoring to prevent theft.

Both forms of theft require ongoing intervention, with telecom operators focusing on **enhanced surveillance, community engagement, and alternative technologies** to safeguard infrastructure.



Further together
vodacom

Vodacom joining forces to protect the people and the sector we all serve

At Vodacom, we're deeply committed to creating a safe and secure digital environment, one where fraud and crime have no place. We understand that cybercrime and criminal syndicates don't just threaten our operations, they undermine the trust that people place in mobile technology every day.

That's why we're proud to be a founding member of the Communications Risk Information Centre (Comric). This non-profit initiative, formed in collaboration with South Africa's mobile operators, is dedicated to proactively tackling fraud, financial crime, and other risks that affect our industry.

Our mission at Vodacom has always gone beyond just providing connectivity. We believe in building a digitally inclusive society, one where everyone can connect, communicate, and transact with confidence. Through our involvement in Comric, we are sharing insights, contributing to intelligence networks, and helping shape industry-wide frameworks that strengthen risk management.

Fraud doesn't just impact individuals, it chips away at the very foundations of digital inclusion and economic progress. By working together through Comric, we're helping to raise the bar across the sector, encouraging best practices, and building stronger defences against criminal activity.

This first sector report marks a significant milestone. It shows what is possible when competitors come together for a common cause: protecting the people and the industry we all serve.

We are grateful to our peers across the mobile sector for their collaboration and shared commitment to a safer, more resilient communications landscape. Because when we work together, we go further, ensuring no one is left behind. Further Together.

Top Common Cyber Threats

Ransomware Attacks:
Highly prevalent, with sophisticated tactics like double extortion becoming common.

Phishing Scams:
A major concern, costing South Africans R200 million in 2023 — a 50% increase from the previous year.

Business Email Compromise (BEC):
Rapidly growing, constituting 24-25% of financially motivated cyber incidents.

Malware and Exploits:
Significant increases in exploit attacks (55%) and backdoor vulnerabilities (42%) have been observed.

Synthetic Identity Fraud:
A 153% rise in synthetic identity fraud has been reported, posing challenges for financial institutions.

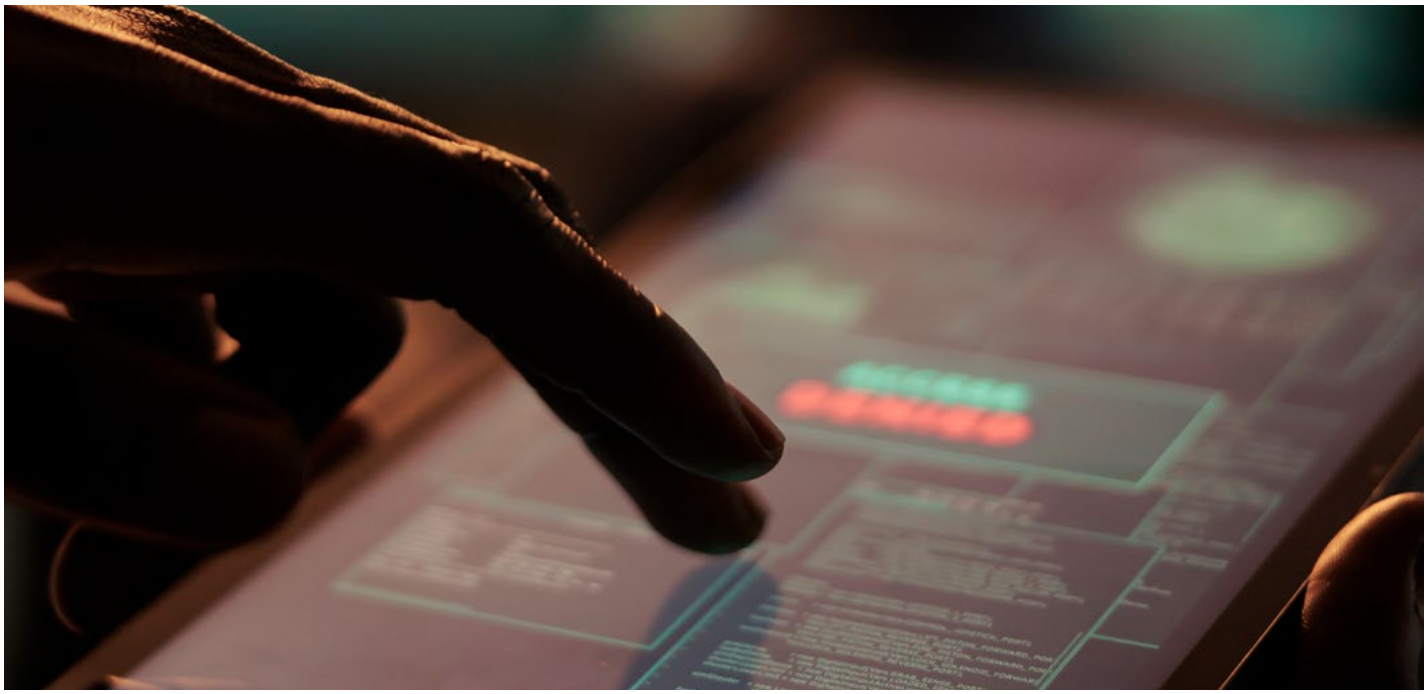
Cyber Attacks in Africa 2024

South Africa: Faces 3,312 cyberattacks each week targeting government systems. Ransomware attacks are increasing quickly, and cybercrime is now costing the country close to 1% of its GDP.

Kenya: 4,719 weekly cyberattacks on government infrastructure. Cybersecurity sector is growing 20-25% annually. Growth is driven by investments in AI technologies and digital infrastructure.

Nigeria: Faces 4,718 attacks each week. Recent banking Trojan attack affected 100,000 accounts, resulting in $3 million in losses. Highlights growing vulnerability in the financial sector.

Morocco: Is one of the most targeted nation in Africa. With 8,733 attacks per week on government organizations. The government recently faced a state-sponsored cyberattack that compromised classified communications, raising significant national security concerns.



Global Cyber Attacks in Q1 2025

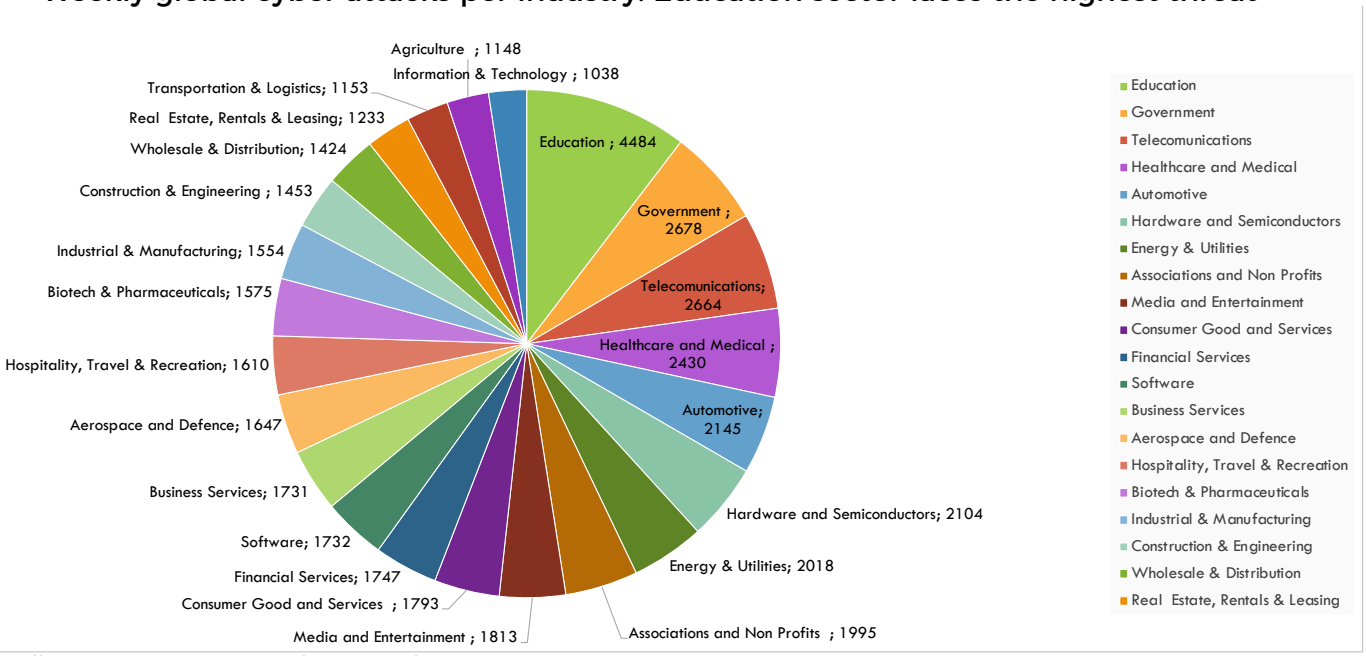
Cyber Attack Increases: Several organisations faced 1,925 cyberattacks per week, a 47% increase from the previous year.

