



What Good Looks Like: Building a Cyber-Resilient Telecom Operator

Telecommunications firms in emerging markets need to focus on how to increase the resilience of their businesses and networks—an effort that spans cybersecurity, disaster recovery, and workforce training.

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

In the fourth quarter of 2025, attempted cyberattacks against Kenyan network infrastructure surged more than 440 percent, reaching nearly 4.6 billion threat detections in just three months. The vast majority of those threats represented cybercriminals targeting unpatched flaws and weak internal controls in organizations' systems (National KE-CIRT/CC 2026a, 7; 2026b, 7)

Among those targets were government digital services and the mobile payments app, M-Pesa, managed by telecom operator Safaricom. In its latest fiscal year ending on March 31, 2026, Safaricom noted that the M-Pesa platform handled 46.41 billion transactions—roughly 127 million a day—worth KES 41.68 trillion (\$323 billion), making it not merely a mobile-money app but a foundation of the Kenyan economy (Safaricom 2026, 12, 27).

In response to the increasing attempted attacks, the company, as the largest telecommunications provider in Kenya, pursued a deliberate KES 40 billion (\$310 million) update to the infrastructure of M-Pesa, with a focus on cyber-resilience. Its cybersecurity initiatives included a 24/7 managed security operations center and a geo-locking antifraud system that blocked more than 8,000 threat agents in 2024 (Sama 2024).

Safaricom is not unique in facing these pressures, but its approach underscores the outcome of efforts to shore up security. The visible executive commitment to resilience, investing in new technology, and the establishment of continuous monitoring capabilities designed to detect and respond to threats helped the company maintain its critical services. As telecommunications operators become critical to emerging economies—and as cybercriminals increasingly target their networks and operations—cybersecurity and cyber-resilience must be treated as strategic priorities, not afterthoughts or cost centers.

To attain a high level of security of deployed networks, a holistic strategy is required—one that emphasizes that mitigation takes into account four key players: standards, products and related development processes, network deployments, and network operation.

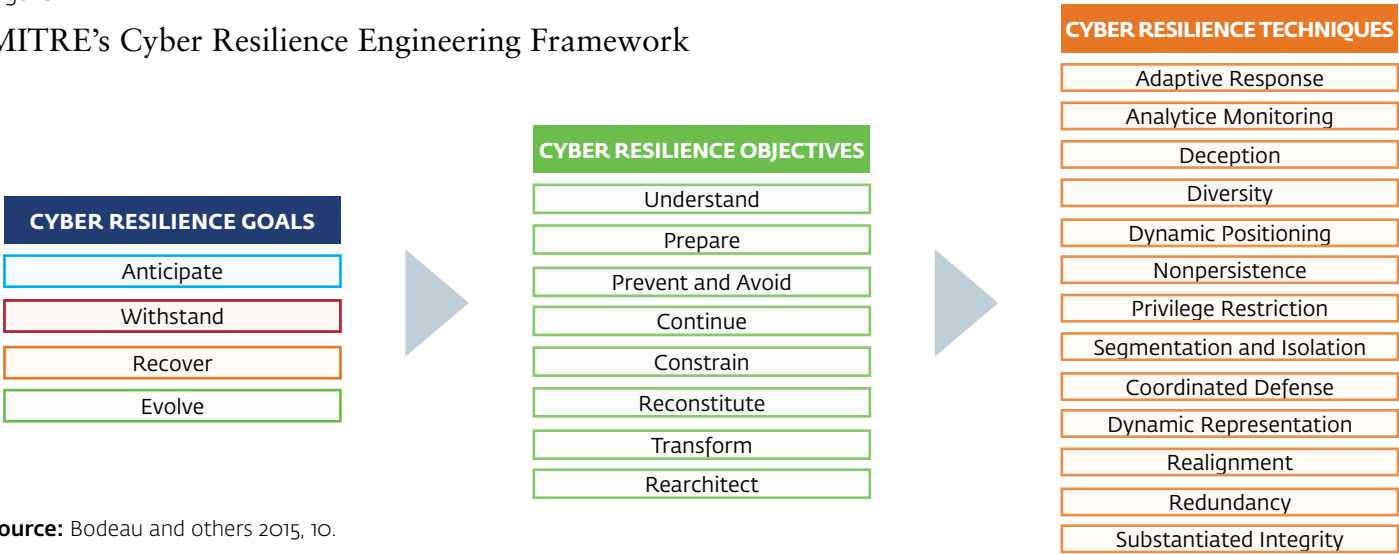
— **RENE SUMMER**
Director of Government and Policy Advocacy
Ericsson

“Collectively, these players define the security status of deployed networks and hence the de-facto end-user security experience.”

