



Securing *the* Ecosystem: *The* Role of Regulators, Industry, *and* Investors *in* Telecom Cyber Resilience

To secure telecom networks in emerging markets, operators need to work with regulators, investment groups, and other industry players to create a more resilient ecosystem.

This article is part of the **Safeguarding the Digital Backbone: Building Resilient Telecom Infrastructure in Emerging Economies** series, produced by the International Finance Corporation (IFC, Note 1). Drawing on original IFC research into the cyber-readiness of telecom operators across Africa, Asia-Pacific, Europe, Latin America, and the Middle East, the series examines why cybersecurity has become a strategic imperative for the sector, and what operators, regulators, and development finance institutions (DFIs) can do to close the gaps. Each article stands alone and builds toward a practical picture of what resilient telecommunications infrastructure looks like in emerging economies.

- Article 1: From Connectivity to Critical Infrastructure: Why Cybersecurity is Now a Telecom Imperative
- Article 2: The Expanding Threat Landscape: How Cyberattacks Are Targeting Telecom Networks
- Article 3: Breaking Through Barriers: Cybersecurity Challenges Facing Telecom Operators in Emerging Markets
- Article 4: What Good Looks Like: Building a Cyber-Resilient Telecom Operator
- **Article 5: Securing the Ecosystem: The Role of Regulators, Industry, and Investors in Telecom Cyber Resilience**

On February 3, 2025, representatives of 40 African governments signed the constitution of the African Network of Cybersecurity Authorities (ANCA), committing to a five-year strategy for cross-border threat intelligence sharing, policy harmonization, and coordinated incident response (Smart Africa 2025). The signing came less than a year after hacktivist groups simultaneously attacked three Ugandan mobile operators in the same campaign and exposed a central vulnerability: operators facing the same threat within the same country had limited mechanisms for coordinating their responses (Geopolitical Report 2024; Kwinika 2024; Otago 2024).

The ANCA is a direct response to the lack of coordination between computer emergency response teams (CERTs), policy makers, and investment groups in the various member nations. It builds on years of capacity-building investment by the International Telecommunications Union (ITU), the African Union, and international donors. By April 2026, those efforts had produced a three-point blueprint to establish a framework for partnerships, a goal of launching two or three pilot programs within six months, and the creation of a Continental Cybersecurity Collaboration Roadmap for 2026–2028 (AlgeriaTech 2026).

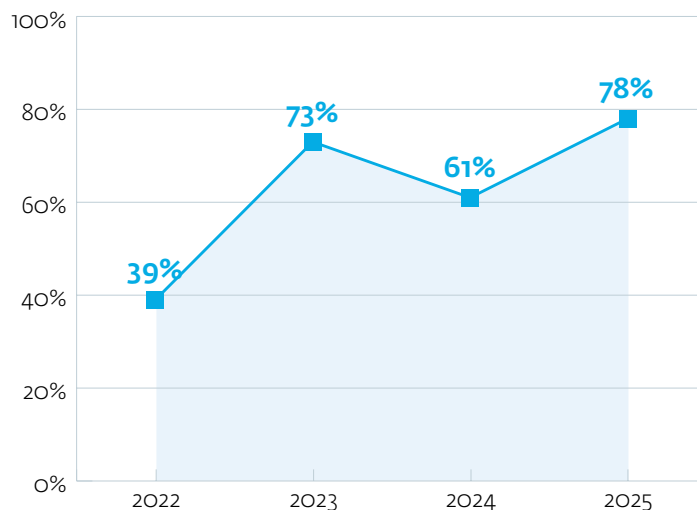
The group aims to solve two key problems facing telecom operators: regulatory fragmentation and lack of coordination in cyberattack responses. The World Economic Forum’s *Global Cybersecurity Outlook 2025* found that, while 78 percent of business leaders considered regulation effective in reducing risks (Figure 1), 69 percent found them “too complex or too numerous or experiencing difficulty verifying whether third-party suppliers are complying with the requirements” (WEF 2025, 27–28), suggesting that more work on regulatory frameworks and support is needed.

The consequences extend well beyond compliance headaches. Telecom networks are the foundation of modern economies, and when they fail or are compromised, the damage cascades to every system that depends on them, including banking, health care, and government services. For example, the September 2023 ransomware attack on Colombian cloud and telecom provider IFX Networks also affected more than 50 government agencies (Grieg 2023).

Closing the gap demands coordinated action from three groups that have historically operated in parallel rather than in concert: governments and regulatory authorities, which set the operating environment through licensing conditions, reporting mandates, and supply-chain security requirements; industry and standards bodies, which define and propagate what “secure” looks like in practice, and development finance institutions (DFIs), which shape investment incentives across markets that commercial capital often bypasses.