Most Targeted Sectors: Education saw the highest number of attacks, with 4,484 weekly, followed by government 2678 and telecommunications with 2664 attacks.

Regional Attack Growth: Africa experienced the highest number of attacks, averaging 3,286 per week. Latin America saw the fastest growth, with a 108% year-over-year increase.

Ransomware Attack Increases: Ransomware attacks increased by 126%, with North America accounting for 62% of global incidents, and Consumer Goods & Services being the most targeted sector.

Weekly global cyber attacks per industry: Education sector faces the highest threat



https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/

Threat outlook and emerging risks 2025

Global, African and South African organisations appear to have prioritised the mitigation of cyber risks over the next 12 months.
The table below shows a comparison of cyber risk across Global, Africa, and South Africa.

	Global (4,052)	Africa (218)	South Africa (94)
Cyber risks	57%	61%	66%
Digital and technology risks Inflation	53%	55%	53%
Digital and technology risks Inflation	48%	41%	47%
Environmental risks	30%	35%	33%
Macroeconomic volatility	30%	28%	18%
Geopolitical risks	25%	14%	16%
Societal risks	21%	15%	16%
Health risks	17%	21%	22%

PWC: Global Digital Trust Insight Survey: South Africa and Africa Report

Comparing South Africa to the rest of the world

Comparing South Africa and the rest of the world, our priorities are not too far apart for the next 12 months.

Cyber threats that organisations are most concerned about over the next 12 months:

	Global (4,052)	Africa (218)	South Africa (94)
Cloud-related threats	42%	36%	47%
Hack-and-leak operations	38%	38%	40%
Third-party breach (i.e., data breaches)	35%	37%	28%
Attacks on connected products	33%	36%	46%
Ransomware	27%	18%	16%
Business email compromise / account takeovers	24%	29%	26%
Social engineering (i.e., deep fakes, disinformation)	24%	29%	26%
Software supply-chain compromise	22%	22%	28%
Distributed denial-of-service attacks (DOS)	17%	15%	13%
Exploits of zero-day vulnerabilities	13%	11%	6%
Quantum computing	9%	4%	6%

PWC: Global Digital Trust Insight Survey: South Africa and Africa Report

Liquid Intelligent Technologies
Powering Africa's Digital Future

Liquid Intelligent Technologies is a business of Cassava Technologies (Cassava), a technology company of African heritage with operations in 40-plus markets across Africa, the Middle East, and Latin America, where the Cassava group companies operate. Liquid has firmly established itself as the leading provider of pan-African digital infrastructure with a 110,000 km-long fibre broadband network and satellite connectivity that provides high-speed access to the Internet anywhere in Africa. Liquid is also leveraging its digital network to provide Cloud and Cyber Security solutions through strategic partnerships with leading global players. Liquid is a comprehensive technology solutions group that provides customised digital solutions to public and private sector enterprises and SMEs across the continent.

Through this combined offering, Liquid Intelligent Technologies is enhancing customers' experience on their digital journey, with the vision of a digitally connected future that leaves no African behind. Liquid Intelligent Technologies is one of five founding companies that collaborated to form COMRIC in 2020, along with the Mobile Network Operators Vodacom, MTN, Cell C and Telkom. Liquid Intelligent Technologies shares in the vision of COMRIC which is to provide a platform to share relevant and vital crime and risk information that is reliable and value-adding to the telecommunications industry and other stakeholders such as Law Enforcement Agencies and Regulators, by financially supporting the efforts of COMRIC, attending and addressing vital meetings and providing accurate crime detail; and, in doing so, providing value and sustainability to the South African telecommunication community.

For more information, visit https://www.liquid.tech/.

za.liquid.tech

LIQUID
INTELLIGENT TECHNOLOGIES

CSIR Survey 2023/24

The CSIR Information and Cybersecurity Centre, together with the Cybersecurity Hub from The Department of Communication and Digital Technologies, has released national cybersecurity survey for the year 2023/24.

The survey looked at important issues like:

- How well government and public organisations are prepared for cyber threats
- The shortage of skilled cybersecurity workers
- The number and types of cyberattacks happening
- The current state of digital identity in South Africa

The findings help show where South Africa stands in cybersecurity and what needs to improve.

Key Findings from the 2023/24 CSIR Survey

Prevalence of cyberattacks: 47% of organisations reported experiencing between 1 to 5 cybersecurity incidents in the past year, indicating widespread exposure.

Malware and phishing: Remains the most prevalent threats, exploiting both technical and human vulnerabilities.

Data breaches: 88% have experienced at least one data breach, with 90% of those facing repeated targeting.

Cybersecurity awareness: Only 32% of organisations report having trained more than half their staff in cybersecurity awareness, exposing a major gap in organisational preparedness and culture.

Skills gaps: Many cybersecurity jobs are not being filled. 63% of roles remain open because there aren't enough trained people. This puts organisations at greater risk of cyberattacks since they lack the staff needed to defend their systems.

Talent retention: Is a critical issue, 35% of cybersecurity professionals leave for better opportunities or due to inadequate training and support.

Cybersecurity monitoring: Only 41% of organisations check for cyber threats daily. This means most are not well-prepared to stop attacks. In South Africa, there are over 20 million cyber threats each month, showing how serious the risk is.

Digital identity: Financial institutions are leading with (88%), while technologies like biometrics (68%) and encryption/privacy technology (71%) are seen as key enablers. Identity theft remains a top concern that digital identity solutions aim to counter.

Cybersecurity Trends in Africa/ South Africa 2025

Telcos are proactively addressing the evolving cybersecurity landscape in 2025 by implementing advanced technologies and strategies. Below are key cybersecurity trends and how the sector is responding to each trend.

1. Rise of ransomware and digital extortion: Ransomware remains a significant threat in Africa, with 69% of South African businesses affected in 2024.

2. AI-driven cybersecurity: MNOs utilise AI and machine learning to detect anomalies and respond to threats in real-time, enhancing their security posture.

3. Zero Trust security models: trust no one, verify everything - Telcos implement continuous verification processes for users and devices accessing the network.

4. Quantum-resistant cryptography: MNOs are piloting NIST-recommended post-quantum cryptographic algorithms to secure communication and data.

