GLOBAL BLUEPRINT FOR TRUSTED ICT INFRASTRUCTURE

Flagship Report

September 2025

GLOBAL CYBERSECURITY FORUM | stc

GLOBAL CYBERSECURITY FORUM

The Global Cybersecurity Forum (GCF) is a non-profit organization that seeks to strengthen global cyber resilience by advancing purposeful dialogue, enhancing international multi-stakeholder collaboration, and supporting high impact initiatives.

GCF is a platform where the world's cybersecurity stakeholders can exchange knowledge and collaborate in tackling critical issues around Cyberspace. GCF aims to catalyze socioeconomic change, expand the boundaries of knowledge on critical cybersecurity topics, and build the foundations for global cooperation on the key challenges and opportunities in Cyberspace.

By uniting decision makers and thought leaders from around the world, GCF aligns with international efforts to build a safe and resilient Cyberspace that enables prosperity for all nations and communities.

stc

stc, as the leader in ICT services in the Middle East, has grown beyond telecommunications to connect the world, enrich lives, and drive transformation of the cyber world. Through world-class infrastructure, emerging technologies, and a strong commitment to sustainability, stc empowers communities, businesses, and industries in Saudi Arabia, the region, and beyond.

stc's investments are pivotal in establishing Saudi Arabia as a major hub to enable the cyber ambitions that are redefining industries and enhancing lives in society. Guided by its values of drive, devotion, and dynamism, stc addresses environmental and social challenges while upholding strong governance, ensuring a secure, sustainable, equitable, and cyber-empowered future for all.

Foreword

Mazen Alahmadi
stc;
Chairman of the 'Safeguarding Future Networks and Emerging Technologies' Knowledge Community

As we progress toward an advanced cyber future, it is critical to ensure that the mobile infrastructure we rely on is secure and resilient.

We aim to spark a global policy and investment discussion on protecting the often-overlooked layer of mobile signaling before threats outpace our ability to respond.

This report aims to catalyze this dialogue. Its findings support the development of pragmatic, scalable, and inclusive cybersecurity strategies to secure the silent backbone of mobile communications signaling — aligning with GCF's mission to strengthen the safety and resilience of Cyberspace for all through collaborative priorities, purpose-driven dialogue, and impactful initiatives.

I would like to thank the members of the 'Safeguarding Future Networks and Emerging Technologies' Knowledge Community for their expert and valuable input to this work. It is through the inclusion of diverse experiences that we can ensure our interconnected world is built on trust.

Contributors

- **Ian Keller,** Ericsson
- **Abdulmajeed A. Aleid,** stc
- **Islam R. Swelam,** stc
- **Nauman Khan,** stc
- **Mohammed Y. Uddin,** stc
- **Abdul Razzak Arif Shaikh,** stc
- **Muhammad Abu Bakar Khan,** stc
- **Mohammed Imran Ahmed Khan,** stc
- **Farhan A. Anjum,** stc

Knowledge Community: Safeguarding Future Networks and Emerging Technologies

In an increasingly interconnected world, the evolution of next generation ICT technologies, such as 6G, has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities, safeguard its deployment, and to harness its capabilities for the benefit of society. The 'Safeguarding Future Networks & Emerging Technologies' Knowledge Community is committed to promoting and safeguarding current and future ICT networks, bringing together a diverse array of expertise from multiple stakeholder groups.

The community welcomes ICT providers, telecom companies, telecom industry players, cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of ICT networks.