Figure 1

Perceived Benefit of Cybersecurity Regulations among Business Decision-Makers



Source: WEF 2025, 27.

No telecom operator can achieve meaningful cyber resilience in isolation. The threat environment is too complex, the resources required too large, and the geopolitical dimensions too significant for any single company to manage alone. Securing the telecom ecosystem requires coordinated action between these three interlocking groups, with each bringing their own expertise and capabilities and playing a distinct and necessary role in securing the telecommunications sector from cyberattacks.

Why ecosystem coordination matters

Telecommunications networks reach into every aspect of the economies they serve; therefore, a breach at one operator can propagate to roaming partners, shared infrastructure providers, and ultimately the services that banks, hospitals, and governments depend on to function. The impact of the attack on IFX Networks did not just affect a single provider’s network but cascaded into a national emergency within hours (see Article 1).

According to Lacina Koné, CEO of Smart Africa, coordination and collaboration between national government and industry sectors is critical for creating cyber-resilient economies.

“Cybersecurity is no longer a national issue; it is a continental and global concern,” said Koné, at the adoption of the ANCA constitution. “Through ANCA, we are building a strong,

coordinated framework that will allow African nations to tackle cyber threats collaboratively. This is essential not only for the safety of our digital infrastructure but also for the realization of our vision of a single digital market by 2030.”

When operators share intelligence rather than guarding it, collective capability exceeds what any individual actor can build alone. The Global System for Mobile Communications (GSMA) Telecommunications Information Sharing and Analysis Centre (T-ISAC) brought together threat intelligence specialists from operators across more than 100 countries in September 2024. By year’s end, AI-powered commercial feeds were enabling near-real-time attacker profiling across the platform, a capability that no emerging-market operator could sustain unilaterally (GSMA 2024). This capability is especially powerful for smaller operators that may not otherwise have the internal resources to track adversaries targeting their networks.

Collaborating with government and regulatory authorities, DFIs, and industry and standards agencies helps telecom operators better understand the risk landscape, how they can improve their own cybersecurity posture, and how they can provide feedback on the regulatory frameworks in which they operate.

Governments and regulatory authorities: Sharing intelligence and harmonizing legislation

Governments set the environment in which telecommunication providers operate. Licensing requirements, incident-reporting mandates, supply-chain security requirements, and data-protection standards all determine how seriously operators invest in security. When those requirements are absent, weak, or incompatible across borders, the resulting patchwork can become a burden for telecom operators.

Government agencies and regulatory authorities can first help by setting minimum cybersecurity and resilience standards for critical infrastructure. Incident reporting, for example, is one of the most significant areas where regulatory frameworks fall short. Only 30 percent of African countries have a functioning system for operators to report cyber incidents to regulators, which means that most of the continent’s regulatory authorities are making cybersecurity policy without knowing what threats their operators are facing (INTERPOL 2025, 23). The Inter-American Development Bank’s 2025 *Cybersecurity Report* documents a parallel deficit across Latin America and the Caribbean: data privacy and basic compliance requirements are relatively common, but supplier security, product security, and

secure development practices are almost entirely absent from most national frameworks (IDB 2025).

Progress is being made. South Africa’s Information Regulator began mandating structured online breach reporting in 2025. Kenya updated its Computer Misuse and Cybercrimes Act in 2024 to strengthen protections for critical information infrastructure. The European Union’s NIS2 Directive, which designates telecoms as essential entities and requires 24-hour incident notification, is lifting the baseline for what operators have come to expect of regulators wherever they operate (Ndege 2025; INTERPOL 2025).

Yet, the other area that governments can help is harmonizing regulations across borders. The primarily African mobile-network operator MTN Group faces a patchwork of cybersecurity and data-protection standards because it has customers in 19 countries across Africa and the Middle East (see Article 2). In each one, its cybersecurity teams confront a different legal environment, with potentially different incident-reporting timelines, different supply-chain security requirements, and different data-protection rules. To somewhat simplify the problem, the company relies on six different cybersecurity regulatory regimes, including ISO/IEC 27001:2013, the United States’ NIST Cybersecurity Framework, the European Union’s General Data Protection Regulation, and South Africa’s Protection of Personal Information Act (MTN Group 2025).

Harmonization of legal frameworks could help simplify operations for every telecommunication provider, rather than make compliance a headache.

“Staying compliant means regularly updating the compliance matrix to reflect new events, along with data mapping for data location identification and risk classification to maintain a high standard of compliance,” says Marcio Felix, head of information security for Scala, a data center operator.