Cyber-resilience requires deliberate choices about people, processes, and technology, with a strategy that must be tested regularly and updated as threats evolve. Telecommunications operators that invest in cyber-resilience can absorb and recover from cyber incidents, rather than suffer outages and operational disruption. Adding resilience is as much an investment in mindset and business culture as it is a financial cost, a distinction that allows emerging-market operators to work within real budget and talent constraints to attain resilient operations.

Figure 1

MITRE’s Cyber Resilience Engineering Framework



Source: Bodeau and others 2015, 10.

"In the digital age, excellence is driven by proactive risk management, where threats are not just identified but deeply understood, and resources are allocated to fortify the most critical assets," said Suresh Sankaran, head of cybersecurity and data privacy for Axiata, a Malaysian multinational telecommunications conglomerate.

Resilience versus security: A critical distinction

Security and resilience are often used interchangeably, but they answer different questions. Security focuses on keeping attackers out, while resilience assumes that some attacks will invariably succeed given enough time and a determined adversary; therefore, resilience focuses instead on how to limit the damage and keep services running—or recover as quickly as possible.

For telecom operators, the distinction matters, because those failure modes are measured not in compromised records but in dropped calls, low bandwidth, and payments that stop clearing.

As shown in Figure 1, resilience rests on four foundations: operate in a state of informed preparedness (anticipate), maintain essential business functions during an attack or disruption (withstand), quickly restore critical operations (recover), and adapt security and operations to account for lessons learned (evolve). Anticipate means that telecommunication providers must promote the exchange of information with other industry players. In addition, they must withstand attacks by maintaining service availability and be ready to recover quickly. Finally, operators must analyze threat actors' efforts, evolving their strategies to prevent, detect, and respond to attacks.

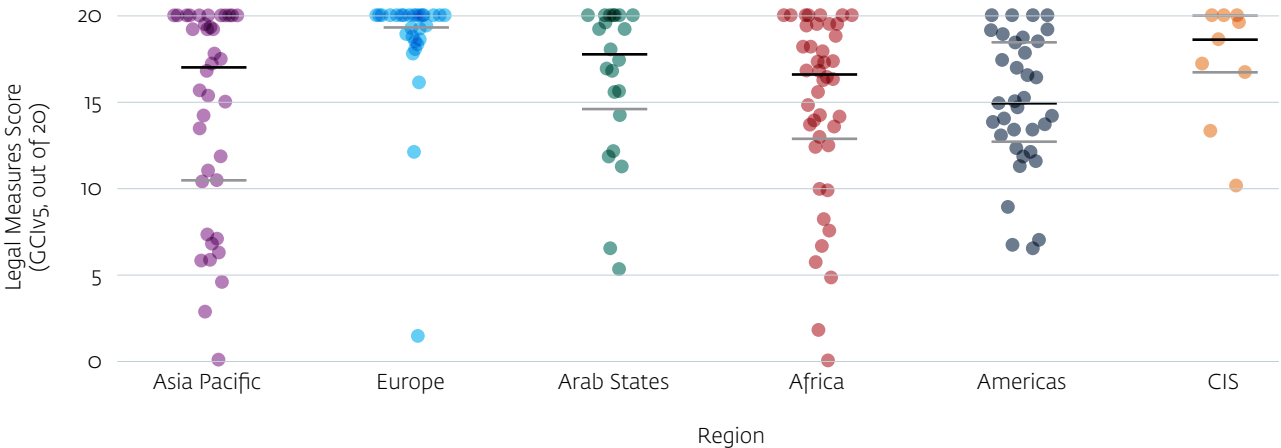
An operator with excellent perimeter defenses but no rehearsed recovery plan will still face a prolonged outage when prevention eventually fails, while strong detection is wasted if no one is empowered to respond. Mature operators invest across all four areas rather than focusing solely on prevention because cyber-resilience failures are more often due to poor execution. Resilience requires financing, and most companies (90 percent) anticipated having to make "moderate" to "high" levels of investment to be more prepared to tackle cyber incidents (Allianz 2026, 4–5).

