



Breaking Through Barriers: Cybersecurity Challenges Facing Telecom Operators *in* Emerging Markets

From aging networks to geopolitical supply chain pressures, telecom operators in emerging markets face a compounding set of structural barriers to effective cybersecurity.

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

Telecom operators worldwide are facing continued structural obstacles to effective cybersecurity implementation. Most organizations face tight budgets that restrict cybersecurity spending, workers and executives who lack security training, and new regulations with which they must comply. Telecom operators often face steeper resistance.

“The telecom industry often faces four key challenges: a lack of cybersecurity awareness, difficulty in justifying security spending, a shortage of security professionals in some regions, and rising geopolitical tensions around what is a sensitive and critical industry,” says Roi Yarom, the associate director of cybersecurity at the European Bank for Reconstruction and Development. As cyberattacks targeting the industry increase, network and telecommunications providers in emerging markets are struggling to defend themselves and make their businesses more cyber-resilient.

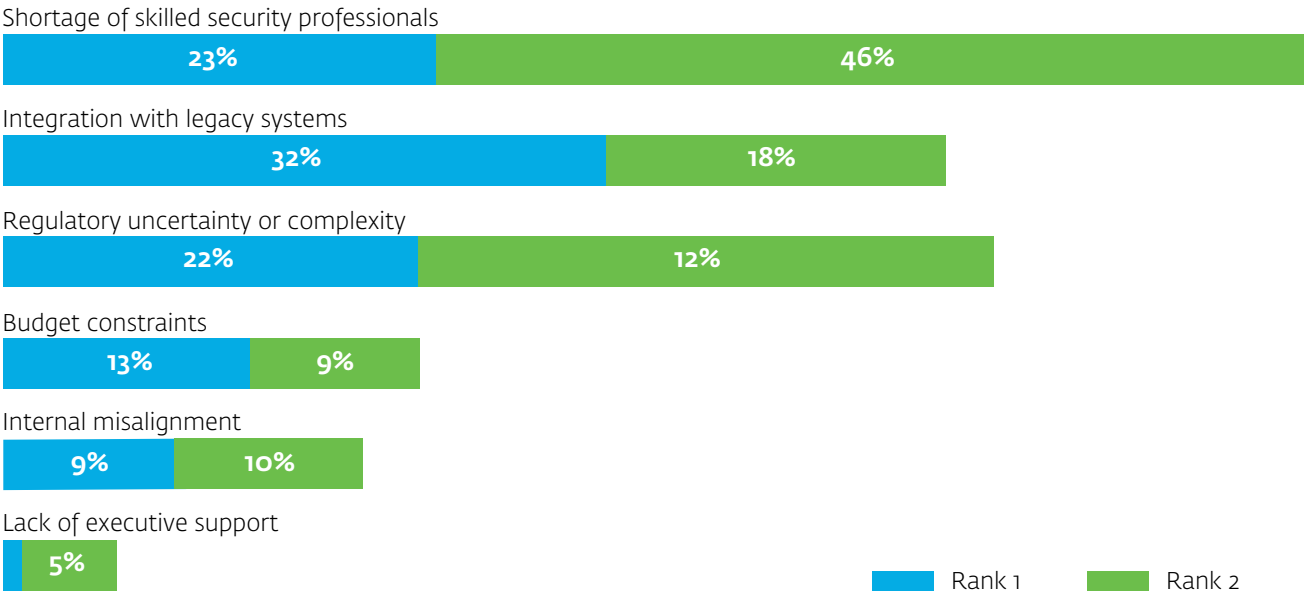
In June 2024, Indonesia’s Temporary National Data Centre, operated by a subsidiary of the state-owned telecommunications firm PT Telkom Indonesia, suffered a ransomware attack that compromised over 210 governmental agencies and disrupted 282 public services (Azhar 2024). It took five days to regain some access to the National Data Centre’s database and five months to recover 90 percent of services (Shafira 2024). In 2022, the government of Costa Rica suffered major disruption from a ransomware attack when the UNC1756 group stole and leaked over 672 GB of sensitive information from almost 30 public institutions, including

state-owned telecom company RACSA and the Ministry of Science, Innovation, Technology, and Telecommunications. This resulted in aggregate economic losses of up to 2.4 percent of GDP, and the declaration of a national emergency (Fadilpašić 2022).