Contents

Useful Acronyms 05

Executive Summary 07

Introduction 08

Research Methodology 09

Survey Design and Participation 11

Key Survey Insights 13

1. Macro-Level Strategic Analysis 14

1.1 Safeguarding an interlinked ecosystem 14

1.2 Why signaling security matters strategically 14

1.3 Mobile financial services impact 15

1.4 IoT environments impact 16

1.5 Emergency alert systems impact 16

1.6 Mapping signaling-related threats to national interests 16

1.6.1 National security 16

1.6.2 Cyber economy 17

1.6.3 Cross-border trust 17

1.6.4 Systemic risks and governance blind spots 18

1.6.5 Third-party dependence and vendor lock-in 18

2. Security of Mobile Network Signaling 19

2.1 The silent threat 19

2.2 Current defensive measures 20

2.3 Maturity in detecting and responding 21

2.4 Barriers in improving security 22

2.5 Visibility into interconnect and roaming-based signaling threats 23

2.6 Vendor effectiveness 24

3. Cyber Resilience of Critical ICT Infrastructure 25

3.1 Assessing readiness and closing resilience gaps 25

3.2 The pervasive impact and visibility gap of signaling threats 25

3.3 Critical disparity in contingency plan maturity 25

3.4 The infrequent cadence of operational stress testing 26

3.5 An industry mandate for national policy action 27

4. 5G Rollout and Its Cybersecurity Implications 28

4.1 Global 5G deployment status and security maturity 28

4.2 Key security challenges in deployment 29

4.3 Architectural complexity of 5G 30

4.4 Supply chain risks 31

4.5 Biggest concerns regarding 5G signaling 32

4.6 Expert insights from the field 34

5. Recommendations 35

5.1 For MNOs 35

5.2 For vendors 36

5.3 For regulators 37

5.4 For academia and industry alliances 37

5.5 Five-point policy roadmap 38

Conclusion 39

Bibliography 40

Disclaimer

This document has been published by the Global Cybersecurity Forum (GCF) in collaboration with Knowledge Partners as part of their efforts to promote thought leadership in cybersecurity. While GCF and the knowledge partners have made every effort to ensure the accuracy and reliability of the information provided, neither party assumes any responsibility for errors, omissions, or inconsistencies in the content, nor for any consequences arising from its use or interpretation. The content is provided for general information purposes and may be subject to change without prior notice at the discretion of GCF. This publication is protected by copyright law. No part of this report may be reproduced, distributed, or transmitted in any form or by any means—whether electronic or mechanical—without prior written permission from both GCF and the Knowledge Partners. All requests for such permissions should be directed to KC@GCForum.org.

Useful Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
4G	4th Generation Cellular Network Technology
5G	5th Generation Cellular Network Technology
6G	6th Generation Cellular Network Technology
AI	Artificial Intelligence
API	Application Programming Interface
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CNF	Containerized Network Functions
CRI	Composite Resilience Index
CSP	Communication Service Provider
DoS	Denial-of-Service
EDR	Endpoint Detection and Response
GCF	Global Cybersecurity Forum
GDP	Gross Domestic Product
GSMA	GSM Association
GTP	GPRS Tunneling Protocol
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IoT	Internet of Things
IPsec	Internet Protocol Security
ITU	International Telecommunication Union
LTE	Long-Term Evolution
MEC	Multi-Access Edge Computing
MNO	Mobile Network Operator
NB	Narrowband
NE	Network Element
NF	Network Function
OTP	One-Time Password
PCAP	Packet Capture
RAN	Radio Access Network
RF	Radio Frequency

Acronym	Definition
SA	Standalone
SBA	Service-Based Architecture
SBI	Service-Based Interface
SBOM	Software Bill of Materials
SDN	Software-Defined Networking
SEPP	Security Edge Protection Proxy
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signaling System 7
TLS	Transport Layer Security
TPRM	Third-Party Risk Management
UAE	United Arab Emirates
USD	United States Dollar

Executive Summary

Mobile network signaling, the foundational layer that enables devices, services, and networks to communicate, is increasingly recognized as a strategic cybersecurity blind spot. Despite its critical role in enabling global cyber infrastructure, this layer remains inconsistently secured, poorly monitored, and underrepresented in both policy frameworks and risk assessments.