In addition, execution requires rehearsal and practice, not just the purchase of tools and technology. While many of the factors that reduce the cost of a data breach come from tools—such as security information and event management systems and security orchestration, automation, and response tools—much of the ability to reduce these breaches come from practices such as using DevSecOps for application development, or artificial intelligence and machine learning to reduce alert fatigue. Each of these can reduce the \$4.4 million average global cost of a data breach by about 5 percent (IBM and Ponemon Institute 2025, 42–43).

Regulations and best practices make a baseline to build on

Telecom operators are not starting from zero. Years of regulatory pressure and vendor requirements have established a meaningful baseline, as most operators maintain network perimeter defenses and run vulnerability assessments and penetration tests on a regular cycle. Almost every nation, including emerging markets, has passed cybersecurity regulations or compliance measures that meet at least one international standard (Figure 2), and 177 countries

Figure 2
Regulatory Cybersecurity Measures, by Region



Source: ITU 2024a.

Note: CIS = Commonwealth of Independent States, which includes Russia and eight former Soviet states.

have established at least one regulation addressing data protection, data privacy, or breach notification as of 2024 (ITU 2024a).

However, industry research consistently shows that these strengths are concentrated in a narrow set of areas. Operators tend to be strongest precisely where external pressure demands it: compliance audits, vendor security requirements, network security, and telecom protocols and signaling security are generally well-covered by national legislation in most regions, with a few countries in Africa and the Asia-Pacific lagging behind. Yet, IFC research has found that capability usually falls sharply when external pressure is absent (Note 2).

Telecom operators in emerging markets need to create blueprints identifying and reinforcing weaker areas, such as cyber visibility, product security, and software development life cycles. For example, Global System for Mobile Communications Association’s (GSMA) FS.31 provides baseline security controls for mobile network operators, including a structured checklist of security measures across network domains, signaling, infrastructure, and operational practices to help operators assess and improve their security posture (GSMA 2025).

Creating a core playbook for security and resilience

To develop deep resilience, telecom operators need to focus on strengthening security controls, boosting visibility, and creating a

metrics-based strategy. For example, Safaricom committed to, and then brought a security operations center (SOC) online, reducing security incidents for enterprise customers by nearly 90 percent and showing the value of following the right resilience playbook. The company’s chief corporate security officer positioned the strategy as a shift to a zero-trust architecture that would mitigate damage in the case of a compromise (Ndege 2025).

In a survey of dozens of telecom operators in emerging and developed markets, IFC found that building the right kind of capability requires developing a playbook encompassing 14 domains (table 1). Each domain requires individual attention, but all are interdependent, meaning that a weakness in any one undermines the others. Table 1 includes 13 domains with the cyber-visibility and security operations center (SOC) domains combined.

These domains extend beyond just the operators’ own networks to ensuring the security of the cloud services and suppliers that they use.

“It is crucial to have a comprehensive understanding of the security risks introduced by third parties and suppliers, particularly during milestone-based deployments,” said Eric Maes, head of security architecture and solutions at Nokia Group Security. “Ensuring supplier availability is a part of maintaining the integrity of a supplier’s commitments.”

Table 1
Domains for Cyber Defense and Resilience

DOMAIN	DESCRIPTION	BEST PRACTICES
 Cybersecurity strategy and budgeting — 56 % adoption	The overall cybersecurity strategy guides the organization’s effort and helps determine budget priorities. The strategy must be aligned with business objectives and regulatory requirements, with clear roles and strategic oversight within a dedicated cybersecurity team . It also needs to consider the risks facing the business, the maturity level of the operator’s infrastructure and workforce, and the budget available. Baseline practices include the use of risk registers and adherence to relevant regulations and benchmarks .	<ul style="list-style-type: none">• Cybersecurity awareness and workforce development: Provide role-based cybersecurity training, phishing awareness, technical upskilling, and executive tabletop exercises to strengthen organizational resilience.• Invest in updating legacy equipment: To reduce the risks associated with aging and unsupported technology, operators should identify older equipment that is difficult to maintain or nearing end of life and assess whether it is still need or should be updated or replaced.