5. Business Email Compromise (BEC) and phishing scams: MNOs have joined the GSMA Open Gateway initiative, implementing Number Verification and SIM Swap APIs to combat fraud and digital identity theft.

6. Third-party risk management: Telcos conduct frequent evaluations of third-party security practices to identify and address vulnerabilities.

7. Human-centric Security: Telcos are enhancing human-centric security by Conducting regular cybersecurity awareness and training programs.

Cybercrime Threats Impact MNOs

MNOs have increasingly become high-value targets for cybercriminals due to the sensitive data and critical infrastructure they manage. In recent months, several major MNOs operating across South Africa and broader African markets have reported significant cybersecurity incidents. The below demonstrates some of the initiatives by the MNO's to combat cybercrime:

- In alignment with national regulatory requirements, including those set by (Information Regulator and ICASA), MNOs have implemented robust incident reporting mechanisms to ensure compliance and transparency.
- MNOs are enhancing infrastructure security by deploying advanced firewalls, intrusion detection systems, AI-powered traffic monitoring, and conducting regular vulnerability assessments. These efforts are aimed at reducing the risk of network breaches and service disruptions.
- MNOs are actively involved in cross-sector collaboration with financial institutions, government agencies, and cybersecurity task forces to share threat intelligence and coordinate responses.
- Collaboration with Law enforcement through technical training, secure information exchange platforms, and joint operations that facilitate the investigation and prosecution of cybercrimes.

South Africa Cybercrime Statistics 2024/25

R 2.2 Billion

Cybercrime costs South African economy approximately R2.2 billion per year.

The average cost of a data breach in South Africa has surged to R53.1 million in 2024.

Approximately 78% of South African companies experienced ransomware attacks in 2023.

In South Africa, the average cost of a data breach for companies has reached nearly R50 million in 2024.

The cyber security market in South Africa is expected to reach a projected revenue of $ 4,1 billion by 2030.

Cybercrime Statistics Globally 2024/2025

$10.5 Trillion

Projected cost of cybercrime by 2025

$30 Billion

Cost of Crypto – Annually by 2025

$1.5 Trillion amount earned by cybercrime activity yearly.

80% of cybercrime are phishing attacks in the technology sector.

2.7 Billion hours total time spend resolving cybercrimes; average of 6 to 7 hours daily

$5.9 Million is the highest cost of data breach in the U.S.A in 2023.

Market Size: 13%
A Compound Annual Growth Rate is expected to grow from 2025-2030 worldwide in cyber security.

$265 Billion

Estimated annual cost of ransomware to victims by 2031

South Africa's cybersecurity collaborations

Financial Sector Collaboration

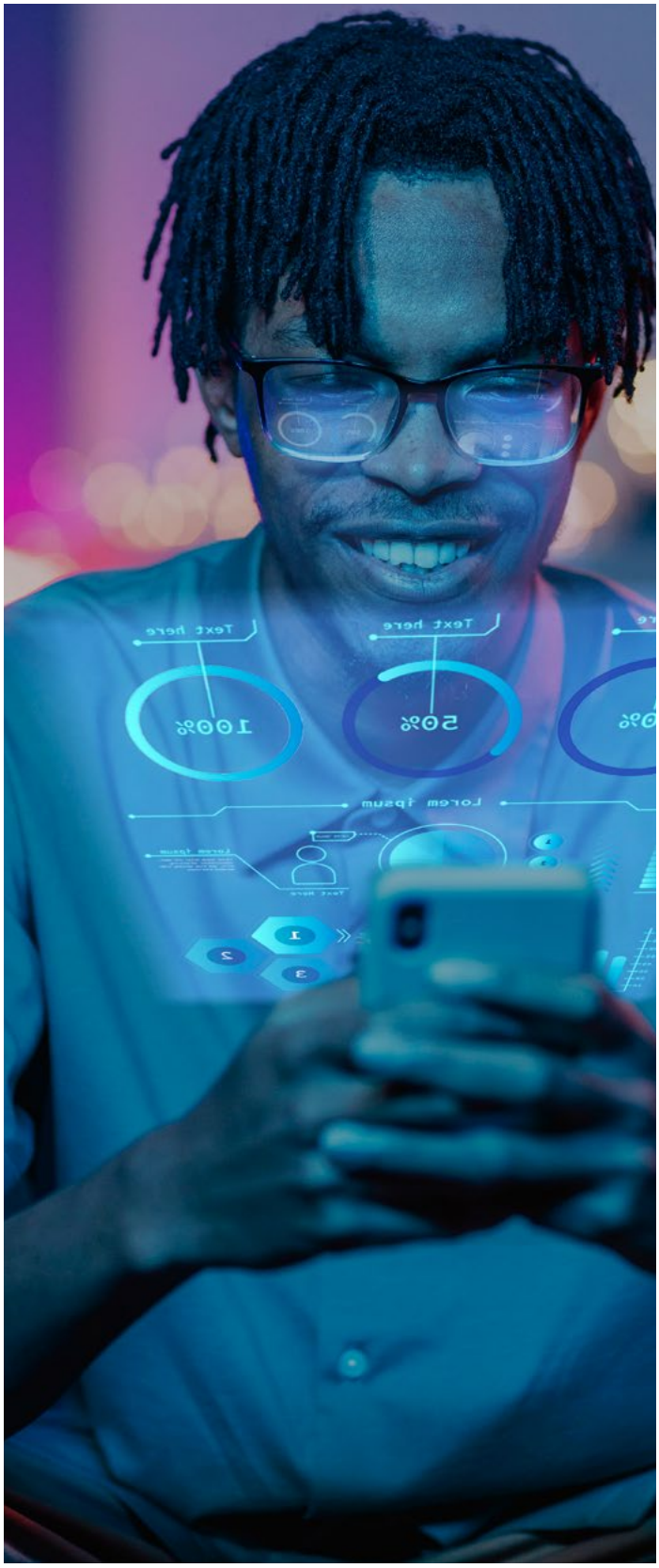
- Banks and other financial institutions are following a new set of shared rules called the Joint Standard on Cybersecurity and Cyber Resilience. These rules require banks and financial institutions to put strong cybersecurity systems and management practices in place to help protect against cyber-attacks.
- Regulatory Coordination: Regulatory bodies are collaborating to promote cyber resilience across the financial sector, ensuring a unified approach to cybersecurity challenges.

Telecoms and Internet Sector Collaboration

- COMRiC acts as a central hub for cybersecurity collaboration. Through COMRiC, operators share threat intelligence, coordinate responses to cyber incidents, and develop best practices to strengthen sector-wide cyber resilience.
- Industry associations have been instrumental in shaping telecommunications policy, providing submissions and feedback on key legislation related to cybersecurity.

Private Sector Partnerships & Innovation

- Cybersecurity Hackathons: Collaborative hackathons have been organized to address specific cybersecurity challenges, such as unauthorized SIM-swaps linked to digital identity theft. These events bring together diverse teams to develop innovative solutions.
- Educational Initiatives: Academic institutions, supported by international organizations, have launched programs to expand cybersecurity training, equipping students with skills to protect digital infrastructure.
- Government Initiative: The Cybersecurity Hub has partnered with private sector organizations and universities to host themed hackathons, fostering innovation and addressing cybersecurity issues through collaborative efforts.



The Urgent Need for a National Cybersecurity Resilience Plan in South Africa

COMRiC calls for a National Cybersecurity Resilience Plan (NCRP) to unify government, business, law enforcement, and cybersecurity experts.

Urges urgent and coordinated action to strengthen South Africa's cybersecurity infrastructure.

Welcomes government focus on cybercrime, AI-driven fraud detection, and digital infrastructure investment but stresses need for faster implementation and integration.

