



From Connectivity to Critical Infrastructure: Why Cybersecurity is Now a Telecom Imperative

Telecommunications continues to be one of the most frequently targeted sectors because of its role in connecting citizens and governments, its privileged access to data, and every other business' reliance on its capabilities.

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

Critical infrastructure is under attack from financially motivated cybercriminals, political hacktivists, and nation-state cyber operators. Telecommunications providers are squarely in the crosshairs.

In September 2023, a ransomware gang struck IFX Networks, a Colombian cloud and telecommunications services provider with infrastructure across 17 Latin American countries. Yet, the attack did not just affect the company. Within hours, more than 50 government agencies had lost access to essential systems, the national judicial system suspended most court proceedings, and the Ministry of Health lost access to key databases and applications required to serve citizens (Grieg 2023).

The incident underscored the central role that telecommunications and network service providers have come to play in nearly every nation's economy. Like other facets of the digital supply chain, a wide array of businesses, industries, and government services rely on telecom providers' resilience. Communications networks are especially vital in emerging markets, where mobile connectivity often substitutes entirely for fixed infrastructure. Mobile money platforms, e-government services, emergency dispatch, and supply chains all route through mobile, wireless, and fixed telecom networks, making any disruption an economic and public-safety event for the nation.

Cyberattackers understand this and have escalated their operations accordingly. Telecommunications providers have ranked as the third most targeted industry for each of the past two years (Vedere Labs 2026). In a study conducted by IFC, 63 percent of telecom operators ranked ransomware and malware as high-priority threats (Note 2). Overall, at least 90 telecommunications firms, including IFX Networks, suffered major, reportable ransomware attacks in 2025, a four-fold increase in three years (Geller 2026).

Telecom operators are high-value targets

Cyberthreat actors see an opportunity: the connectivity and data managed by telecommunications firms can help them gain intelligence on—and access to—other businesses and public-sector activities. Operators are conduits for uniquely sensitive data, such as call records, financial transactions, subscriber locations, and government communications. They also occupy a dual role as commercial operators and critical infrastructure providers, providing internet connectivity and payment capabilities for many citizens in numerous emerging markets.

Mobile telecommunications have become a necessity in emerging markets, not just for communications but as a foundation of the economy. In Africa, for example, fixed-broadband household penetration is only 17 percent, while mobile penetration is 1.01 subscriptions per person on average, according to data from Telegeography (Note 3). Mobile financial services and mobile money platforms often substitute entirely for banking branches, which means telecom outages are instantly felt by the unbanked and underbanked populations.

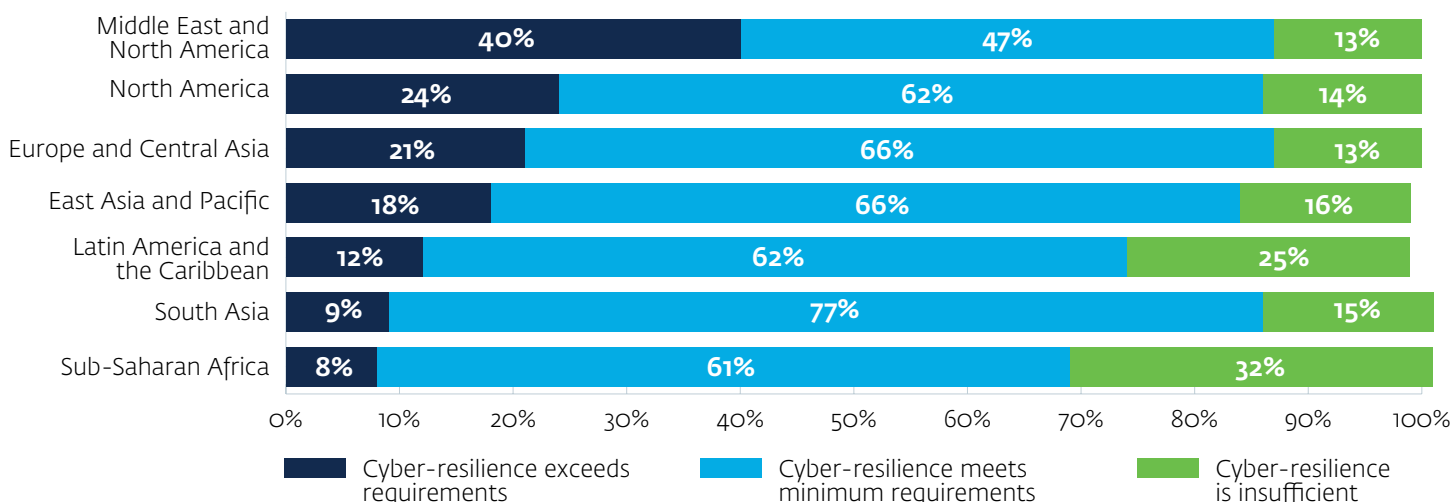
Meanwhile, organizations in many emerging markets continue to lag behind in building cyber-resilient networks capable of not only withstanding cyberattacks but recovering quickly after a successful attack. *Organizations in both Latin America and Sub-Saharan Africa report the region's most severe cybersecurity talent gaps, with 65% and 63%, respectively, say they lack critical people and skills, while only 8% of Sub-Saharan African organizations rate their cyber resilience as exceeding requirements, compared to 19% globally. (WEF and Accenture 2026, pp. 34, 49, 51).*