DOMAIN	DESCRIPTION	BEST PRACTICES
 <p>Vulnerability management and security assessments — 56 % adoption</p>	<p>A proactive approach to security requires that operators conduct regular—even continuous—security assessments, vulnerability discovery, and penetration tests. Combined with asset discovery, these measures allow telecom operators to focus on managing their attack surface area and reducing vulnerabilities in critical assets. Baseline practices include combining manual and automated processes to remedy vulnerabilities and prioritizing remediation based on risk and criticality.</p>	<ul style="list-style-type: none"> • Vulnerability and patch management: Conduct regular vulnerability scanning, prioritize remediation based on risk, and establish patch management processes for critical assets. • Threat intelligence utilization: Use adversary intelligence and vulnerability analysis to proactively identify weak points and threats. • Incident response and business continuity planning: Develop, test, and maintain cyber incident response plans, disaster recovery procedures, backup strategies, and crisis communications processes.
 <p>Data privacy — 52 % adoption</p>	<p>Telecom operators play a significant role as custodians of their customers' sensitive data. Protecting the information requires identifying and consolidating data stores, determining the required data-protection regulations, and automating monitoring. Baseline practices include classifying data sensitivity and collection severity and frequent training on applicable regulations to ensure proper handling of data.</p>	<ul style="list-style-type: none"> • Implement security controls based on data sensitivity: Encryption, role-based access controls (RBAC), and audit trails should be applied more rigorously with greater sensitivity. • Minimization of sensitive data collection: Companies should collect only the data they need to minimize the impact of a data breach.
 <p>Compliance management — 69 % adoption</p>	<p>Data-protection regulations, critical-infrastructure protection requirements, and other regulations need to be followed and documented. Operators need a compliance management process that tracks requirements and delivers insight into the organization's status. Baseline practices include the collection of clear metrics to fuel continuous improvement and reporting that provides visibility into compliance failures and policy violations.</p>	<ul style="list-style-type: none"> • Comprehensive compliance management process: The organization systematically tracks and reports on compliance with independent reviews with a focus on continuous improvement. • Identity and access management: Implement multifactor authentication, least privilege access, privileged account management, and periodic access reviews.
 <p>Product security — Only 36 % adoption</p>	<p>Telecom products typically had lifetimes measured in decades, with few update mechanisms. With their reliance on information and operational technology, the situation has changed, with faster update cycles, remote management and monitoring, and on-board security. Baseline practices include routine security audits to identify and promptly address product vulnerabilities and adhering to industry specifications and protocols for product development to ensure robust secure configurations.</p>	<ul style="list-style-type: none"> • Secure-by-design: Security should start during product design with regular testing throughout the product life cycle. Secure-by-design is increasingly required by government regulations. • Integrate security into DevOps: Embedding security practices into the development-operations pipeline improves product security and reduces time to remediate vulnerabilities. • Collaborate on vulnerability disclosure: Work with security research groups and original equipment manufacturers to proactively identify and mitigate potential security flaws.

It is crucial to have a comprehensive understanding of the security risks introduced by third parties and suppliers, particularly during milestone-based deployments.