Warns that South Africa's financial, business, and government sectors are vulnerable to cyberattacks, data breaches, and fraud.

Supports establishment of a digital forensics lab but calls for adequate resourcing and alignment with international best practices.

Emphasises importance of rigorous cybersecurity protocols for the digital identity rollout to protect citizens' personal data and prevent a single point of failure.

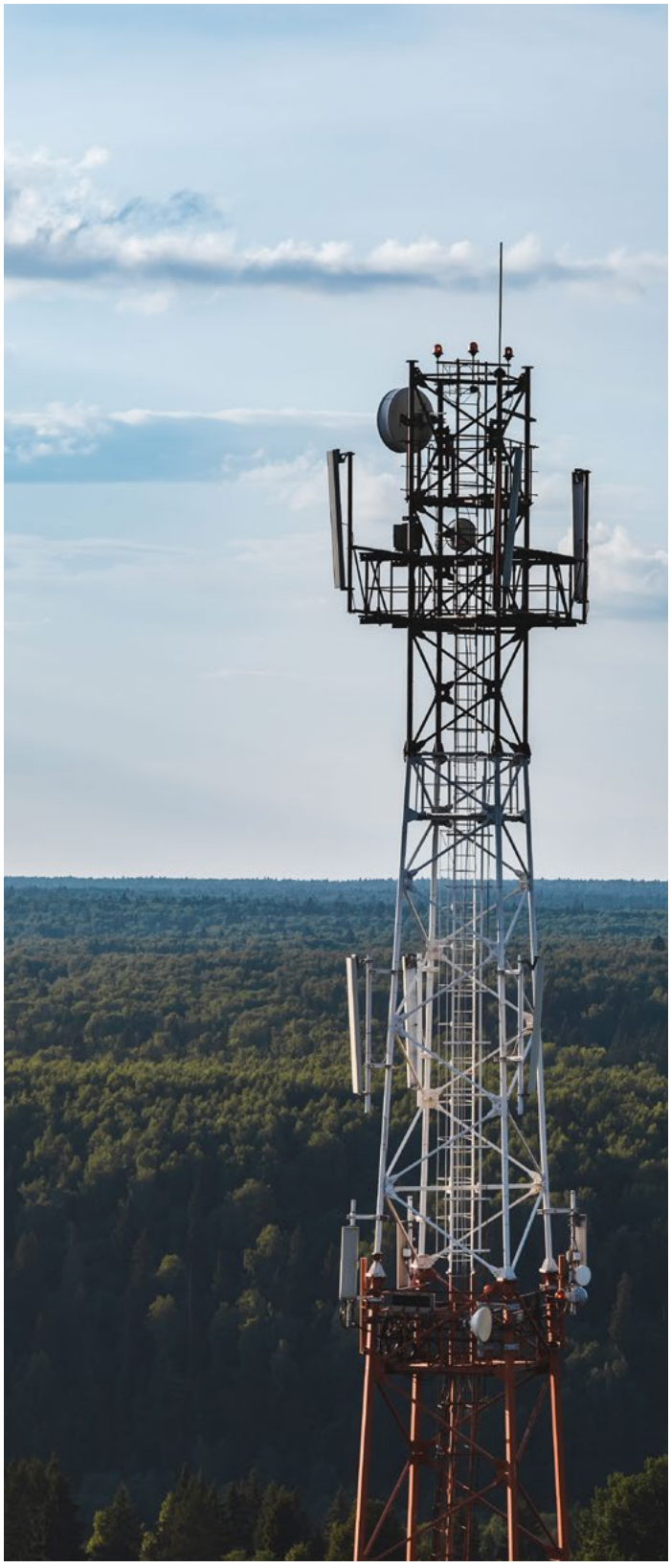
Highlights need to strengthen cybersecurity in the telecoms sector and protect public digital infrastructure.

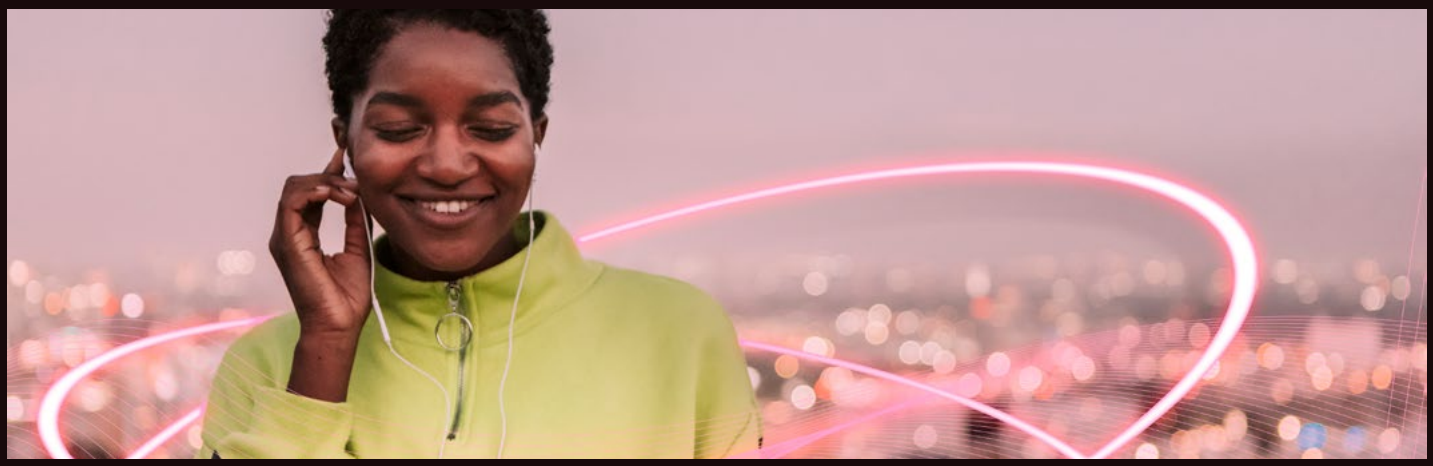
Points out that growth in digital services depends on strong cybersecurity, regulatory compliance, and risk management.

Stresses that cybersecurity is a national imperative, requiring proactive, coordinated, and relentless efforts.

Warns that failure to act decisively on risks cyberattacks, will lead to financial crime, systemic vulnerabilities, loss of public trust and economic damage.

Calls for all stakeholders to collaborate in building a resilient and secure cyber environment as South Africa digitizes services and integrates AI.





Allies in Strengthening Telecom Resilience for a Safer Digital Future for South Africans

In an era where connectivity powers our everyday lives, ensuring the security and resilience of our telecommunications networks has never been more critical. At Cell C, we believe that safety is not a siloed effort — it's a shared responsibility. That's why we are proud to stand alongside COMRiC and our industry peers in building a more secure digital environment for all.

In a world where digital connection is both a lifeline and a lever for progress, the need for secure, resilient telecommunications infrastructure has never been more urgent. The rise in criminal activity targeting network infrastructure not only threatens service continuity — it threatens the very fabric of how South Africans live, work, and thrive.

As proud members of the Communication Risk Information Centre (COMRiC), Cell C reaffirms its stance: we are not just players in this industry — we are allies in ensuring that we are able to maximise consistent connectivity delivery to South Africans, finding solutions to minimise the impact of rising crime of telco infrastructure damage. We are allies in protecting the lives and livelihoods that depend on uninterrupted, safe communication. We have a shared mission to create a sector that is not only connected, but secure.