“As artificial intelligence becomes increasingly integral to cybersecurity, the industry must prioritize securing AI systems while harnessing AI-based defense capabilities to fortify our digital systems against an expanding threat landscape.”

— **SAMANTHA KIGHT**
Head of Industry Security
Global System for Mobile Communications Association
(GSMA)

Figure 1

Organizations in Emerging Markets Feel Unprepared for Cyberthreats



Source: WEF and Accenture 2026, 40.

Given the importance of telecommunications infrastructure, the rise in attacks comes as no surprise to industry watchers. “This high volume of attacks shows the sector’s appeal to cybercriminals, which is likely due to factors such as its critical infrastructure role, ease of espionage once compromised, and the vast amounts of sensitive data it manages,” stated cybersecurity firm Cyble in its *Telecommunication Sector Threat Landscape Report 2025* (Cyble 2026).

The World Economic Forum’s *Global Cybersecurity Outlook 2025* found that emerging markets had concerns about their cyber resilience, with 25 percent of respondents in Latin America and 32 percent in Sub-Saharan Africa lacking confidence in their preparedness. Other regions had greater confidence: in North America, 24 percent of respondents said their cyber-resilience exceeded their requirements, while 40 percent in the Middle East and North Africa also believed they surpassed cyber-resilience requirements (WEF and Accenture 2026, 49).

Crucially, the research suggests that a lack of resilience is not due to a lack of awareness. Companies identified cyber incidents as a top business-related risk for the fifth year in a row, while business interruption is the third most significant risk, highlighting that organizations are aware of the threats (Allianz 2026).

Five structural vulnerabilities need protection

A telecommunications provider’s dual role as a commercial operator and critical infrastructure provider creates unique exposures that appeal to different attackers. A cybercriminal may target the operator for financial gain, while a nation-state actor could compromise the network to gain access to its customers and government systems. Depending on the goal, cyberattackers use a broad array of tactics, including distributed denial-of-service (DDoS) attacks to shut down connections, credential-based attacks to compromise privileged accounts, exploitation of unpatched software flaws, and AI-powered social engineering to lure users into running code or giving up sensitive information.

Telecom operations need to assess the most critical aspects of their businesses and identify any weaknesses that could allow threat actors to compromise their systems and operations. As they adopt artificial intelligence, the technology will both be an amplifier of attackers’ operations and defenders’ capabilities to react to compromises more quickly.

“As artificial intelligence becomes increasingly integral to cybersecurity, the industry must prioritize securing AI systems while harnessing AI-based defense capabilities to fortify our digital systems against an expanding threat landscape,” said Samantha Kight, the head of industry security at the Global System for Mobile Communications Association (GSMA).

Cyberattacks typically target five main structural vulnerabilities that pose a risk to telecommunications network providers:



Critical connectivity

A variety of individuals and organizations—from government agencies to companies to citizens—rely on the network connectivity provided by telecoms companies. Network intrusions, such as DDoS attacks, can co-opt functionality for malicious purposes or deny legitimate customers and clients' access to services.



Sensitivity of custodial data

Telecoms networks transmit highly sensitive data—call detail records, Internet Protocol detail records, financial transactions, real-time subscriber location, and government communications—making them targets of interest for criminal, commercial, and state actors. The volume and sensitivity of data operators hold—such as location, financial, and identity—makes them a consistently high-value target for data extortion or sale on the dark web.



Supply chain dependencies

Third-party vendor relationships and software dependencies create entry points that are difficult to monitor and control. Telecommunications firms are at the nexus of these relationships: gaining access could give cyberattackers an easier path into customer networks, while exploiting weaknesses in third-party service providers could expose multiple telecom clients.



An expanding attack surface

A variety of technology choices, such as backward compatibility for 5G devices—cloud-native architectures, network application programming interfaces, edge deployments, Internet of Things integrations, and AI-enabled services—are each expanding the perimeter that network operators must defend. Attacks can vary widely in the weaknesses they target, from exploits for software vulnerabilities in edge devices to increasingly convincing AI-powered phishing attacks. In addition, telecoms operators are modernizing their infrastructure while continuing to provide critical services, creating hybrid environments that are difficult to secure.