The most ambitious regional response is the ANCA, which represents the continent’s first structured mechanism for sharing threat intelligence and harmonizing legislation across borders. These capabilities are precisely the kind of coordination that individual operators, however capable, cannot build for themselves (Smart Africa 2025).

The role of industry and standards bodies

When regulations and policies do not yet exist—or are fragmented across markets—industry standards and best practices are a solid foundation on which to build a more mature cybersecurity program. Industry and standards bodies define, in technical terms, what a secure telecom network looks like. The GSMA, ITU, European Telecommunications Standards Institute, and 3rd Generation Partnership Project collectively produce the frameworks on which every operator’s security program should be built.

The ITU’s *Global Cybersecurity Index (GCI) 2024* established a yardstick by which emerging markets can measure the maturity of their cybersecurity programs (Figure 2). Assessing 194 countries across legal, technical, organizational, capacity, and cooperation dimensions, the index found that in Africa, only 5 of 46 assessed states—Ghana, Kenya, Mauritius, Rwanda, and Tanzania—ranked in the global top tier, while most fell in the “establishing” or “evolving” categories. Among the factors keeping African economies behind are limited cybersecurity laws and a lack of capacity to enforce them or respond operationally to incidents (ITU 2024).

Rwanda offers the clearest evidence that this gap can be closed. By embedding minimum security requirements in telecom licensing conditions, mandating incident reporting, and integrating cybersecurity criteria into infrastructure investment approvals, the country ranked in the top third globally on the ITU GCI 2024—the highest-performing state in its subregion (ITU 2024).

For operators not yet at Rwanda’s level, the GSMA’s FS.31 Baseline Security Controls offer a practical starting point: a minimum standard covering the core controls every mobile operator should have in place, with clear benchmarks against which progress can be measured (GSMA 2025). In addition, the ITU Telecommunications Standardization Sector’s (ITU-T)

technical specifications cover network virtualization security, threat intelligence integration, and interconnection security and can help translate policy requirements into engineering implementation. However, adoption of both frameworks in Africa and Latin America remains uneven, so closing that gap can result in a significant medium-term payoff.

Public-private collaboration in practice

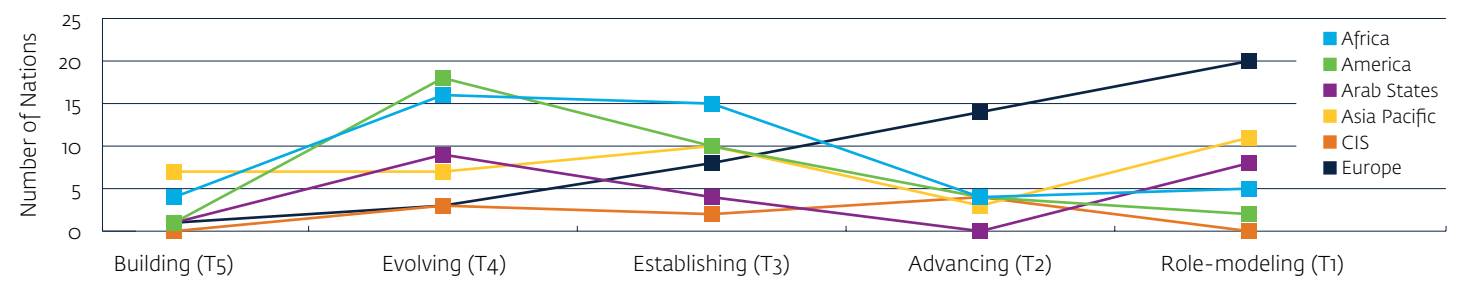
The strongest models of telecom cyber resilience combine all three levers—regulatory requirements, DFI-funded technical assistance, and industry standards adoption—combined so that each reinforces the others. Organizations that do not advance in all three areas tend to have poorer outcomes.

Brazil’s Lei Geral de Proteção de Dados, enacted in 2018 and enforced from 2020, prompted telecommunications firms to invest in cybersecurity and compliance, but translating a law into operational reality required multiyear technical assistance programs that the legislation itself did not fund. Such a gap could be filled by DFIs (Recording Law 2026).

The ANCA’s February 2025 constitution creates the governance architecture for an end-to-end model, with member-state regulators sharing threat intelligence and harmonizing legislation, industry bodies providing the technical frameworks that regulators need to write meaningful rules, and a dedicated CERT based in Morocco providing the operational backbone for cross-border incident response (Smart Africa 2025). The coordination enabled by the collaborative group allows each nation to respond to cross-border threats (Smart Africa 2025).

The areas of collaboration make a difference because they establish trusted relationships and communication channels that become critical during an incident.