COMRiC's work is a powerful reminder that safety in telecoms isn't an isolated effort — it is a collective responsibility. Our collective efforts through COMRiC underscore our unwavering commitment to this ethos of shared vigilance, the industry pooling of intelligence, aligning risk mitigation strategies, and taking proactive steps to defend the backbone of digital South Africa.

With this mission in mind, being an ally goes beyond just a statement — it must be a way of working. It means collectively as an industry consistently collaborating and showing up, not just in times of crisis, proactively with purpose and integrity. This is with the citizens of South Africa at the heart of every decision and sustainability of infrastructure.

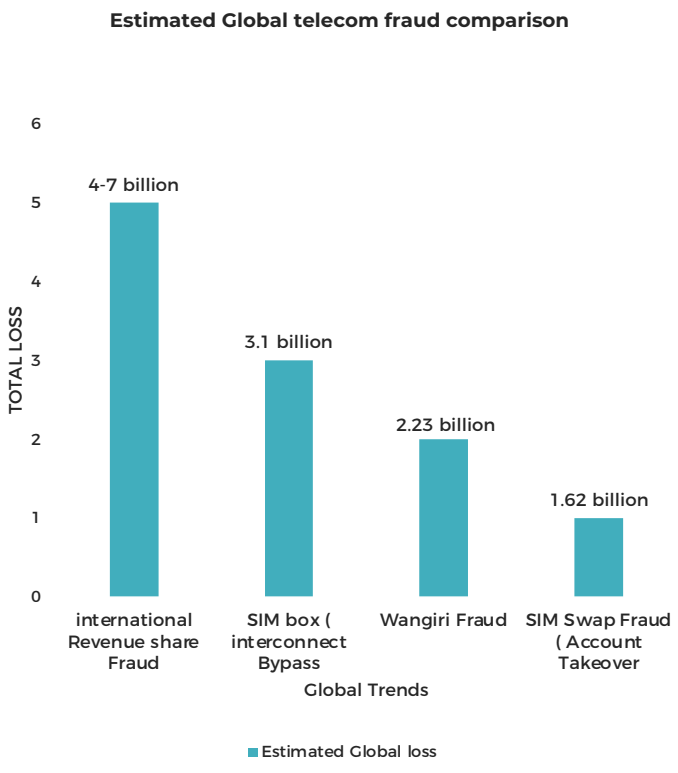
As this inaugural COMRiC Sector Report outlines the progress, challenges, and road ahead, we stand proudly in solidarity. We understand that every partnership formed takes us one step closer to a future where South Africans can connect with confidence — anytime, anywhere.

Together, we are not only responding to threats — we are shaping a safer, smarter future for telecommunications in South Africa.

White Collar Crime Fraud Analysis

Global Trends
- SIM Swap Fraud
- Digital Fraud
- Subscription fraud
- International Revenue Share Fraud (IRSF)
- Wangiri Fraud

South Africa Trends
- SIM Swap Fraud
- Phishing, Smishing, and Vishing
- Internal Fraud
- Digital fraud
- Subscription fraud
- One-Time Pin Scams



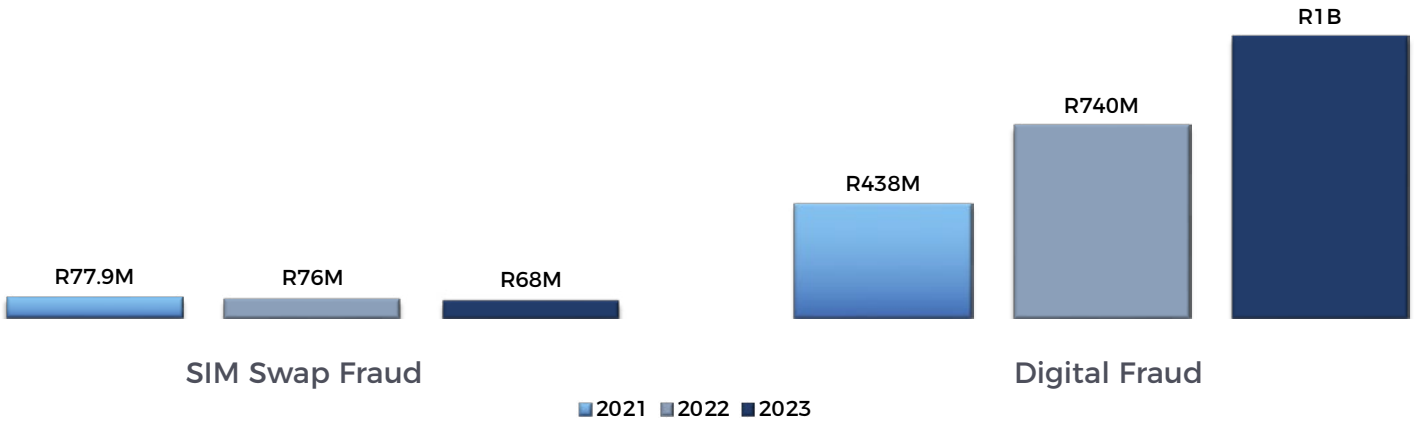
https://dialzara.com/blog/telecom-fraud-analytics-key-trends-2024

Summary of Global Trends in 2024
- IRSF remains the biggest global telecom fraud threat in terms of financial loss.
- SIM Box Fraud still has a major impact but is being reduced in countries like Tanzania, Ghana, and Kenya.
- Wangiri fraud is increasing globally, particularly in regions with low consumer awareness.
- SIM Swap Fraud is growing fast, especially in markets with weak mobile number protection tied to financial accounts.

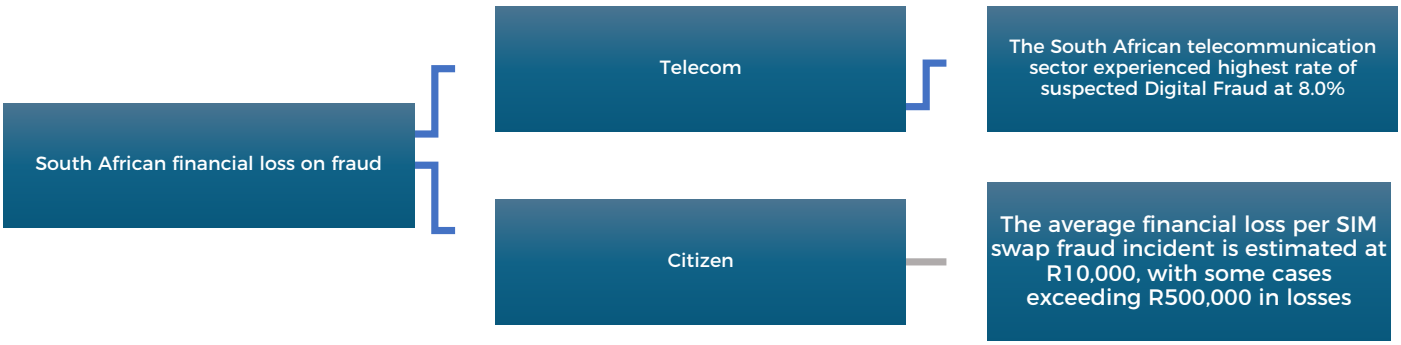
South Africa's telecommunication has faced a surge in fraud – related incidents including SIM-related fraud, digital banking breaches and infrastructure theft. Weak enforcement and technology evolution has allowed fraud syndicates to exploit vulnerabilities, leading to revenue losses and damaged consumer trust.

SIM Swap fraud remained dominant mobile banking threat accounting for 58% of fraud incidents in 2023 according to SABRIC.