— **ERIC MAES**
Head of Security Architecture and Solutions
Nokia Group Security

DOMAIN	DESCRIPTION	BEST PRACTICES
 <p>Risk management — 56 % adoption</p>	<p>A strong risk-management program is critical to building a resilient business. Telecom operators should look to adopt a risk management framework, such as the National Institute of Standards and Technology's Risk Management Framework or the International Standards Organization's (ISO) 31000 risk management guidelines (CSRC 2026; ISO 2018). Baseline practices include planning for disaster recovery, conducting manual risk assessments, and adopting a system to regularly analyze risks to critical assets. In addition, the organization should determine and define its enterprise risk appetite.</p>	<ul style="list-style-type: none"> • Cybersecurity governance framework: Establish cybersecurity policies, standards, roles, responsibilities, and executive oversight aligned with business objectives and risk appetite. • Risk quantification: Utilize risk quantification techniques to prioritize mitigation strategies and allocate resources to the most critical vulnerabilities.
 <p>Cyber visibility and security operations — Only 27 % adoption</p>	<p>An operator cannot protect what it does not know exists. In practice, many operators—particularly those running mixed legacy and modern environments—have equipment that was deployed, never fully documented, and never patched. Companies need visibility into the state of their assets and the ability to respond to incidents. Baseline practices include automation of processes and dashboard creation for asset monitoring, detailed tracking with a configuration management database, and the use of security information and event management (SIEM) tools to monitor security status and events.</p>	<ul style="list-style-type: none"> • Hardware- and software-asset inventory: Maintain an up-to-date inventory of all network, information technology, cloud, and operational technology assets, including ownership, location, and life cycle status. • Continuous asset and configuration monitoring: Track both sanctioned and unsanctioned hardware and software to identify vulnerabilities and misconfiguration using CMDB capabilities for continuous visibility. • Threat detection and monitoring: Deploy SIEM tools to monitor network activity, identify anomalies, and generate alerts for potential security incidents.
 <p>Supplier security — Only 31 % adoption</p>	<p>Telecom operators must manage not only their own security but that of their third-party suppliers and vendors. A supplier-security program begins with contract requirements and due diligence and requires regular monitoring of supplier compliance and access to the organizations' resources. Baseline practices include RBAC for supplier access and strict contracts and service level agreements that define security responsibilities and protocols for all third parties.</p>	<ul style="list-style-type: none"> • Third-party and supply chain security: Establish minimum cybersecurity requirements for vendors, conduct security due diligence, incorporate security obligations into contracts, and periodically assess risk of critical suppliers. • Vendor access controls: Implement RBAC and infrastructure segmentation to limit supplier access to only what is necessary for their specific functions. • Automated vendor risk assessment: Use automation tools for vendor risk assessment and qualification processes to proactively identify and mitigate potential vulnerabilities in the supply chain.
 <p>Cyber-resilience — Only 39 % adoption</p>	<p>Companies frequently build strong threat-detection capabilities but fail to plan for the worst-case scenario. Cyber-resilience requires that telecom operators have both a documented playbook and frequent testing and rehearsals across relevant teams, such as network operations, legal, communications, and executives. The goal is not just to have a plan but to be able to execute quickly under pressure. Baseline practices include comprehensive enterprise incident response plans and an operationally focused cyber-resilience strategy that prioritizes critical services.</p>	<ul style="list-style-type: none"> • Incident response planning: Develop, maintain, and regularly test enterprise incident response plans with documented procedures, defined roles, and clear escalation paths. • Business continuity and recovery: Implement an operationally centered cyber-resilience strategy that prioritizes critical services, with tested disaster recovery procedures and backup strategies. • Crisis simulation exercises: Conduct regular tabletop exercises and cyberattack simulations led by senior management to evaluate organizational readiness and update response playbooks.