The success of these cyberattacks shows that awareness and intent are not enough to prevent serious compromises. Telecom operators, especially in emerging markets, face structural limitations in building their defenses and responding to attacks. Five key structural barriers stand between emerging-market telecommunications operators and the security they need: aging infrastructure, cybersecurity talent gaps, fragmented regulatory landscapes, the structural tension between investing in growth and investing in security, and geopolitical supply-chain pressures. Figure 1 highlights four of the challenges—legacy systems, a shortage of skilled professionals, regulatory complexity, and budget constraints—while other surveys conducted by IFC and EY surfaced the fifth challenge, geopolitical events.

Understanding these barriers and their interactions is the first step toward overcoming them. Yet, companies do have the ability to prioritize which structural weaknesses are most critical, rather than attempting to tackle all challenges simultaneously. A risk-based prioritization approach focused on the most critical assets and services often produces the greatest resilience gains when resources are limited.

Figure 1
Biggest Cybersecurity Challenges Organizations Face



Source: GSMA Intelligence 2025a, 32.

Note: Telecoms operators were asked to select the two biggest challenges their organizations faced when deploying cybersecurity tools.

Legacy infrastructure: The most cited barrier

Legacy system architecture emerged as the top structural barrier to improved cybersecurity in a recent IFC–EY survey, with three-quarters of telecom service providers identifying it as a significant challenge. Legacy systems—often referred to as “technical debt”—require extra effort to secure because they are often incompatible with modern tools, difficult to patch or monitor effectively, and expensive and disruptive to replace in live networks (Min and others 2025).

Currently, most telecom markets in China, Europe, the Middle East, and North America have largely transitioned their infrastructure to 4G and 5G mobile architectures. The situation in emerging markets is far more complex, with greater dependencies on outdated systems and fewer resources available to modernize or replace them. As of June 2025, 52 percent of connections in Africa rely on 2G and 3G networks and are projected to shrink to 25 percent by 2030 (GSMA 2025b, 42). Other emerging markets—including Asia Pacific, Eurasia, and Latin America—must manage heterogeneous networks comprising 2G through 5G architectures concurrently (GSMA 2025b, 42).

Legacy infrastructure layering creates complex, hybrid environments with multiple vulnerability surfaces. Each generation of technology that remains introduces new points of intersection and new attack vectors. Signaling System 7 (SS7), the signaling protocol underlying most 2G and 3G infrastructure was originally designed in the 1970s and contains well-documented vulnerabilities such as call rerouting, SMS interception, and

real-time location tracking that remain fully exploitable as long as those networks remain live (Schmidt 2025). Even operators that have switched off their own 2G and 3G networks are often still connected to SS7 to support international roaming, meaning exposure within the industry is global and systemic given the reliance on legacy architecture (Quintin 2024).