Reported financial loss in South African in the telecommunication sector



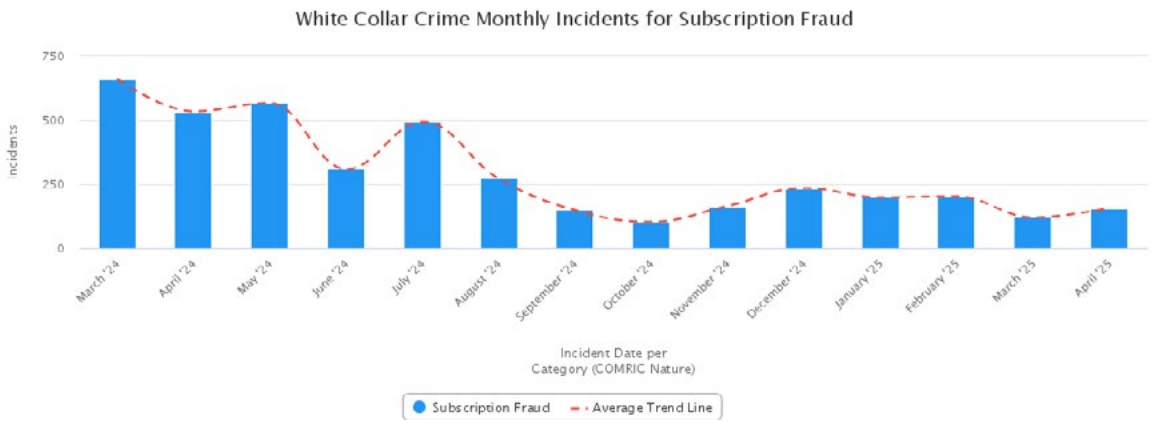
https://mybroadband.co.za/news/banking/464867-big-surge-in-banking-app-fraud-in-south-africa-beware-sneaky-sim-swaps.html?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054
https://www.itweb.co.za/article/sa-sees-alarming-rise-in-digital-banking-fraud/VgZey7JlzZPqdjX9?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054
https://www.banking.org.za/news/sabric-reports-significant-increase-in-financial-crime-losses-for-2023/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054



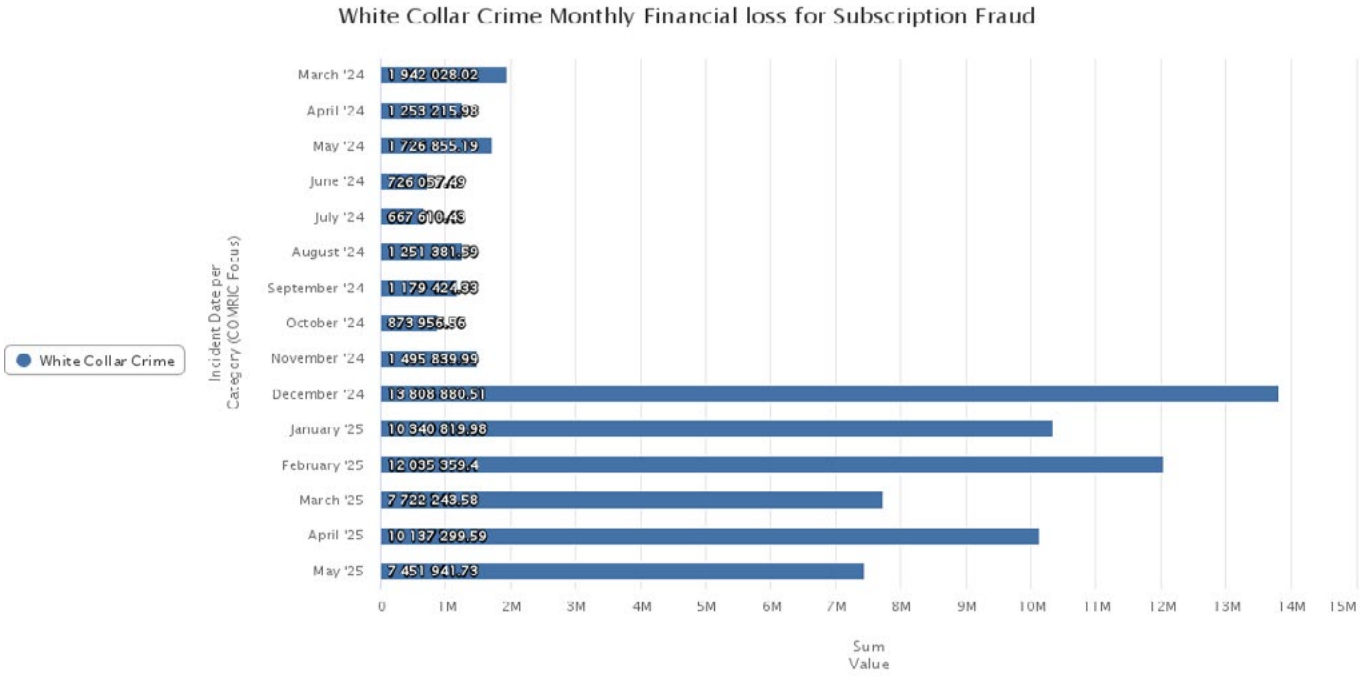
South Africa's telecommunication industry faced mounting pressure as SIM swap and digital fraud surged between 2022 and 2023. While incident numbers are dropping, the MNO's are putting stricter controls to arrest the situation.

Synthetic Identity Fraud: Used to create fraudulent telecom subscription.AI-driven phishing scams: targeting mobile banking users through fake SMS and emails. Premium rate call scams: criminals rerouting calls for financial gain.

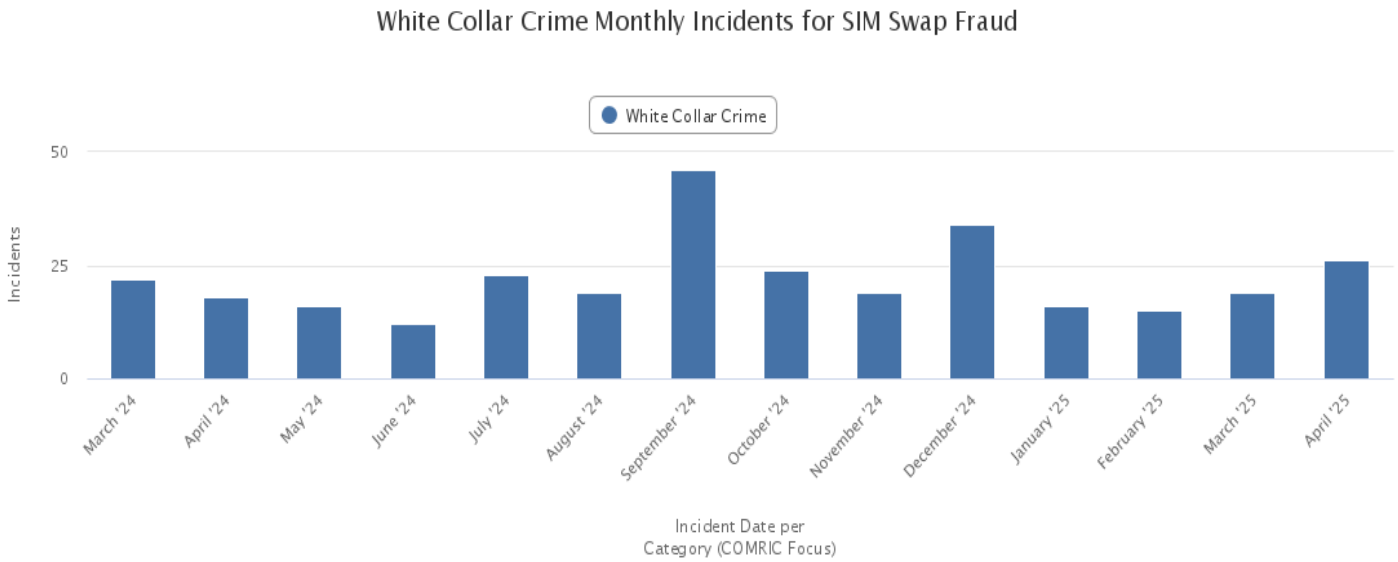
Pre-RICA'd SIM Cards remain a problem with 62% of extortion cases linked to telecom fraud. Should new SIM regulations not be introduced, fraud incidents will continue growing.