Deep network interconnection

No matter the motivation, the impact on the telecommunications network, businesses, and government services can be severe. Telecom networks are highly interconnected through extensive interconnections among operators globally. As a result, vulnerabilities in one network can propagate across systems, creating a domino effect on dependent services. Threat actors can exploit the weakest link in this interconnected ecosystem to gain access and potentially impact multiple networks.

A 2023 cyberattack on Ukraine's largest telecommunication provider, Kyivstar, left 24 million subscribers without voice or data connectivity for two days and cost its parent company, Netherlands-based Veon, nearly US\$100 million (Antoniuk 2024). In March 2024, the severing of an undersea cable disrupted Internet traffic across West Africa, with bandwidth falling by more than 50 percent in affected countries. This halted financial transactions and made some cloud services inaccessible, underscoring the impact of telecom disruption to modern economies (Adegboyega 2026).

The signaling protocols that enable global mobile connectivity—in particular, Signaling System 7 (SS7) for legacy networks—were designed for a closed ecosystem of trusted partners, with minimal authentication requirements that made sense decades ago but are now a serious liability. Today, those same protocols underpin

the roaming agreements and shared infrastructure that tie together hundreds of operators worldwide, meaning a vulnerability in a poorly secured carrier in one country can serve as a steppingstone into networks on the other side of the world. For operators in emerging markets, where security investment and regulatory oversight may lag behind more developed peers, that interdependency cuts both ways: their networks can be targeted through a trusted foreign partner, and they can inadvertently become the weak link through which adversaries reach larger, higher-value systems.

"[A] robust digitalization plan is critical to increase efficiency, accuracy, and alignment [in] managing a larger footprint of sites," said Domingos Savio Vieira De Almeida, vice president of group technology and operations at EdgePoint Infrastructure, a Kuala Lumpur-based telecommunications provider.

The threat will only grow

Emerging economies are rapidly digitizing, and telecommunications firms are focused on rolling out more advanced technologies, such as combining 5G connectivity, Open Radio Access Network architecture, and AI management for smarter, more efficient, and more robust communications. In addition, digital transformation and network virtualization are accelerating as operators seek cost efficiencies, introducing new vulnerability classes alongside efficiency gains.

Each new revenue stream—such as mobile banking, smart-city services, and streaming content—adds another potential entry point for attackers. With a larger technological footprint comes a greater attack surface. For example, the next generation 5G technology has already become the dominant mobile infrastructure in urban areas, providing bandwidth coverage to 55 percent of the world's population. At the same time, it comes with a new set of components, protocols, and potential weaknesses.

"Compared to its predecessors, 5G networks boast a wider attack surface due to the increased number of connected devices and the denser network infrastructure," said Kight in a 2023 column (Kight 2023). "Additionally, its reliance on cloud, virtualization, and software-defined networking introduces new avenues for exploitation."

While 5G also comes with better security capabilities, and network operators have generally improved their baseline security, attackers have become more sophisticated as well. AI is a major contributor to that trend. In March 2026, cybersecurity researchers discovered a cyber-threat group's playbook—coded as an AI prompt—that was used to compromise government agencies in Mexico by turning major AI systems into vulnerability-finding partners (Lemos 2026).

"[T]here has been a progressive lowering of [the] skill and resource levels required to launch effective attacks, establishing a relatively low barrier to the use of security attack tools," the GSMA stated in its *GSMA Mobile Telecommunications Security Landscape 2026* report (GSMA 2026, 6).

Costs and call to action

For telecommunications firms, cybersecurity is no longer just an information technology issue; it has become a core business and national-security risk. On the business side, data breaches are expensive. In 2025, the average cost of a single data breach was US\$4.4 million in 2025 (Ponemon Institute 2025, 10–11). Although

the cost can be much less in emerging markets—\$1.2 million in Brazil and \$2.4 million in South Africa, for example—other attacks, such as ransomware, come with a risk of halting operations, a much more significant argument for investing in cybersecurity.

Nations face serious harms as well. Telecom operators serve as the communications infrastructure for governments and national economies. In May 2023, evidence came to light that a series of state-linked cyberattacks captured communications and intelligence from eight ministries of the Kenyan government (Ross, Pearson, and Bing 2023). Later the same year, a different state-linked actor disrupted Ukrainian telecom operator Kyivstar, disconnecting 24 million users for days (Hunder, Landay, and Bern 2023).

Yet, the return on investment for cybersecurity is hard to quantify because it is measured against estimated, prevented future losses, which are probabilistic and easy to ignore. As a result, companies often defer investment rather than risk hobbling growth.

In the end, the cybersecurity gap in the sector is caused not by a lack of awareness but a failure to adequately prioritize and invest in security. Research consistently shows that operators have baseline compliance programs in place but have not progressed to leading practices. In IFC's 2025 study, for example, 83 percent of telecom operators have baseline cyber visibility, but only 27 percent have advanced to "leading" status (Note 2). The challenge is making the case for investment in risk reduction rather than minimum compliance. Only 24 percent of companies are prioritizing proactive cybersecurity measures rather than spending equally on reactive and proactive measures, according to a PWC 2025 survey.