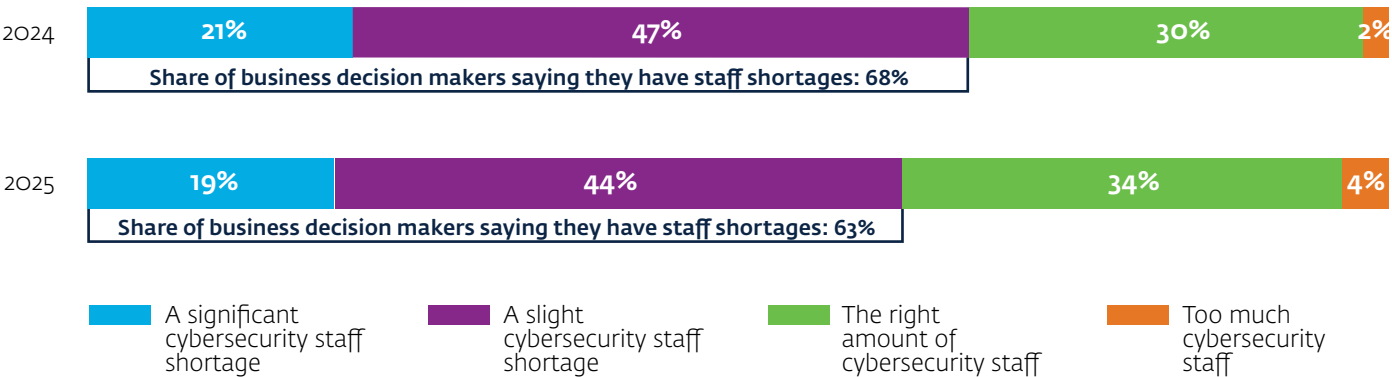
“Against a backdrop of growing cyberthreats and expanding attack surfaces, network defenders are drowning in the operational complexity of a legacy security mindset,” said Nikesh Arora, chairman and chief executive officer of Palo Alto Networks, in a 2025 World Economic Forum (WEF) report (WEF and Accenture 2025). “They struggle to stitch together dozens of disparate security solutions and enforce security policies across an enterprise’s network, cloud, and endpoint environments.”

However, accelerating the retirement of legacy infrastructure is often financially impractical for operators in emerging markets, especially among those serving rural and low-income populations that rely on 2G or 3G coverage. The result? A long tail of exposure with no near-term exit.

The skills and talent gap

The past two years of economic uncertainty have left many companies with gaps in cybersecurity skills. In 2025, 63 percent of companies globally had staff shortages (Figure 2), and 59 percent lacked one or more critical skills on their cybersecurity team (ISC2 2025, 10–11). These gaps have material organizational impacts, with 88 percent of organizations reporting at least one significant cybersecurity consequence occurring due to a lack of such skills (ISC 2025, 15).

Figure 2
Executives See Skill and Talent Gaps in Cybersecurity Staffing



Source: ISC2 2025, 10.

These negative impacts emerge from four key talent-related obstacles that organizations and the cybersecurity industry face: attracting talent into cybersecurity, educating and training professionals, recruiting the right cybersecurity talent, and retaining their professionals (WEF 2024, 3). Attracting talent has become increasingly difficult as demand for skilled cybersecurity professionals continues to outpace available supply. The cybersecurity workforce gap was estimated at almost five million in 2024, a 19 percent year-on-year increase from 2023 (ICS2 2024, 11). Additionally, employees have a wide range of potential compensation options, with 42 percent of companies reporting being “outbid” by competitors on salary and benefits (Fortinet 2025, 22).

Cybersecurity education is also extremely varied across the globe, with the absence of a standardized approach to education and certifications, a shortage of qualified instructors, and limited awareness among potential learners of career options or study pathways. Recruiting poses its own unique challenges, with 52 percent of organizations reporting difficulty hiring for cybersecurity roles because of supply shortage, limited human resource capacity to effectively prescreen candidates, and reluctance to hire entry-level employees (Fortinet 2025, 22; WEF 2024, 15). Finally, retention can be challenging for organizations. Budget cuts, insufficient appreciation, a lack of training and upskilling opportunities for employees, and better compensation at other companies can all drive attrition (WEF 2024, 20).

The skills and talent gap is an issue facing telecom operators across the globe; however, the gap is more pronounced in emerging markets (de Salins and Lewin 2023). Emerging-market telecommunication operators struggle to find the cybersecurity talent needed to protect their networks, business, and customers. While about two-thirds of organizations in Europe and North America believe they have the people and skills they need to meet their security requirements, more than 50 percent of CEOs in emerging markets report difficulty recruiting cybersecurity-skilled workers, including 70 percent in Sub-Saharan Africa and 69 percent in the Latin America and Caribbean regions (WEF and Accenture 2026, 16).