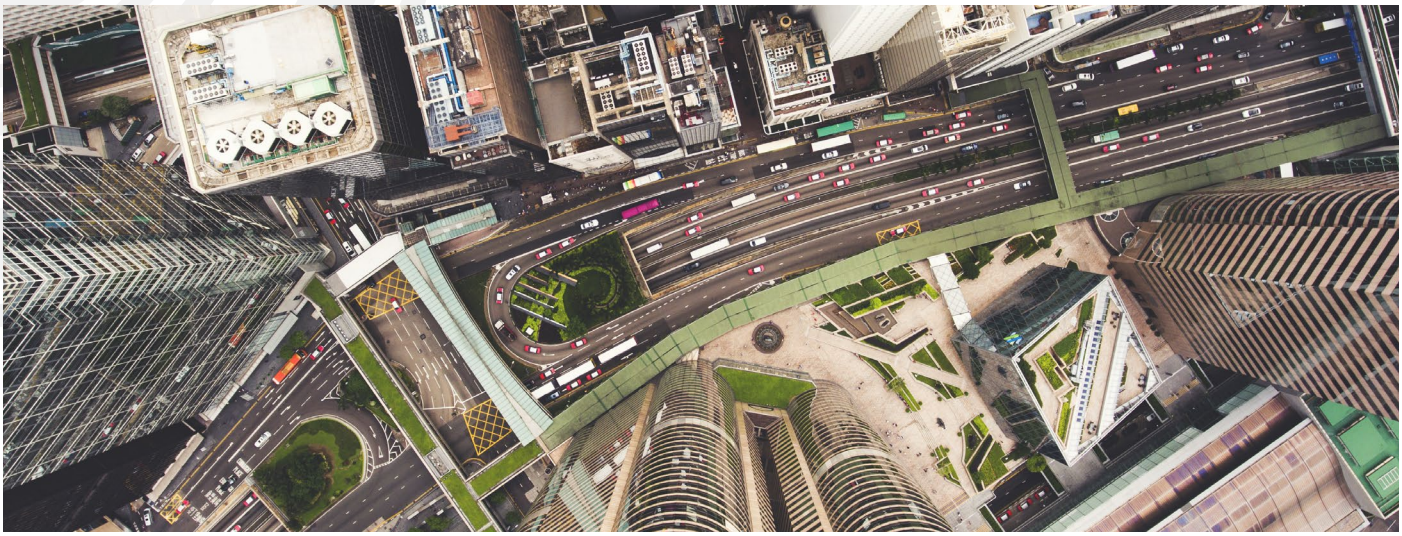
While 5th Generation cellular network technology (5G) and future mobile networks continue to evolve through cloud-native architectures and enhanced security measures, the telecom industry will, for years, operate hybrid environments that also support older generations. This sustained reliance on legacy technologies leaves a broader attack surface, and long-standing vulnerabilities in signaling protocols such as Signaling System 7 (SS7), Diameter, GPRS Tunneling Protocol (GTP), and Session Initiation Protocol (SIP) remain largely unaddressed.

More than 5 billion mobile users worldwide rely on secure mobile services, making the need for robust protection paramount. This flagship report, commissioned by the Global Cybersecurity Forum (GCF), is a result of continuous collaboration among GCF Knowledge Community members. It delivers a globally coordinated, data-driven analysis of signaling-layer threats and resilience challenges across mobile generations (2G-5G+). The report is based on a mixed-methods research approach that includes global survey data, expert interviews, and comparative secondary analysis.

Yet, while the methodology provides a strong evidence base, the findings reveal a striking reality: the operational and governance landscape has not kept pace with the risks.

The threats and challenges analyzed in this report include:

- **Widespread operational gaps:** Many mobile network operators (MNOs) lack formal threat detection or auditing mechanisms for signaling-layer traffic, particularly in legacy protocols.
- **Policy and governance misalignment:** In most countries, signaling security is not explicitly addressed in national cybersecurity strategies or critical infrastructure policies.
- **Emerging technology blind spots:** The cybersecurity implications of 5G innovations, such as application programming interface (API)-based service exposure, mobile edge computing, and network slicing, are poorly understood and underrepresented in existing threat models.
- **Low data transparency:** Operator maturity levels, incident data, and cross-border coordination practices remain difficult to benchmark due to limited data sharing and fragmentation.
- **Third-party dependence and vendor lock-in:** Relying heavily on external vendors and cloud providers for signaling security creates risks of vendor lock-in, limited interoperability, and dependence on proprietary technologies. These risks reduce flexibility, weaken bargaining power, and hinder resilience planning.
- **Strategic implications:** Without urgent and coordinated action, signaling vulnerabilities will continue to serve as attractive entry points for both nation-state adversaries and cybercriminal groups, potentially disrupting essential services, compromising user privacy, and eroding trust in global mobile ecosystems. These risks are especially pronounced in emerging markets, where infrastructure upgrades outpace security investment and institutional capacity.



Introduction

In today's hyperconnected world, mobile networks serve as the invisible infrastructure powering global communications, cyber economies, and essential services. Yet beneath their surface lies a complex and often overlooked component. This is the signaling layer, which is increasingly emerging as a critical cybersecurity concern. Despite its foundational role in ensuring the seamless operation of everything from phone calls and short message service (SMS) to 5G-enabled smart systems, the security of mobile network signaling remains fragmented, fragile, inconsistently monitored, and inadequately prioritized at both the technical and policy levels.

This flagship report offers a macro-level strategic analysis of the current and future risks associated with mobile network signaling, including the systemic implications these risks pose to trust, national cybersecurity, and cross-border cyber infrastructure. The report goes beyond conventional threat assessments by providing a comprehensive, cross-generational examination ranging from legacy SS7 and Diameter protocols to emerging 5G Service-Based Architecture (SBA) elements.