Figure 2
Regional Distribution of Cybersecurity Maturity Levels



Source: ITU 2024, 1.

Note: CIS = Commonwealth of Independent States

DFIs and Commercial Banks: Driving resilience through investment

DFIs occupy a distinctive position in this ecosystem. Unlike regulators, they cannot compel telecom operator behavior, and unlike industry bodies, they are not primarily in the business of setting technical standards. Instead, DFIs have capital, technical assistance capacity, and sustained relationships with operators and governments across markets that commercial financiers routinely bypass. This combination gives them unusual leverage over where and how telecom cybersecurity investments are made. Commercial banks can have the same influence by including conditions in the due-diligence and loan agreements.

IFC has been a first mover in many markets and subsectors, helping deliver pioneering investments and bringing private sector expertise and solutions. Its investments represent 40 percent of all DFI investments in the sector globally.

For example, IFC invested more than \$950 million in telecommunications sectors globally—about 5 percent of its total investments in FY25. IFC recognizes that the compromise of a telecom operator results in harm that flows not only to the impacted organization but to the communities that depend on that operator for connectivity, commerce, and access to public services. These investments aim to develop capabilities to reduce cybersecurity risk and improve development outcomes.

The most direct lever available to DFIs is the investment relationship itself. An institution that requires measurable cybersecurity improvements as a condition of financing can also provide technical assistance to help operators meet those requirements. In addition, DFIs can bring together various organizations from their portfolios, promoting cross-sector collaboration between operators, regulators, and industry experts. This guiding relationship can drive security improvements faster and more durably than regulatory mandates alone.

Because the focus is on long term investment, DFIs do not treat cybersecurity as a due-diligence checkbox, but as a monitored performance metric throughout the investment life cycle. DFIs are also well positioned to develop and share sector-specific telecom security assessment tools, which help to fill the gaps in expertise and incentives that most commercial institutions lack. In markets where regulatory frameworks are still developing and adoption of industry standards is uneven, DFIs can add regional perspectives, share global insights on best practices, and offer hard-earned lessons from previous engagements. Overall, they may be a reliable source of guidance and aid for regional telecom operators.

Conclusion: Key actions for each stakeholder

Enhancing telecommunications cyber resilience demands a multistakeholder approach that integrates the efforts of regulatory bodies, the investment community, and industry participants. In emerging markets, where resource limitations and capacity constraints are more pronounced, such systemic coordination becomes a critical prerequisite for success.

Regulators need to close three gaps in parallel. First, mandate and operationalize incident reporting so that authorities know what is happening on the networks they oversee. This is a basic prerequisite for evidence-based policy that 70 percent of African countries currently lack (INTERPOL 2025, 23). Second, create robust regulatory coverage that covers security requirements for critical infrastructure, suppliers, products and software. National economies and industries tend to grow faster in countries with higher levels of cybersecurity maturity (Vergara Cobos, Cakir, Mei-Zahav, and Barakcin Berkay 2024, 4). Third, invest in enforcement capacity alongside rule-writing, because regulations that cannot be enforced do not change operator behavior. Regional harmonization, such as the ANCA in Africa and the Organization of American States frameworks in Latin America, brings additional aid to organizations that have operations in multiple markets.

Industry and standards bodies need to concentrate on two priorities in emerging markets. First, operators should be encouraged to participate in T-ISAC groups to add their own telemetry and experiences to the threat-intelligence capability and cooperate with national CERTs or cyber incident response teams. Second, they should encourage telecom operators in markets without an established baseline to adopt industry cybersecurity standards, such as GSMA FS.31 and ITU-T standards.

Telecom operators need to take an ecosystem-wide view of cyber resilience, rather than focusing only on their own defenses. Only through collaborating with other stakeholders, such as government agencies, industry specialists, and even competing companies, can operators improve their own cybersecurity maturity and the resiliency of their networks.

DFIs need to embed cybersecurity criteria into preinvestment due diligence and require repeated checks throughout the investment life cycle. Funding cybersecurity improvement, developing sector-specific telecom security assessment tools, and treating security posture as an ongoing performance indicator should all be critical parts of any funding agreement.