Based on the information received from our members, we have observed a downward trend from 2024 to 2025. While ongoing data collection may reveal minor fluctuations, the global adoption of artificial intelligence is expected to further reduce incidents. This anticipated decline is attributed to the implementation of more robust systems, particularly in the areas of subscriptions and other digital services.

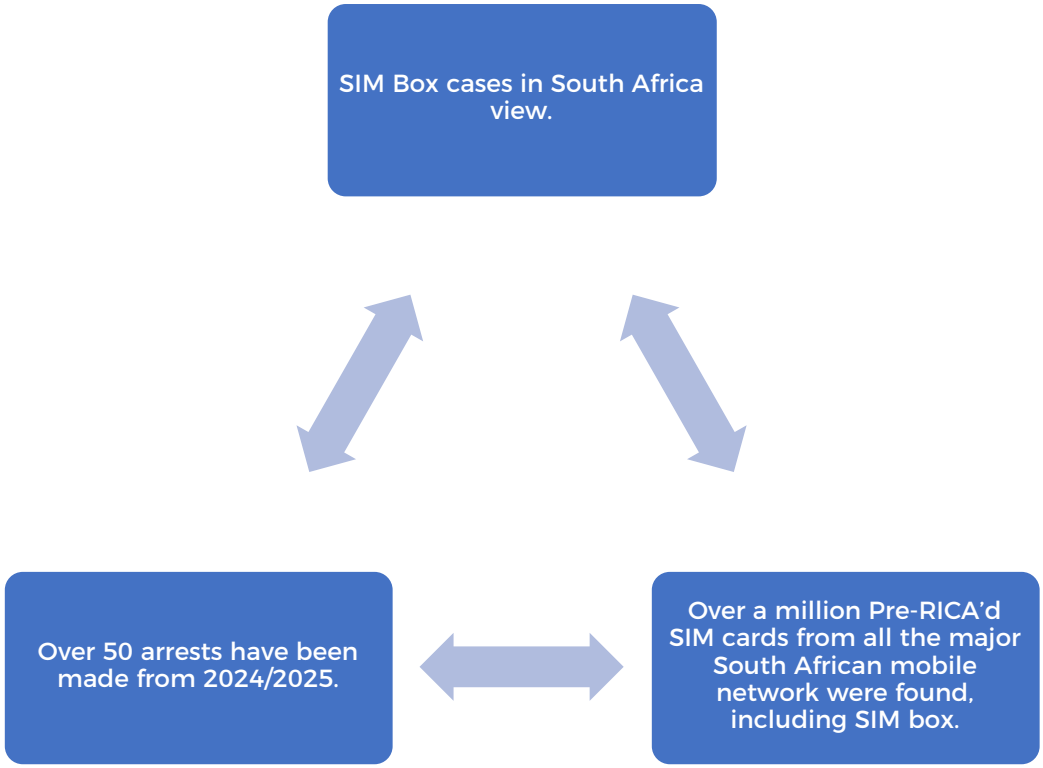


From March 2024 to April 2025, we have observed fluctuations in SIM Swap fraud cases. This serves as a reminder that fraud prevention requires ongoing vigilance and continuous adaptation to emerging threats. There remains a commitment in the sector to continue protecting consumers and enhance security measures.



SIM box remain a major global challenge, costing telecom providers billions annually compromising network integrity. While regions like Europe and Asia have successfully reduced fraud through AI – driven detection, biometric verification and rapid response systems, South Africa faces enforcement gaps that allow fraudsters to exploit weak regulations.

Globally, SIM box fraud prevention has seen significant progress, with law enforcement and telecom providers adopting advanced technologies and stricter regulations.



South Africa's response to SIM box fraud has been slower compared to global efforts but recent crackdowns shows progress.

MTN proud to stand with COMRiC in the fight against network infrastructure crime

By Bradley Swanepoel Chief Risk Officer, MTN SA

MTN South Africa is proud to stand alongside fellow industry partners as an active member of the Communications Risk Information Centre (COMRiC), a vital collaborative platform aimed at addressing one of the sector's most pressing challenges: crime targeting telecommunications infrastructure.

As South Africa's digital economy grows, the protection of critical network infrastructure has become more important than ever. The theft of batteries, vandalism of network sites, and other criminal activities not only disrupt essential communication services but also hinder economic participation and social connectivity in communities across the country. Through COMRiC, MTN and its industry peers have formed a united front to combat this scourge through shared intelligence, coordinated efforts, and strategic collaboration with law enforcement agencies.

Since joining COMRiC, MTN has made significant strides in its infrastructure protection efforts, from deploying advanced security measures at high-risk sites to improving response protocols and working closely with law enforcement to ensure swift action against criminal networks. The results speak for themselves: a reduction in incidents at targeted sites, improved network resilience, and enhanced service reliability for our customers.

MTN's participation in COMRiC is not only about safeguarding infrastructure, it's about protecting the digital lifeline of millions of South Africans who rely on mobile connectivity for work, education, healthcare, financial services, and staying connected with loved ones. This commitment forms part of our broader ambition to lead digital solutions for Africa's progress.

Looking ahead, MTN will continue to invest billions of rands in strengthening and modernising its network infrastructure across South Africa. These investments are designed not only to expand coverage and improve network quality but also to ensure that the network remains secure, resilient, and future-ready in the face of evolving threats.

MTN commends COMRiC for its continued leadership and impact in uniting the industry against infrastructure crime. We believe that by standing together, sharing knowledge, and taking decisive action, we can build a safer, more reliable digital future for all.

How other countries have seen a decline in the SIM box cases due to reasons listed below and how should South Africa respond.

Tanzania
Has continued reducing International call fraud by 15% in the early 2024, which is linked to SIM box activity. Following the deactivation of fraudulent SIM cards - and building on its earlier success in reducing fraud from 65% to 10% between 2017 and 2020, the initiative continues to strengthen digital security.

Ghana
- Achievement: Significant dismantling of SIM box fraud networks.
- Established a Fraud Management System in collaboration with the National Communications Authority (NCA), Ghana Revenue Authority (GRA), and law enforcement agencies.
- Conducted coordinated raids leading to the seizure of SIM boxes and the arrest of operators.
- Mandated telecom operators to deactivate unregistered SIM cards and held them accountable for SIMs used in fraudulent activities

This is how some countries have responded to SIM box related fraud. By adopting some of these measures, South Africa will align with global best practices and significantly reduce SIM box fraud.

Telecom fraud in South Africa has been widespread, with certain areas experiencing higher risks due to digital vulnerabilities, pre-RICA'd SIM cards, and organised crime syndicates.

Urban centers (Johannesburg, Cape Town, Durban) - these cities have seen high rates of SIM swap fraud, Subscription fraud and digital banking scams.

Fraud Prevention Measures in Telecom

AI – Powered Fraud Detection – Mobile operators have integrated machine learning models to detect suspicious transactions and prevent fraud.

Biometric SIM Registration – As of 2025, South Africa is in a transitional phase regarding the implementation of biometric SIM registration under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).

Real- Time Monitoring Systems – Telecom providers now use automated fraud detection tools to track unusual activity.