At the heart of this research lies a recognition that the cyber resilience of critical information and communications technology (ICT) infrastructure, particularly in telecom networks, is increasingly shaped by both inherited vulnerabilities and future-facing architectural decisions. The convergence of artificial intelligence (AI)-driven analytics, cloud-native infrastructure, and distributed edge components is expanding the attack surface in ways that existing frameworks are not yet fully equipped to address.

Equally important is the need for this topic to be approached through a policy and capacity-building lens, especially for countries where uneven cyber infrastructure, resource limitations, and a lack of localized threat intelligence present additional challenges. This report therefore incorporates regionally representative data and expert insights and proposes actionable recommendations aimed at empowering decision-makers to prioritize signaling-layer threats in regulatory, technical and operational strategies.

Finally, this report responds to a broader call for evidence-based policymaking. Through the integration of primary survey data, expert interviews, and international case studies, it presents a one-of-a-kind maturity benchmark and practical framework for guiding investment, regulation, and multi-stakeholder collaboration. It is a timely contribution to the global cybersecurity discourse, aligned with GCF's mission to advance cybersecurity for all through collaborative priorities, purpose-driven dialogue, and impactful initiatives.

Research Methodology

This flagship report applies a multi-method research approach, designed to generate data-driven insights into the cybersecurity risks associated with mobile network signaling across legacy and next-generation telecom infrastructures. The methodology was developed in close coordination with domain experts, industry practitioners, and members of GCF's Knowledge Communities.

Research design

The research was structured around a primary assumption: that mobile network signaling remains a globally under-assessed attack surface, despite its strategic importance in securing cyber infrastructure, particularly in the context of 5G rollout and critical ICT services. To test this, the study employed a mixed-method design including:

- **Quantitative survey data collection**
- **Expert interviews and roundtables**
- **Secondary research and literature review**

Each approach enriched the others, enhancing the validity of the themes and ensuring robust results.

Primary data collection

A customized, anonymized global survey was developed to gather perspectives from MNOs, telecom regulators, cybersecurity agencies, researchers, and industry vendors. The survey was distributed across multiple regions. It consisted of a variety of questions across four thematic domains, including:

- **Macro-level strategic analysis**
- **Security of mobile network signaling**
- **Cyber resilience of critical ICT infrastructure**
- **5G rollout and its cybersecurity implications**

Secondary research

The report draws on a curated analysis of:

- **Existing technical standards (e.g., 3GPP, GSMA, ITU)**
- **Governmental and intergovernmental reports**
- **Academic studies and white papers**
- **Threat intelligence sources from industry computer emergency response teams (CERTs), and telecoms and security vendors**

This supported the identification of research gaps, validated emerging risks, and informed thematic chapter development.

Analytical framework

The analysis followed a structured process:

- **Data cleaning and validation:** All survey responses underwent quality checks to eliminate outliers and incomplete data
- **Thematic coding:** Open-ended responses and interview notes were coded thematically to identify recurring concerns
- **Trend scoring:** Trends were assessed using three dimensions: impact, urgency, and feasibility to guide prioritization in recommendations
- **Comparative benchmarking:** Key responses (e.g., audit frequency, tool adoption) were benchmarked against known best practices

The analytical framework helped in formalizing the analysis process, building uniform and structured approach.

Limitations

While the study provides rich cross-sector and cross-regional insights, the following limitations apply:

- **Some regions remain underrepresented due to limited access to local telecom stakeholders**
- **Inconsistent terminology in global contexts (e.g., "signaling threat") may affect comparability**

These limitations are acknowledged in the interpretation of results and addressed through triangulation and expert validation.

Survey Design and Participation

To ensure that the findings of this flagship report are grounded in current industry realities, a targeted survey was conducted between June 2025 and July 2025. The questionnaire was designed to capture a multi-dimensional view of signaling security across mobile network environments, with a particular focus on emerging challenges introduced by 5G and cloud-native architectures.