DOMAIN	DESCRIPTION	BEST PRACTICES
 <p>Cloud security — Only 33 % adoption</p>	<p>A variety of cloud-security technologies exist to help companies monitor and manage their hosted instances and services. Cloud security posture management (CSPM) continuously assesses an organization's public and private cloud services to evaluate and manage risks. Cloud workload protection platforms (CWPPs) manage the security of workloads used in cloud instances, while cloud access security brokers (CASBs) help companies manage employees' connections to public cloud services. Baseline practices include adopting security solutions for comprehensive cloud security compliance, monitoring, and robust access management.</p>	<ul style="list-style-type: none"> • Cloud security posture management: CSPM continuously evaluates public and private cloud environments to identify misconfigurations, policy violations, and compliance gaps. • Cloud access security broker: Deploy CASB solutions to enhance visibility, control data flow, manage employee access to cloud services, and support cloud governance. • Cloud workload protection: Implement CWPP solutions to secure workloads across physical servers, virtual machines, containers, and serverless functions.
 <p>Network security — 42 % adoption</p>	<p>The traditional perimeter model—trust everything inside, block everything outside— fails against an attacker who has already compromised a contractor account or an unmanaged device. Network segmentation and zero-trust architecture help limit the damage (commonly called the "blast radius") from an attack that gets past the perimeter. Baseline practices include rigorous network segmentation and access permissions based on need and subject to regular reviews, and regular third-party assessments and continuous scanning during network changes.</p>	<ul style="list-style-type: none"> • Network segmentation and zero-trust principles: Separate business systems, operational technology, core telecom infrastructure, and customer-facing services to reduce lateral movement during incidents. • Regular security assessments: Conduct regular third-party assessments and continuous scanning during network changes, with access permissions based on need and subject to regular reviews. • Advanced network monitoring: Deploy deep packet inspection tools for detailed traffic analysis and swift response to threats.
 <p>Secure software development and DevSecOps — 44 % adoption</p>	<p>Software is a critical part of telecommunications infrastructure, but also a major source of vulnerability. Operators need to focus on securing the development-to-operations pipeline using a framework such as DevSecOps, which fosters collaboration between development, security, and operations teams. Baseline practices include periodic security testing—including static and dynamic application security testing (SAST/ DAST)—for developed applications, and active management of open-source and third-party software to reduce inherent vulnerabilities.</p>	<ul style="list-style-type: none"> • Secure development life cycle: Test and confirm security throughout the development and operations pipeline. • Static and dynamic application security testing: Conduct regular SAST/DAST testing to identify and remediate vulnerabilities before deployment. • Open-source and third-party software management: Maintain a software bill of materials, monitor for vulnerabilities in dependencies, and apply centralized patch management.
 <p>Telecom protocol and signaling security — 60 % adoption</p>	<p>Unlike other enterprises and organizations, telecom operators have two networks: business and service. Telecom security focuses on securing the network services delivered to customers and includes mobile networks, signaling services, operational technology, and the applications needed to manage the infrastructure. Baseline practices include service-based security assessments against voice, data, and Short Message Service (SMS) services, and a security toll-gating process aligned with unified compliance frameworks and regional and global security practices.</p>	<ul style="list-style-type: none"> • Implement best practices for telecom security: Mobile telecom networks can use Global System for Mobile Communications Association (GSMA) FS.31 for baseline security controls and its checklist of security measures (GSMA 2025). • Service-based security assessments: Conduct regular security assessments against voice, data, and SMS services to identify protocol vulnerabilities and signaling weaknesses. • Fraud prevention based on artificial intelligence (AI) and machine learning (ML): Use AI or ML tools and SMS spam filters to detect and block fraudulent messages across interconnect and roaming interfaces.

Organizational and governance discipline

Technical controls are necessary but not sufficient. Every capability described in the preceding sections depends on an organizational structure in which cybersecurity decisions carry real authority and accountability.



Governance

The starting point is governance. A chief information security officer with direct board-level reporting establishes that cyber risk is treated as an enterprise risk, not a technical problem delegated to the information technology department. Operators that have made this shift tend to show it in how they manage their risk registers, capital planning, and crisis response.

Take responsibility for risk management at the executive level and regularly review policy and progress.



Due diligence and compliance

Operators that vet vendors before onboarding, establish service-level agreements that define security responsibilities and incident notification timelines, and continuously monitor third-party access are materially better positioned than those that rely on periodic audits and goodwill. A significant share of major telecom breaches in recent years have come through third-party access that was not adequately governed.

Require cybersecurity language in third-party contracts and regularly monitor compliance.



Training

A network engineer, a billing system administrator, and a customer service agent face different threat surfaces and need different skills, making generic annual awareness training insufficient. Instead, training will produce better outcomes when it is tailored to each role and the actual threats each function is likely to encounter.

Train employees regularly to face the current threats to telecom networks and customers.



Practice

Tabletop exercises and full incident simulations reveal the coordination failures—the unclear escalation paths, undefined decision authorities, and legal and communications tensions—before an attacker does. Operators that have already worked through those problems recover faster when a real incident occurs.