Corporate boards and executives need direct visibility into cyber posture, not only compliance status. Currently, 90 percent of companies do not have a cybersecurity program mature enough to counter AI-augmented cyberthreats, and almost 67 percent lack both the strategy and the capability to combat cyberthreats, leaving them in the "Exposed Zone," according to Dal Cin, Kendzior and Seedat 2025.

Improving resilience requires telecom organizations to invest in proactive controls to strengthen their networks and operations, such as the 18 critical security controls espoused by the Center for Internet Security (CIS 2024), or the National Institute of Standards and Technology's Cybersecurity Framework (NIST 2024).

The transition from reactive to proactive security will define the decade ahead, and operators that act now will be far better positioned than those who wait for a crisis.

NEXT IN THE SERIES: ARTICLE 2 | THE EXPANDING THREAT LANDSCAPE

The next article examines the evolving cyberthreat landscape, including the actors targeting telecom networks, the tactics they use, and the growing role of AI in cyberattacks.

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 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. A study of telecommunications firms in emerging markets was conducted by International Finance Corp. and consultancy EY in 2025.
3. Telegeography Globalcomms Database

References

- Adegboyega, Ayodeji. 2026. "Cable Failures Expose Weak Links in West Africa's \$150 Billion Digital Economy." *Business Insider Africa*. April 21, 2026. <https://africa.businessinsider.com/local/markets/africa-internet-outage-exposes-dollar150bn-digital-economy-risk/wohpgg>
- Allianz. 2026. *Allianz Risk Barometer 2026: Identifying the Major Business Risks for 2026*. Allianz, Munich. <https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
- Antoniuk, Daryna. 2024. "Cyberattack on Ukraine's Largest Telecom Provider Will Cost It About \$100 Million." *The Record*. January 18, 2024. <https://therecord.media/kyivstar-cyberattack-costs-100-million-waived-fees>
- CIS (Center for Internet Security). 2024. "CIS Critical Security Controls Version 8.1." CIS, June 25, 2024. <https://www.cisecurity.org/controls/v8-1>
- Cyble. 2026. *Telecommunications Sector Threat Landscape Report 2025*. Cyble, Cupertino. <https://cyble.com/resources/research-reports/telecommunications-sector-threat-landscape-report-2025/>
- Dal Cin, Paolo, Daniel Kendzior and Yusof Seedat. 2025. "State of Cybersecurity Resilience 2025." Accenture. June 25, 2025. <https://www.accenture.com/us-en/insights/security/state-cybersecurity-2025>
- Geller, Eric. 2026. "Telecom Sector Sees Steady Rise in Ransomware Attacks." *Cybersecurity Dive*. January 9, 2026. <https://www.cybersecuritydive.com/news/telecom-ransomware-spike-cyble/809224/>
- 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). 2026. *GSMA Mobile Telecommunications Security Landscape 2026*. (GSMA, London). <https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2026/>
- Hunder, Max, Jonathan Landay and Stefaniia Bern. 2023. "Ukraine's Top Mobile Operator Hit by Biggest Cyberattack of War." *Reuters*. December 12, 2023. <https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/>
- IBM (International Business Machines Corporation) and Ponemon Institute. 2025. *Cost of a Data Breach Report 2025*. IBM, Armonk. <https://www.ibm.com/reports/data-breach>
- Kight, Samantha. 2023. "Safeguarding the Future: Managing 5G Security Risks." GSMA blog. October 3, 2023. <https://www.pwc.in/assets/pdfs/new-world-new-rules-cybersecurity-era-uncertainty.pdf>
- Lemos, Robert. 2026. "Cyberattack on Mexico's Gov't Agencies Highlight AI Threat." *Dark Reading*. March 6, 2026. <https://www.darkreading.com/application-security/cyberattack-mexico-government-ai-threat>
- NIST (National Institute of Standards and Technology). "NIST Cybersecurity Framework." NIST. February 26, 2024. <https://www.nist.gov/cyberframework>
- PwC Research. 2025. "New World, New Rules: Cybersecurity in an Era of Uncertainty." PricewaterhouseCoopers. October 1, 2025. <https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/global-digital-trust-insights.html>
- Ross, Aaron, James Pearson and Christopher Bing. 2023. "Exclusive: Chinese Hackers Attacked Kenyan Government as Debt Strains Grew." *Reuters*, May 24, 2023. <https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/>
- Vedere Labs (Forescout Research – Vedere Labs). 2026. "2025 Threat Report: Exploitation Grows Across IT, IoT, and OT." Forescout. January 29, 2026.