Survey objectives

The survey aimed to:

- Measure awareness and perceived severity of signaling-layer threats
- Assess the maturity of operational defenses and incident readiness
- Identify vulnerabilities in critical services dependent on mobile signaling (e.g., mobile banking, IoT, and emergency alerts)
- Explore the security implications of 5G rollout, architecture choices, and supply chain dependencies
- Gather industry preferences on policy, technology, and operational measures to improve signaling resilience

Target audience

The survey was distributed to a global sample of professionals across the telecommunications and cybersecurity ecosystem, including:

- MNOs
- Telecom equipment vendors
- Regulatory authorities and policy makers
- Critical infrastructure operators
- Security researchers and academia

Survey methodology

- A questionnaire format using a mix of multiple-choice and Likert-scale
- Delivery distributed through industry mailing lists, GCF partner networks, and targeted outreach to telecom security professionals
- A response window of three weeks, with follow-up reminders to increase participation rates
- Data integrity ensured by anonymizing responses to encourage candid input

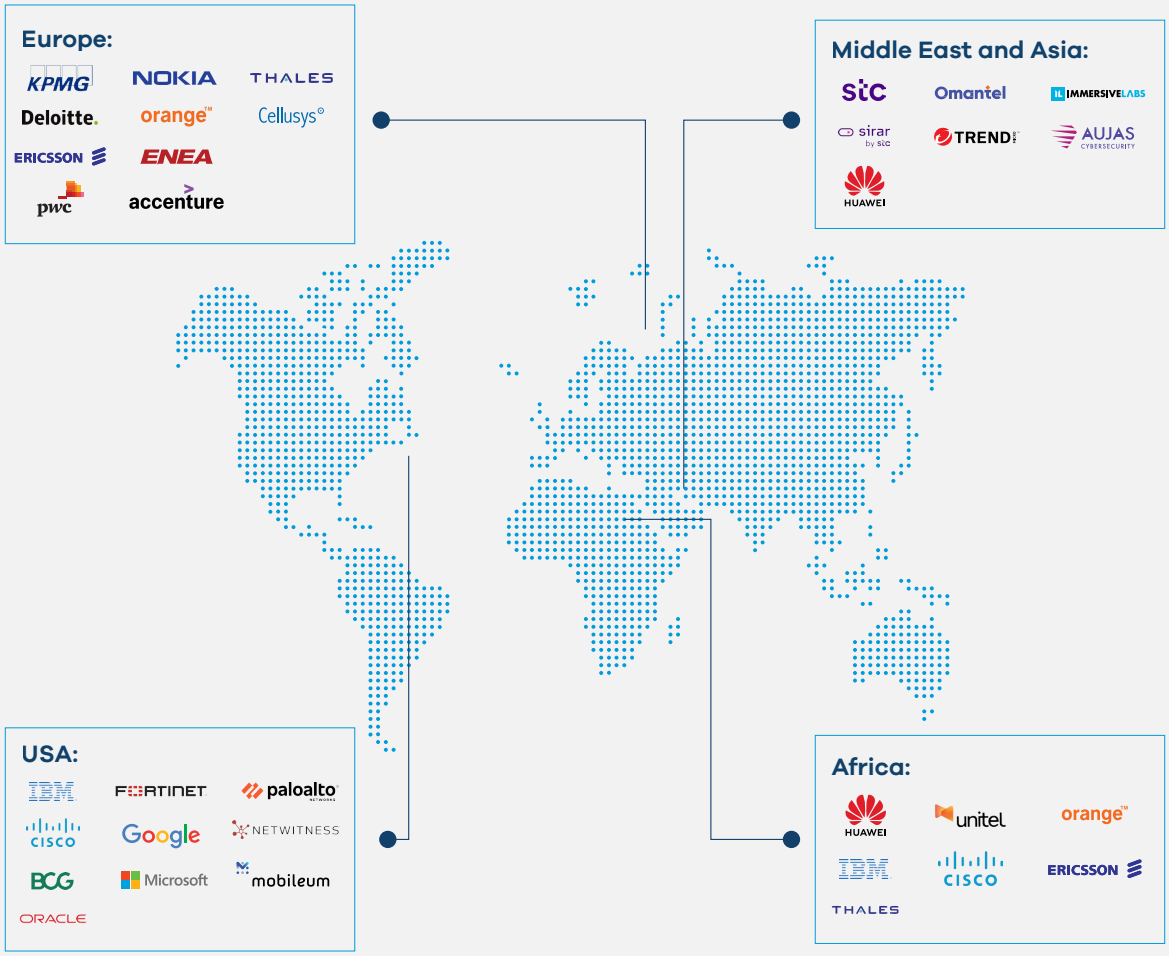
Participation overview

A total of 240 complete responses were collected from participants from 5 regions, representing both developed and emerging mobile markets.

- **By region: 71%** Middle East, **13%** Asia-Pacific, **8%** Africa, **5%** America, **3%** Europe
- **By roles: 47%** technical leaders, **35%** engineers, **15%** middle management level, **3%** C-suite executives

This diverse participation ensured that the findings capture both technical and strategic perspectives, enabling the development of recommendations that are globally relevant yet adaptable to local contexts.