In emerging markets, the rapid evolution of the cybersecurity landscape has been vastly outpacing the development of the associated workforce (WEF 2024, 4). A systemic lack of investment in cybersecurity skills has created deeper gaps than in more developed markets, although in recent years, public and private programs have been surfacing to fill the cybersecurity education gap. The United Nations Development Program launched a regional cybersecurity training program targeting young people across West and Central Africa in late 2025, the International

Telecommunication Union started a training program in 2025 focused on women across dozens of emerging regions, and Microsoft South Africa is collaborating with the Youth Employment Service to train young people in digital skills. As of 2026, with more than 70,000 young people have been engaged in digital learning pathways, and over 140,000 certification opportunities have been unlocked (UNDP 2025; ITU 2025; Microsoft 2026).

“Closing the cybersecurity skills gap is essential for safeguarding enterprises and addressing global workforce shortages. Programs like Cyber Girls, Africa’s biggest female-focused cybersecurity training programme, not only equip women with critical cybersecurity expertise but also empower them to enhance their own well-being and economic prospects. Investing in such programmes is a vital step towards building a more secure and inclusive digital future,” said Confidence Staveley, founder of the CyberSafe Foundation (WEF and Accenture 2025).

As these skill and talent gaps persist, it is becoming increasingly important to take decisive, forward-thinking action to mitigate potential long-term impacts. “It’s critical we help close the growing cyber skills gap with a focus on training, reskilling, recruiting and retaining cybersecurity talent,” said Chuck Robbins, chair and chief executive officer of Cisco (Moschetta and Winslow 2025).

 This dual-layered approach ensures that the organization not only complies with local legal requirements but also adheres to globally recognized best practices in information security management. 

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

Regulatory fragmentation and compliance burden

Telecommunication operators in emerging markets frequently work across multiple jurisdictions, where cybersecurity and data-protection requirements can vary widely. Regulations can be complex, contradictory, or extensive in scope, increasing the

compliance burden for operators. Sixty-nine percent of chief information security officers (CISOs) felt that regulatory fragmentation across jurisdictions “greatly affects” their organization’s ability to maintain compliance (WEF and Accenture 2025, 28).

The extent of fragmentation differs by regions, with emerging markets experiencing the greatest lack of coherence. A 2025 Latin America cybersecurity report by the Inter-American Development Bank and Organization of American States documents substantial variation in the maturity and coverage of the region’s regulatory frameworks. As of 2025, only 10 out of 30 countries have reached a maturity level of three or higher out of five in Legal and Regulatory Requirements for Cybersecurity (Note 2), while 15 have a similar maturity level in the development of a national cybersecurity strategy (Porrúa and others 2025, 27; Note 2).

The African Union developed the Malabo Convention on Cyber Security and Personal Data Protection to unify regulations in the region. However, its effectiveness is limited because as of late 2025, only 16 of the 55 member states have ratified it, representing a minimal ~30 percent adoption rate (Ifeanyi-Ajufo 2025). Low ratification rates hinder the coherence of policies across the continent and create uneven compliance burdens for those that have endorsed it.

Across Asia-Pacific regions, regulatory frameworks vary significantly by country. Singapore has robust cybersecurity regulations, last amended in 2024; Malaysia has been regularly updating laws and policies, most recently with their Cyber Security Act 2024; while Indonesia has extremely fragmented cybersecurity laws, missing key areas that address critical infrastructure attacks and public cybersecurity—a situation that the long-delayed Cyber Security and Resilience Bill could fix (CSA Singapore 2026; PT Security 2025; Lebang 2025).

This fragmentation creates problems for compliance, because operators spend resources meeting minimum regulatory requirements in each jurisdiction rather than building coherent, risk-based security programs. In this disjointed regulatory landscape, internationally recognized frameworks, such as NIST CSF, ISO 27001, and GSMA FS.31, can provide a consistent baseline across jurisdictions that still allows operators to satisfy local regulatory requirements. Rather than focusing only on local regulatory requirements, telecom operators can use international standards to guide their cybersecurity efforts.

“This dual-layered approach ensures that the organization not only complies with local legal requirements but also adheres to

globally recognized best practices in information security management with a prioritized risk rating which highlights and categorizes vulnerabilities and threats based on their severity, impact, and business context with established processes to ensure continuous monitoring,” said Eric Maes, head of security architecture and solutions for Nokia Group Security.