Conduct tabletop exercises and regular incident and recovery simulations to ensure the organization is ready when it matters.

Leading operators also measure cybersecurity performance through objective metrics, such as vulnerability remediation timelines, asset inventory coverage, incident response effectiveness, phishing resilience, and third-party risk reduction, enabling management to track progress and prioritize investments.

Cyber insurance: Complementary, not a substitute

Awareness of cyber insurance as a financial risk management tool has grown sharply across the telecom sector, driven in part by the scale of incidents affecting major operators in recent years. The ransomware attack on Telecom Namibia in late 2024 and the

data breach disclosed by MTN Group in April 2025 turned what many corporate boards had viewed as a theoretical risk into a tangible concern and accelerated conversations about how to transfer at least part of that financial exposure (Arghire 2025; Lemos 2025).

Insurers have responded to growing demand by raising the bar for coverage. Evidence of baseline security controls, such as

documented practices in identity management, incident response, and vulnerability management, is increasingly required to obtain a policy. In addition, bolstering cybersecurity and cyber resilience leads to lower premiums for the policyholder. For operators with weaker programs, this creates a direct financial incentive to improve, because the coverage needed to manage tail risk depends on investments that reduce it.

However, the market presents real challenges in emerging economies. Risk quantification requires exposure data that are not available in many African and Latin American telecom markets, especially those without strong data protection standards. Telecom operators are strongly recommended that they have cyber insurance whose policy terms can be tailored to the operator's needs so that the coverage is appropriate fitting the company's risk exposure. Standard, off-the-shelf, products may not be suited to each entity's specific coverage needs. Despite significant claims activity, cyber insurance premiums are still trending downwards with Quarter 1 globally showing a decrease of 5% (Marsh Global Insurance Index). This should allow well-informed insureds to broaden coverage or enhance the insurance limits.

Finally, cyber insurance helps mitigate risk, but does not necessarily improve cyber resilience. Insurance transfers financial risk after an incident; it does not reduce the underlying vulnerability that made the incident possible. Operators that treat cyber insurance as a substitute for building resilience will find, when a serious incident occurs, that the payout does not compensate for the operational damage, reputational loss, or service disruption their customers experience. Cyber insurance, however, offers a valuable element of crisis response handling by integrating active security and crisis management to minimize financial loss and downtime during a cyberattack. Many policies offer 24/7 hotlines, IT forensics, and crisis communication to assist the insured's cyber teams.

Emerging-market priorities: Resilience under constraint

For telecom operators in emerging markets, developing more cyber resilience can be a tall order. The technical capabilities outlined in the preceding section assume resources that many operators do not have in abundance. Still, an intelligent, targeted approach to cybersecurity can improve an organization's cyber resilience, even under resource constraints.

Wrap controls around legacy infrastructure: The most persistent constraint is legacy infrastructure. Most emerging-

market operators run network equipment and operational systems that were never designed with modern security in mind. Replacing that infrastructure takes years and significant capital. The interim approach is to wrap security controls around these systems by adding monitoring, segmenting them from more sensitive network functions, and patching where possible, while modernization proceeds in parallel.

Outsource security where skilled workers are scarce: The shortage of cybersecurity professionals is a global problem, but it is acute across sub-Saharan Africa and parts of Latin America, where experienced analysts are few and competition from better-resourced sectors is intense. For operators that cannot build fully staffed in-house capability, managed security service providers (MSSPs) offer a practical path to 24/7 detection and response without the full cost of an internal SOC. While visibility and control are partially outsourced, having deeply skilled professionals monitoring threats and responding to incidents can significantly help operators' security posture. Many operators begin their cybersecurity journey by leveraging MSSPs to establish foundational monitoring and incident response capabilities before gradually building internal expertise over time.

Prioritize using a cybersecurity strategy: Prioritization is essential for operators building a program from a low baseline. Not all risks carry equal probability or impact. The GSMA's FS.31 Baseline Security Controls and the National Institute of Standards and Technology's Cybersecurity Framework 2.0 both provide structured, prioritized starting points that allow operators to focus limited resources on the controls that matter most, without constructing a bespoke framework from scratch. Telecom operators should take a phased approach and first establish foundational hygiene, then build toward more sophisticated detection and response capabilities over time.