Survey Participants



Key Survey Insights

The survey results provide a detailed picture of the current state of signaling security awareness, readiness, and priorities across the global telecom sector. Several critical insights emerged.

Vulnerabilities in critical services

When asked which critical service relying on mobile networks is most vulnerable to signaling attacks:

- **69%** identified mobile financial services and SMS-based two-factor authentication OTP
- **21%** cited IoT communications, such as smart grids and healthcare devices
- **10%** selected emergency alerts

This reflects widespread recognition that financial transactions and authentication mechanisms remain the most immediate targets for exploitation, while IoT and public safety services also face a significant, growing risk.

5G rollout readiness and security

The responses show a mixed global security maturity:

- **42%** are mid-rollout, with only basic protections in place
- **11%** are planning 5G deployments without security considerations

This uneven preparedness underscores the urgent need for consistent baselines and regulatory oversight.

Architectural security challenges

When asked which aspect of 5G architecture poses the greatest security challenge:

- **24%** cited virtualized core (cloud/ Software Defined Networking [SDN])
- **19%** chose open Radio Access Network (RAN)
- **17%** identified massive IoT management
- **14%** pointed to network slicing
- **5%** cited edge computing/Multi-Access Edge Computing (MEC)

Biggest 5G signaling concerns

When asked which aspect of 5G signaling is of most concern:

- **32%** identified the cloud-native attack surface
- **27%** highlighted protocol complexity
- **26%** selected core visibility challenges
- **15%** noted vendor lock-in

1. Macro-Level Strategic Analysis

The strategic analysis highlights that signaling security is no longer just a technical matter but a core issue of economic resilience, and international trust. It shows how vulnerabilities in financial services, IoT systems, and emergency communications create systemic risks that extend far beyond telecom operators. By mapping these threats to governance blind spots and vendor dependencies, the analysis underscores why protecting the signaling layer must become a policy and leadership priority worldwide.

1.1 Safeguarding an interlinked ecosystem through resilient mobile infrastructure

In today's interconnected world, the security of mobile networks is no longer a purely technical issue; it is a matter of economic resilience and international trust. As cyber economies expand and nations pursue ambitious cyber transformation agendas, they increasingly rely on mobile infrastructure that is the very backbone of global communications. Yet, beneath this foundation lies a little-known but critically important layer known as signaling, which silently co-ordinates the world's mobile communications.

1.2 Why signaling security matters strategically

While most cybersecurity efforts focus on protecting data, applications, or user devices, the signaling layer – which enables calls, texts, mobile internet, secure connectivity for remote workers, and roaming – often receives less attention in national cybersecurity strategies. This oversight is no longer sustainable. Vulnerabilities in this layer are being actively exploited by malicious actors, including cybercriminal groups and bad actors. The consequences are not just technical failures; they are strategic breaches that can impact public safety, compromise sensitive information, and erode national control over cyber infrastructure.

According to Moody's Ratings, telecommunications networks face the highest tier of cybersecurity risk, given their foundational role in both national infrastructure and global connectivity. A breach in these systems is not merely a corporate concern; it poses direct threats to public safety, national security, and economic stability.

Consider the consequences if emergency response systems were disabled, hospital operations disrupted, or critical energy infrastructure such as oilfields compromised. Communication Service Providers (CSPs) are already navigating the demands of integrating legacy systems with next-generation technologies, including 5G-enabled industrial automation and robotics. This growing complexity amplifies the challenge of balancing innovation with robust security governance.

The survey, which was conducted globally across technical and non-technical stakeholders, including Chief Information Security Officers (CISOs), policymakers, and telecom regulators, sought to gauge perceptions of vulnerability across critical services dependent on mobile networks. The results revealed a clear and pressing concern among stakeholders regarding the exposure of financial and identity verification systems that rely on signaling protocols, particularly those leveraging legacy technologies such as SS7 and Diameter, as shown in Figure 1 below.