Budget constraints and the return on investment (ROI) problem

Budget cuts remain an operational reality for cybersecurity teams. Cybersecurity investment continues to contract as boards that are focused on growth metrics struggle to justify the spending. In 2025, 36 percent of organizations globally reported cuts to their cybersecurity budgets. The telecommunications sector was among the hardest hit, with 41 percent of operators reporting budget reductions (ISC2 2025, 8).

Since cybersecurity investments are measured against prevented losses, which are difficult to prove, assets are typically funneled into projects with more obvious and straightforward returns. For telecommunication operators, cybersecurity budgets frequently compete directly with capital expenditure decisions on infrastructure rollout, new service development, and network enhancements. In emerging markets, where revenue per user is thin and capital expenditure is already stretched, major security spending is frequently deferred.

Moreover, the consequences of underinvestment can be catastrophic. SK Telecom, South Korea’s largest mobile carrier, was breached in April 2025 by malware that compromised almost 27 million subscriber records, an incident that resulted in regulatory fines, forced SIM card replacement for millions of customers, and a pledge by the company to invest approximately 700 billion won (US\$513.38 million) into data protection efforts, customer benefit packages, and government compliance efforts over the next five years (Lemos 2025).

Budget pressures not only impact cybersecurity investments but can also drive talent loss. When security headcount is cut, the most experienced practitioners—the ones who have the most options—leave first, making a lack of budget a top reason for the widening cybersecurity skills gaps (29 percent) (ISC2 2025, 14). This becomes a vicious, self-reinforcing cycle as constrained budgets lead to understaffed teams and reduced cybersecurity investments. This increases the probability of breaches that can incur massive remediation costs, which further constrain future budgets.

Geopolitical exposure and supply-chain risk

Geopolitical rivalries are increasingly intertwined with cybersecurity activity. Intensifying geopolitical tensions drive many of the high-impact cybersecurity attacks facing organizations today, with government-linked threat actors responsible for 53 percent of exploitation activities (Insikt Group 2025). Telecom companies in North and East Africa suffered several attacks in late 2023 when the Seedworm group, linked to a Middle Eastern nation, installed remote access tools in efforts to gather critical intelligence from telecommunication networks (Symantec and Carbon Black 2023).

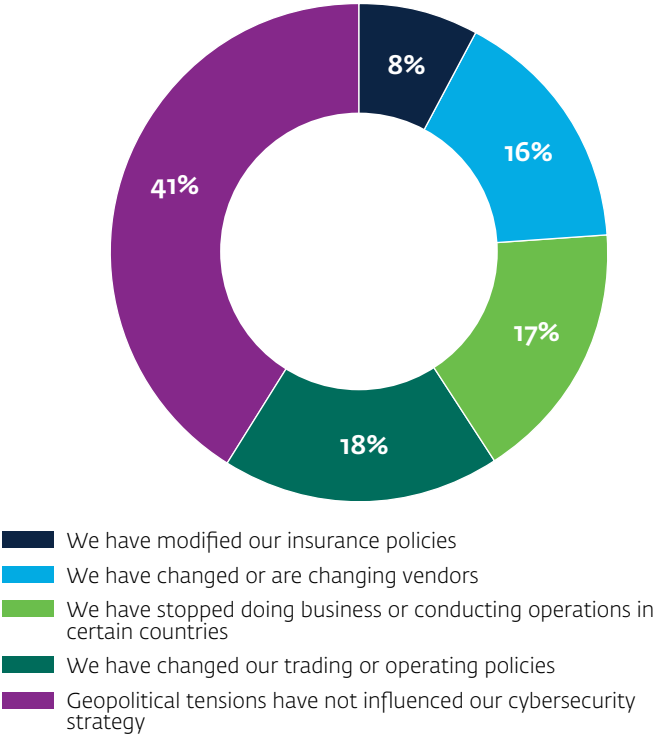
Against the backdrop of increased cyberattacks aimed at espionage, surveillance, or other geopolitical objectives, nearly 60 percent of respondents in a 2025 WEF survey reported that geopolitical tensions have influenced their organization's cybersecurity strategy (WEF and Accenture 2025, 26) (Figure 3). As a result, many companies have stopped doing business or conducting operations in certain countries, altered their trading or operating policies, switched or are planning to switch vendors, or modified their cybersecurity policies.