The Africa Cybersecurity Report 2024/25 documents a growing professionalization of security operations across East Africa, including operators building formal incident response capabilities and beginning to share threat intelligence with one another (Serianu 2025). The gap between leading and lagging operators is real, but for those willing to invest systematically, even incrementally, it is also closing.

Developing a strong cybersecurity program is not out of reach for telecom operators in emerging markets. These companies should first establish baseline controls, then continuously evaluate and improve their security posture. Development finance institutions and other investors can help bridge the costs of implementing better cybersecurity, as discussed in Article 5.

NEXT IN THE SERIES: ARTICLE 5 | SECURING THE ECOSYSTEM

The final article examines how regulators, industry, standards bodies, and investors can work together to strengthen cyber resilience across the telecom ecosystem.

Endnotes

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 clients, 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. A study of telecommunications firms in emerging markets was conducted by International Finance Corp. and consultancy EY in 2025.

References

- Arghire, Ionut. 2025. "African Telecom Giant MTN Group Discloses Data Breach," *SecurityWeek*, April 28, 2025. <https://www.securityweek.com/african-telecom-giant-mtn-group-discloses-data-breach/>
- Bodeau, Deborah, Richard Graubart, William Heinbockel, and Ellen Laderman. 2015. *Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. McLean, Virginia: MITRE Technical Report, September 2015. <https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-aid-updated-cyber-resiliency-engineering>
- CSRC (Computer Security Resource Center). 2026. "National Institute of Standards and Technology (NIST) Risk Management Framework." Updated February 10, 2026. <https://csrc.nist.gov/Projects/risk-management/about-rmf>
- GSMA (Global System for Mobile Communications Association). 2025. "FS.31 GSMA Baseline Security Controls Version 7.0." GSMA, December 16, 2025. https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/
- IBM and Ponemon Institute. 2025. "Cost of a Data Breach Report 2025." IBM, Armonk. <https://www.ibm.com/reports/data-breach>
- Ilascu, Ionut. 2021. "Largest Mobile SMS Routing Firm Discloses Five-Year-Long Breach." *Bleeping Computer*, October 4, 2021. <https://www.bleepingcomputer.com/news/security/largest-mobile-sms-routing-firm-discloses-five-year-long-breach/>
- ITU (International Telecommunication Union). 2024. *Global Cybersecurity Index 2024*. Geneva: ITU. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- ISO (International Standards Organization). 2018. "ISO 31000:2018 Edition 2: Risk Management — Guidelines." ISO, Geneva. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
- Lemos, Robert. 2025. "Ransomware Targeting Infrastructure Hits Telecom Namibia." *Dark Reading*, January 8, 2025. <https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia>
- National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC). 2026a. *Cybersecurity Report, 40th Edition, October – December 2025*. Communications Authority of Kenya, Nairobi. <https://www.ca.go.ke/sites/default/files/2026-01/Cyber%20Security%20Report%20Q2%202025-2026.pdf>
- National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC). 2026b. *Cybersecurity Report, 41st Edition, January – March 2026*. Communications Authority of Kenya, Nairobi. <https://www.ca.go.ke/sites/default/files/2026-04/Cyber%20Security%20Report%20Q3%202025-2026.pdf>
- Ndege, Adonijah. 2025. "Why Safaricom Is Spending \$309 Million Annually to Future-Proof M-Pesa." *TechCabal*, May 6, 2025. <https://techcabal.com/2025/05/06/safaricom-309mn-m-pesa/>
- Safaricom. 2026. "Safaricom PLC Results Booklet." Safaricom PLC, Nairobi. May 7, 2026. <https://www.safaricom.co.ke/images/Downloads/FY26-Earnings-Booklet-2026-7th-May-2026.pdf>
- Sama, Caleb. 2024. "Safaricom Blocks over 8,000 Agents Due to Fraud." *TechWeez*, December 17, 2024. <https://techweez.com/2024/10/28/safaricom-blocks-over-8000-agents-due-to-fraud/>