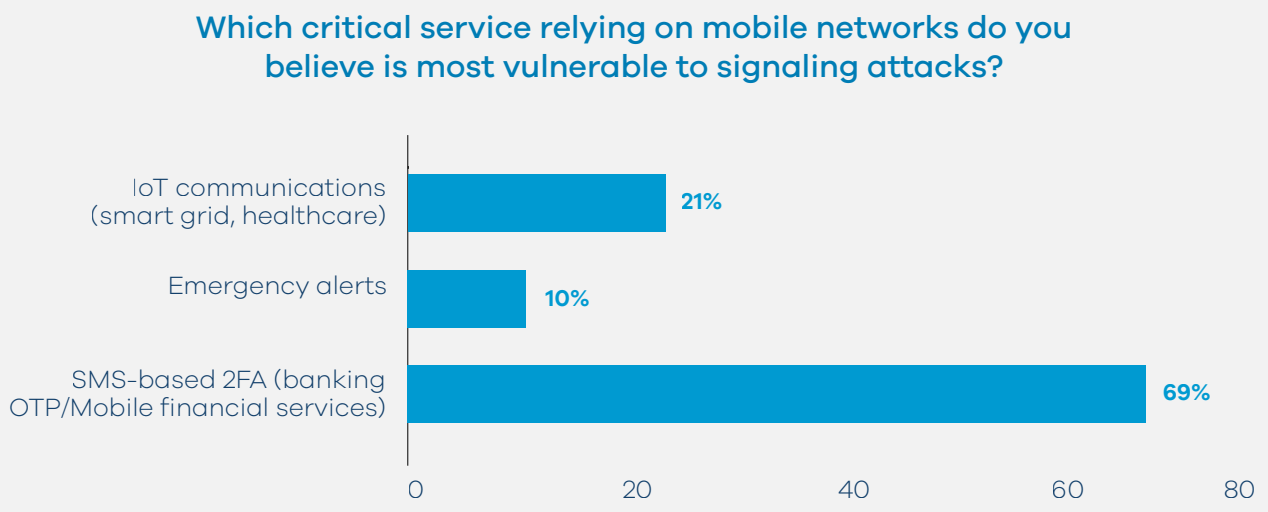


Figure 1: Critical services vulnerable to signaling attacks

1.3 Mobile financial services impact

The overwhelming selection of mobile financial services (over 69%) as being most vulnerable to signaling attacks, highlights the persistent fragility of SMS-based OTPs, which continue to be a cornerstone of customer authentication in banking, e-commerce, and payment platforms.

Despite global awareness of SS7 interception vulnerabilities, many financial institutions remain dependent on telecom infrastructure for user verification.

Stakeholders clearly perceive this dependency as a single point of failure, with far-reaching implications for:

- **Consumer trust in mobile banking**
- **Cyber-identity assurance mechanisms**
- **Cross-sector cybersecurity dependency between telecom operators and financial service providers**

Recent incidents involving OTP interception and Subscriber Identity Module (SIM)-swap fraud, often enabled through signaling exploitation, further validate these concerns. Left unaddressed, these risks may destabilize public confidence in mobile-enabled financial ecosystems and deter cyber transformation.

In July 2025, the Central Bank of the United Arab Emirates (UAE) issued a directive mandating the gradual phase out of SMS and email OTPs across all banks, to be fully implemented by March 2026, demonstrating the UAE's recognition of and action on the vulnerabilities associated with OTP-based authentication.

1.4 IoT environments impact

The 21% of the survey respondents who highlighted the vulnerability of IoT environments, including smart grids and healthcare systems, pointed to a fast-emerging vulnerability frontier. As these services increasingly rely on mobile network connectivity (notably narrowband [NB]-IoT and long-term evolution [LTE]-M), they remain exposed to signaling-based denial-of-service (DoS), session hijacking, and device impersonation attacks. These threats are particularly concerning given the mission-critical nature of these services, where downtime or manipulation could have immediate public safety or health consequences.

1.5 Emergency alert systems impact

Though selected by a smaller share (10%), the concern around emergency alert systems is no less critical. Governments worldwide are deploying cell broadcast and location-based SMS alerting systems to warn the public during natural disasters, terrorist incidents, and health crises. A successful signaling-layer attack could prevent alerts from reaching the public, disseminate spoof alerts to spread disinformation, or degrade trust in emergency communication altogether.

The relatively lower selection of this category may reflect limited awareness rather than limited risk, underscoring a potential gap in national risk prioritization frameworks.

These findings suggest that stakeholders perceive signaling threats not only as technical but as direct enablers of fraud, service disruption, and public trust erosion. For national cybersecurity strategies to remain relevant and resilient, they must treat signaling security as a foundational risk vector that spans sectors and geographies.

1.6 Mapping signaling-related threats to national interests

Signaling threats intersect with a range of high-priority national concerns, including:

1.6.1 National security

Attackers can exploit weaknesses in signaling systems to conduct surveillance on government officials, military personnel, and critical infrastructure operators. Such intrusions threaten not only privacy but also the integrity of national defense and intelligence capabilities.