Unsurprisingly, geopolitical concerns often show up as supply-chain risks. According to WEF 2025 research, 54 percent of large organizations find that supply-chain interdependencies are a major barrier to achieving cyber resilience (WEF and Accenture 2025, 6). Supply-chain cyberattacks and limited third-party security visibility remain persistent concerns, with 48 percent of CISOs reporting difficulty complying with third-party security requirements and managing risks tied to complex supply-chain dependencies (WEF and Accenture 2025, 25).

These challenges can be particularly acute in emerging markets, where cybersecurity capabilities, institutional capacity, and incident-response resources are often less mature, increasing exposure to cybersecurity risks arising from critical supply chain dependencies (World Bank 2025). Illustrating the danger, a five-year compromise of Syniverse, a text-message routing service gave cyberattackers access to the environments of 235 telecom operators and may have exposed some of the 740 billion text message routed annually through the provider's infrastructure. The cyber-threat group likely had access to routing information like source, destination, and timestamps, but may have also gained access to message content (Ilascu 2021).

Data sovereignty requirements are also expanding, with governments increasingly mandating — to differing degrees — that data be stored and processed within national borders, adding compliance complexity and cost for operators with cross-border infrastructure. Regulations like Brazil's Lei Geral de Proteção de Dados (Fennessy 2020), India's Personal Data Protection Bill, and Vietnam's Personal Data Protection Law (Aw 2026) often require data localization or have strict requirements for the sharing of specific data types, all driven by concerns about national security and protecting citizen data (Recording Law 2026; Thales 2025).

Figure 3
The Influence of Geopolitical Tensions on Cybersecurity Strategy



Source: WEF and Accenture 2025, 26.

Conclusion: Balancing growth and security—where to start

The fundamental tension among these five interconnected barriers is that every dollar spent on cybersecurity is a dollar not deployed elsewhere. Investments in network expansion, subscriber acquisition, or new service development are often

prioritized before cybersecurity investments, and for operators serving fast-growing, price-sensitive emerging markets, the trade-off is real and constant. However, incremental improvements can significantly enhance resilience without requiring wholesale transformation.

Practical, action-based starting points for network operators working within constrained budgets include expanding

multifactor authentication or adopting zero-trust security models, improving asset inventories, reducing administrative privileges, strengthening patch management processes, conducting tabletop exercises, and improving vendor access governance. These measures can often provide meaningful risk reduction without requiring significant capital investment.

Overall, telecom operators need to address some common weaknesses. Measures include the following:



Bolster detection of common telecom threats

- Deploy defenses against ransomware and phishing.
- Monitor for behavioral anomalies and lateral movement.
- Correlate events across IT, cloud, and telecom networks.
- Monitor legacy infrastructure for signs of compromise.
- Incorporate threat intelligence into detection capabilities.



Continuously evaluate third-party supplier security

- Conduct security due diligence before onboarding vendors.
- Include cybersecurity requirements in supplier contracts.
- Continuously monitor third-party access and activity.
- Periodically reassess critical suppliers as risks evolve.
- Restrict vendor access using least-privilege principles.



Manage security of cloud services

- Enforce multi-factor authentication and least privilege.
- Continuously monitor cloud configurations for misconfigurations.
- Use cloud security posture management and cloud access security brokers solutions to improve cloud visibility.
- Regularly review privileged cloud accounts.
- Secure cloud workloads throughout their life cycle.



Regularly test security response to eliminate uncertainty

- Maintain documented incident response playbooks.
- Conduct regular tabletop exercises and simulations.
- Test backup and disaster recovery procedures.
- Clearly define roles, responsibilities, and escalation paths.
- Update response plans based on lessons learned.