Stronger Authentication Protocols – Multi – layer security measures including two- factor authentication, have been enforced to prevent unauthorized SIM swaps.

Industry Collaboration – mobile operators like MTN, Vodacom and Telkom have partnered with GSMA Open Gateway to standardize fraud prevention APIs.

Consumer Awareness Campaigns – Public education efforts have increased to help individuals recognize and avoid scams.

Conclusion: Toward a Secure and Resilient Sector

The COMRiC Telecommunications Sector Report 2025 1st Edition arrives at a crucial time for South Africa's telecommunications industry five years after the founding of COMRiC, and during the most complex and fast-evolving risk environment this sector has ever faced.

What began as a voluntary alliance of network operators has matured into a central pillar of South Africa's digital risk landscape. COMRiC's role has grown in both scope and substance convening competitors, connecting sectors, guiding strategic responses, and, crucially, aligning public and private stakeholders around a common threat intelligence framework.

This first edition reflects the scale and seriousness of the issues at hand. Infrastructure vandalism, SIM swap fraud, subscription scams, ransomware attacks, insider threats, and synthetic identity fraud are not isolated incidents they are part of a systemic, multi-billion-rand criminal economy that threatens to derail the country's digital transformation. They degrade service delivery, discourage investment, and weaken trust in the very systems meant to drive inclusion and innovation.

Yet this report is also a testament to progress. In the past year, we've seen industry players move from reactive measures to proactive, data-led prevention. AI-powered fraud detection, biometric authentication, real-time SIM monitoring, and a new generation of consumer awareness campaigns are reshaping how we think about risk. COMRiC's coordination with SAPS, ICASA, NDMC, and international partners has already resulted in the dismantling of several criminal operations and a noticeable dip in certain fraud categories.

But these gains are not permanent, and the stakes are rising. As cyber-physical risks converge, and as geopolitical and economic pressures intensify, South Africa's telecommunications networks are fast becoming high-value targets for criminals, state actors, and opportunists alike. The regulatory environment must now evolve with equal urgency. Legislative reform, particularly to RICA and related frameworks, is not just desirable, it is critical. Without it, our capacity to monitor, respond, and prosecute is dangerously constrained.

This report also highlights an uncomfortable truth: South Africa remains behind global best practice in several key areas. SIM box fraud, for instance, continues to flourish here while other countries have stemmed the tide through the adoption of AI monitoring systems, tighter registration laws, and aggressive enforcement. Our response must be bolder and better coordinated and COMRiC stands ready to lead that charge.

A secure telecommunications sector is not just an operational imperative. It is foundational to everything else from financial services to emergency response, education to e-voting, social cohesion to global competitiveness. The digital economy cannot flourish while its foundational infrastructure remains under siege.

Looking ahead, COMRiC will intensify its focus on building a national Computer Security Incident Response Team (CSIRT), driving implementation of a National Cybersecurity Resilience Plan, and expanding knowledge-sharing between sectors. We call on government, regulators, financial institutions, civil society, and academia to engage with us meaningfully not only when crises erupt, but in building the protocols, partnerships and platforms that will prevent them.

The road ahead demands vigilance, collaboration, and boldness. But with shared intelligence, unified purpose, and the political will to act, we can secure our networks, protect our citizens, and unlock the true potential of a digitally connected South Africa.

The threats are real. The consequences of inaction are severe. But the foundation has been laid, and the momentum is with us.

Our Partners

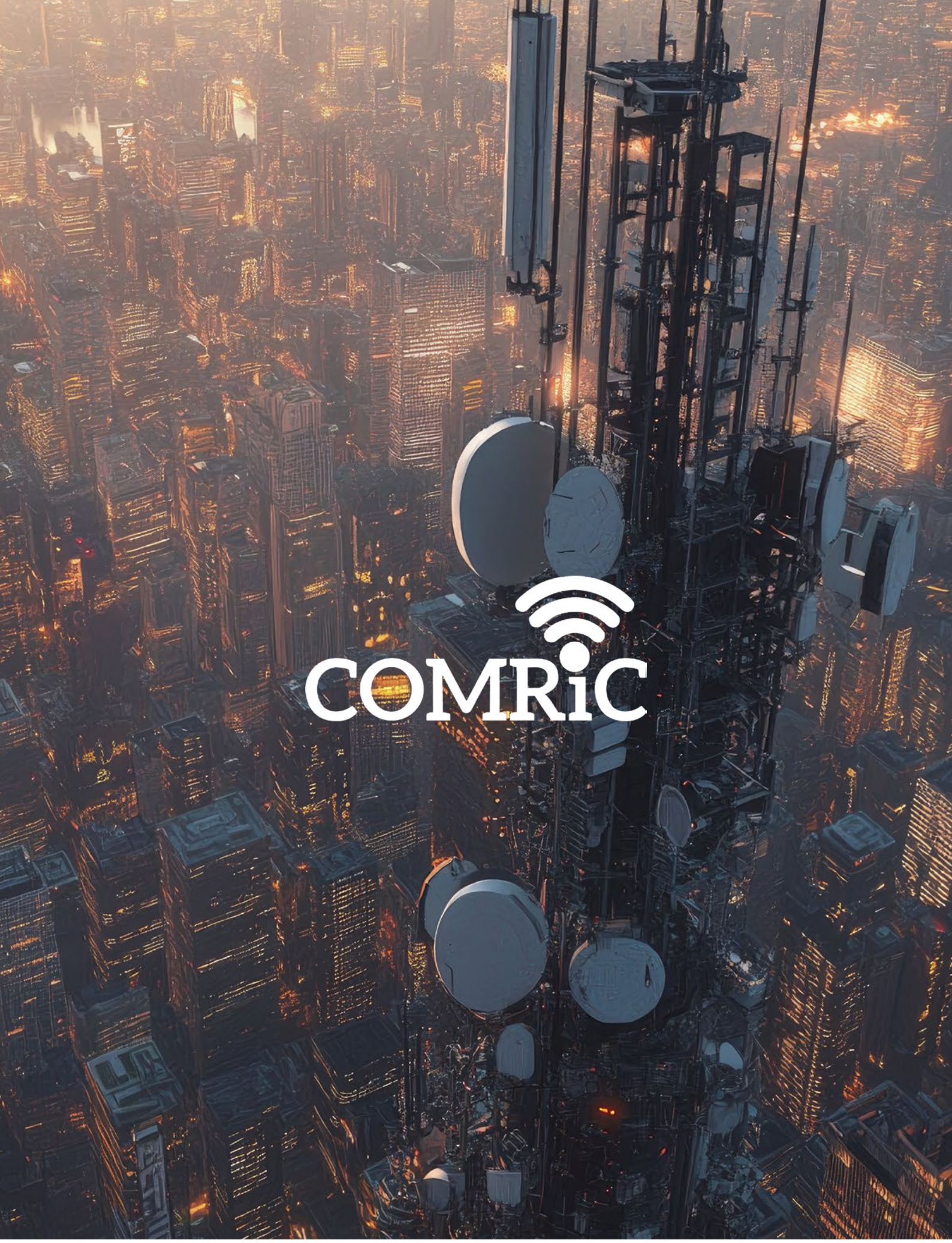
We extend our gratitude to our founders, industry alliances and partners for their indispensable support, expertise, and collaboration throughout the years. Your commitment has been instrumental in advancing our shared goals and driving meaningful impact within our sector.

Founders

Our Collaborators

Connect With Us

www.comric.co.za
Email: info@comric.co.za
Instagram: @comricza
X: @COMRiCSA
Facebook: COMRiC
LinkedIn: COMRiC


COMRiC