Endnote

1. The development of this series was financially supported by the World Bank Cybersecurity Multi-Donor Trust Fund and guided by German Cufre, Director of Access & Affordability. It was delivered as a team effort led by Charlotte Kaheru, with key contributions from Maurice Kaleek Isaac, Massiel Lopez, and Morshed Haque. Significant contributions from Lemos Associates LLC are gratefully acknowledged. The series was informed by a foundational study conducted by IFC in collaboration with Ernst & Young LLP (EY), with appreciation extended to Kunal Bhatia, Partner – TMT Consulting, EY, Ashrut Mahajan, and the broader EY working team. Special thanks are extended to the customers, partners, and stakeholders who contributed to the study and this series, including external peer reviewers. Acknowledgment is also extended to IFC and World Bank colleagues, as well as the Communications teams—including Chris Vellacott, Rob Wright, and Brian Beary—whose feedback helped shape the study and this series.
2. See the ITU Academy's Cybersecurity Capacity Development Programs at <https://academy.itu.int/main-activities/capacity-development/cybersecurity>

References

- AlgeriaTech. 2026. "Algeria and ANCA: A Strategic Playbook for Joining Africa's Continental Cyber Defense Network." AlgeriaTech, May 19, 2026. <https://algeriatech.news/algeria-anca-africa-continental-cyber-cooperation-playbook-2026/>.
- Geopolitical Report. 2024. "Anonymous Sudan Claims Attacks on Ugandan Mobile Providers." February 2024. <https://www.geopolitical.report/anonymous-sudan-claims-attacks-on-ugandan-mobile-providers/>.
- Grieg, Jonathan. 2023. "Several Colombian Government Ministries Hampered by Ransomware Attack." The Record, September 15, 2023. <https://therecord.media/colombia-government-ministries-cyberattack>.
- GSMA (Global System for Mobile Communications Association). 2024. "Uniting Sectors, Strengthening Security: Highlights from the First T-ISAC In-Person Summit 2024." T-ISAC Blog, December 13, 2024. <https://www.gsma.com/solutions-and-impact/technologies/security/t-isac-blog/uniting-sectors-strengthening-security-highlights-from-the-first-t-isac-in-person-summit-2024/>.
- GSMA (Global System for Mobile Communications Association). 2025. "FS.31 Baseline Security Controls v5.0." GSMA, June 9, 2025. <https://www.gsma.com/solutions-and-impact/technologies/security/gsma-fraud-security-group/fs-31-baseline-security-controls/>.
- IDB (Inter-American Development Bank). 2025. *2025 Cybersecurity Report: Vulnerability and Maturity Challenges in Latin America and the Caribbean*. IDB, Washington, DC. <https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and>.
- INTERPOL (International Criminal Police Organization). 2025. *Africa Cyberthreat Assessment Report 2025, 4th ed.* INTERPOL, Lyon. https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf.
- ITU (International Telecommunication Union). 2024. *Global Cybersecurity Index 2024, 5th Edition*. ITU, Geneva. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.
- Kwinika, Savious-Parker. 2024. "Anonymous Sudan Attacks Again, This Time in Uganda." ITWeb Africa, February 9, 2024. <https://itweb.africa/article/anonymous-sudan-attacks-again-this-time-in-uganda/WnxEv4YRKE7V8XL>.
- MTN Group. 2025. "MTN Position Statement: Data Privacy and Protection." Johannesburg, MTN Group. <https://www.mtn.com/wp-content/uploads/2025/06/MTN-Position-Statement-on-Data-Privacy.pdf>.
- Ndege, Adonijah. 2025. "In 2025, Regulation Forced Africa's Cyber Incidents into the Open." TechCabal, December 30, 2025. <https://techcabal.com/2025/12/30/cyber-breaches-became-harder-to-hide/>.
- Otage, Stephen. 2024. "Hackers Target Telecoms, Banks." Daily Monitor Uganda Edition, February 13, 2024. <https://www.monitor.co.ug/uganda/news/national/hackers-target-telecoms-banks-4523294>.
- Recording Law. 2026. "Brazil Data Privacy Laws: LGPD Compliance Guide (2026)." Recording Law, March 21, 2026. <https://www.recordinglaw.com/world-laws/world-data-privacy-laws/brazil-data-privacy-laws/>.
- Smart Africa. 2025. "Smart Africa Adopts Its Constitution and 5-Year Strategy for the African Network of Cybersecurity Authorities (ANCA) to Tackle Cross-Border Cybersecurity Challenges across the Continent." Press Release, February 4, 2025. <https://smartafrica.org/smart-africa-adopts-its-constitution-and-5-year-strategy-for-the-african-network-of-cybersecurity-authorities-anca-to-tackle-cross-border-cybersecurity-challenges-across-the-continent/>.
- Vergara Cobos, Estefania, Selcen Cakir, Hagai Mei-Zahav, and Baran Barakcin Berkay. 2024. *The Role of Cybersecurity in Economic Performance*. Washington, DC: World Bank.
- WEF (World Economic Forum). 2025. *Global Cybersecurity Outlook 2025*. WEF, Geneva. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.