For telecom operators in emerging markets, legacy architecture, the skills and talent gap, fragmented regulatory landscapes, ROI and budget pressures, and geopolitical supply chain influences are operational realities that are compounding in real time. The operators that will emerge most resilient are those that treat security as an essential dimension of network quality, as fundamental to their service promise as widespread coverage and service quality. Article 4 in this series tackles the best practices among telecom operators in emerging markets and has more information on measures companies can take.

NEXT IN THE SERIES: ARTICLE 4 | WHAT GOOD LOOKS LIKE

The next article looks at what good cyber resilience looks like in practice, including the capabilities, controls, governance, and organizational practices telecom operators can put in place to strengthen their defenses and resilience.

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. The author manually counted the number of countries that had a 3 or higher for their CMM score in section 4-1, “Legal and Regulatory Requirements for Cybersecurity,” of the country reports in *Porrua* and others 2025.

References

- Aw, Charmian. 2026. “Notes from the Asia-Pacific Region: Vietnam Lifts Off into Global Data Sphere.” International Association of Privacy Professionals Blog, January 15, 2026. <https://iapp.org/news/a/notes-from-the-asia-pacific-region-vietnam-lifts-off-into-global-data-sphere>.
- Azhar, Mochamad. 2024. “Cyberattack on Indonesia’s National Data Centre Paralyzes Government Services.” *GovInsider*, June 25, 2024. <https://govinsider.asia/intl-en/article/cyberattack-on-indonesias-national-data-centre-paralyses-government-services>.
- CSA Singapore (Cyber Security Agency of Singapore). 2026. “Cybersecurity Act: Information on the Cybersecurity Act.” CSA Singapore. Update: June 3, 2026. <https://www.csa.gov.sg/legislation/cybersecurity-act/>.
- de Salins, Ghislain, and Tatyana Lewin. 2023. “Hacking the Cybersecurity Skills Gap in Developing Countries.” World Bank Blogs, November 28, 2023. <https://blogs.worldbank.org/en/digital-development/hacking-cybersecurity-skills-gap-developing-countries>.
- Fadilpašić, Sead. 2022. “Costa Rica Declares National Emergency after Conti Ransomware Attacks.” *TechRadar*, May 10, 2022. <https://www.techradar.com/news/costa-rica-declares-national-emergency-after-conti-ransomware-attacks>.
- Fennessy, Caitlin. 2020. “Top-5 Operational Impacts of Brazil’s LGPD: Part 3 — International Transfers.” International Association of Privacy Professionals Blog, November 5, 2020. <https://iapp.org/news/a/top-5-operational-impacts-of-brazils-lgpd-part-3-international-transfers>.
- Fortinet Training Institute. 2025. 2025 Cybersecurity Skills Gap. Sunnyvale, CA: Fortinet, 2025. <https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf>
- GSMA (Global System for Mobile Communications Association). 2025a. *The Impact of Cybersecurity Regulation on Mobile Operators*. GSMA, London https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/gsma_resources/the-impact-of-cybersecurity-regulation-on-mobile-operators/.
- GSMA. (Global System for Mobile Communications Association) 2025b. *The Mobile Economy Africa 2025*. GSMA, London. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/10/GSMA_AFRICA_ME2025_R_Web-3.pdf
- GSMA. (Global System for Mobile Communications Association) Intelligence. 2025. *Staying One Step Ahead Telco Security in 2025*. GSMA, London.
- Ifeanyi-Ajufo, Nnenna. 2025. “The AU Can Help African Countries Adopt the UN Cybercrime Convention. But the Challenges Are Significant.” Chatham House, October 2025. <https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant>.
- Insikt Group. 2025. “H1 2025 Malware and Vulnerability Trends.” Recorded Future report, August 2025. <https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-2025-o828.pdf>.
- ISACA (Information Systems Audit and Control Association). 2025. *State of Cybersecurity 2025*. ISACA, Schaumburg. <https://www.isaca.org/resources/reports/state-of-cybersecurity-2025>.
- ISC2 (International Information System Security Certification Consortium). 2024. *Global Cybersecurity Workforce Study*. ISC2, Alexandria. <https://edu.arrow.com/media/wtjfm5zx/2024-isc2-wfs.pdf>.

ISC2 (International Information System Security Certification Consortium). 2025. *ISC2 Cybersecurity Workforce Study*. ISC2, Alexandria. <https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>.

ITU (International Telecommunication Union). 2025. "Her CyberTracks: Policy & Diplomacy CyberTrack." ITU Academy. Accessed June 2026. <https://academy.itu.int/training-courses/full-catalogue/her-cybertracks-policy-diplomacy-cybertrack>.

Lebang, Christian Guntur. 2025. "Indonesia's Cyber Security and Resilience Bill: Strengthening Governance or Expanding Institutional Rivalries?" Lab 45, March 18, 2025. <https://www.lab45.id/detail/298/indonesia-s-cyber-security-and-resilience-bill-strengthening-governance-or-expanding-institutional-rivalries>.

Lemos, Robert. 2025. "South Korean Government Imposes Penalties on SK Telecom for Breach." Dark Reading, July 8, 2025. <https://www.darkreading.com/cyberattacks-data-breaches/south-korea-imposes-penalties-sk-telecom-breach>.

Microsoft. 2026. "From Potential to Opportunity: How Microsoft and YES Are Reshaping South Africa's Digital Future" Microsoft Source EMEA, May 2026. <https://news.microsoft.com/source/emea/2026/05/from-potential-to-opportunity-how-microsoft-and-yes-are-reshaping-south-africas-digital-future/>.

Moschetta, Giulia, and Ellie Winslow. 2025. "Geopolitical Tensions, AI and More Are Complicating the Cyberspace. Here's What to Know." World Economic Forum, January 13, 2025. <https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/>.

Porrúa, Miguel, Guillermo Moncayo, Santiago Paz, Ariel Nowersztern, Jorge Fernando Bejarano, Maria Florencia Baudino, Maria Paula Bordese, Kerry-Ann Barrett, Carlos Eduardo Baena, Mariana Jaramillo, Orlando Garces, Agustin Isidro, Sadie Creese, Michael Goldsmith, Carolin Weisser Harris, and Patricia Esteve-Gonzalez. 2025. *2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean*. Inter-American Development Bank (IDB) and Organization of American States (OAS), Washington, DC. <https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and>.

PT (Positive Technologies) Security. 2025. "Cybersecurity Threatscape in Southeast Asia." Positive Technologies, March 20, 2025. <https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-in-southeast-asia/#Navigation-36>.

Recording Law. 2026. "Data Localization Laws by Country (2026)." Recording Law, May 20, 2026. <https://www.recordinglaw.com/world-laws/world-data-privacy-laws/data-localization-laws-by-country/>.

Schmidt, Jeremy. 2025. "SS7: Securing a Legacy Protocol in a Modern Threat Landscape." Global System for Mobile Communications Association's Telecom Information Sharing and Analysis Center Blog, July 28, 2025. <https://www.gsma.com/solutions-and-impact/technologies/security/t-isac-blog/ss7-securing-a-legacy-protocol-in-a-modern-threat-landscape-and-how-information-sharing-can-help-to-mitigate/>.

Shafira, Monique Handa. 2024. "Temporary National Data Center Recovers 90 Pct of Services After June Cyberattack." *Jakarta Globe*, August 9, 2024. <https://jakartaglobe.id/tech/temporary-national-data-center-recovers-90-pct-of-services-after-june-cyberattack>.

Symantec and Carbon Black. 2023. "Seedworm: Iranian Hackers Target Telecoms Orgs in North and East Africa." *Security.com*, December 19, 2023. <https://www.security.com/threat-intelligence/iran-apt-seedworm-africa-telecoms>.

Thales. 2025. "Global Data Sovereignty: A Comparative Overview." Cloud Security Alliance Blog, January 6, 2025. <https://cloudsecurityalliance.org/blog/2025/01/06/global-data-sovereignty-a-comparative-overview>.