1.6.2 Cyber economy

From mobile banking to smart cities, modern economies rely heavily on trusted mobile communication. If the signaling layer is compromised, it jeopardizes consumer trust, disrupts financial transactions, and undermines key cyber services - potentially affecting gross domestic product (GDP), investor confidence, and innovation.

According to industry research, many 4th Generation cellular network technology (4G) operators fail to enable built-in encryption (e.g., Transport Layer Security [TLS]/IPsec), leading to risks such as subscriber information disclosure, interception, fraud and even network downtime. These weaknesses directly undermine economic confidence in mobile-based financial services such as SMS OTPs and mobile banking, making cyber transactions easier to compromise without technical detection.

Another signaling-related security concern affecting the cyber economy is the fact that fraudsters are increasingly leveraging weaknesses in signaling to bypass billing systems and commit large-scale fraud. According to Juniper Research, global roaming fraud losses will exceed USD 8 billion by 2028, with signaling-based abuses accounting for 80% of total roaming fraud due to poorly built fraud detection policies tied to roaming models.

1.6.3 Cross-border trust

Mobile signaling allows seamless roaming and international connectivity. If one country's signaling infrastructure is insecure, it creates a weak link in the global cyber chain. This undermines trust among nations, service providers, and regulators, raising barriers to global collaboration and data flows.

Multiple European operators have been attacked by advanced threat actors who gained access to their SS7 networks and used them to track the movements of hundreds of users across countries by querying subscriber location information via ProvideSubscriberInfo messages.

Such unsanctioned cross-border signaling queries degrade trust in telecom infrastructure and challenge the integrity of international roaming agreements. They complicate diplomatic and regulatory co-ordination, as signals meant to be trusted are used for covert surveillance purposes.

1.6.4 Identifying systemic risks and governance blind spots

While mobile networks have become deeply integrated into national cyber ecosystems, powering finance, transportation, health, defense, and emergency services, there remains a significant underestimation of the systemic risks posed by signaling-layer vulnerabilities.

The governance of telecom security, especially at the signaling layer, is often fragmented across regulatory, commercial, and technical domains, resulting in blind spots in accountability, oversight, and incident preparedness. These gaps are further exacerbated by the complexity of modern mobile infrastructures (2G-5G+), vendor diversity, and international interconnectivity.

To understand the extent of these risks, the survey explored how signaling security is treated within national cybersecurity strategies. The results suggest a critical misalignment between perceived threats and strategic response. A significant disconnect between decision-makers and the weighing of technical risks against business and operational impact flags up a major governance blind spot. While awareness is rising, most policy frameworks have yet to catch up. As 5G and emerging technologies introduce new risks, including exposure through APIs, mobile edge computing, and automation, the absence of strategic oversight leaves nations increasingly vulnerable.

Furthermore, signaling-related risks are systemic in nature. A successful attack on signaling infrastructure can cascade across networks, impact multiple service providers, and cross borders without warning. Yet, because signaling systems are often managed in the background, visibility and accountability remain limited.

1.6.5 Third-party dependence and vendor lock-in

As operators reliant on third-party vendors, telcos face heightened risks of supplier concentration, vendor lock-in, and a single point of failure.

Overdependence on proprietary ecosystems limits operational agility, increases systemic vulnerabilities, and diminishes an operator's ability to adapt swiftly to evolving threats or switch providers.

Such rigidity can stifle innovation and resilience within signaling-layer protection strategies.

Vendor lock-in is recognized as a dangerous, often invisible innovation barrier. Many telcos remain bound by rigid enterprise software support models, hampering agility, complicating integration, and raising costs even for routine upgrades.

2. Security of Mobile Network Signaling

2.1 The silent threat: Why mobile signaling security cannot be ignored

Mobile networks are the arteries of modern communication, enabling everything from financial transactions to emergency alerts. Yet the signaling protocols that orchestrate these networks – SS7, Diameter, and GTP – were designed decades ago with minimal security considerations. Today, they remain a glaring weak point, exploited by cybercriminals, state-sponsored actors, and fraudsters to intercept calls, track users, bypass authentication, and even disrupt critical services.

While much of cybersecurity focuses on endpoints and data breaches, signaling-layer attacks operate at the infrastructure level, often bypassing traditional defenses. This section examines the real-world risks, operator preparedness and systemic gaps that leave mobile networks exposed to these stealthy yet devastating threats.

Key focus areas

1. The evolving threat landscape

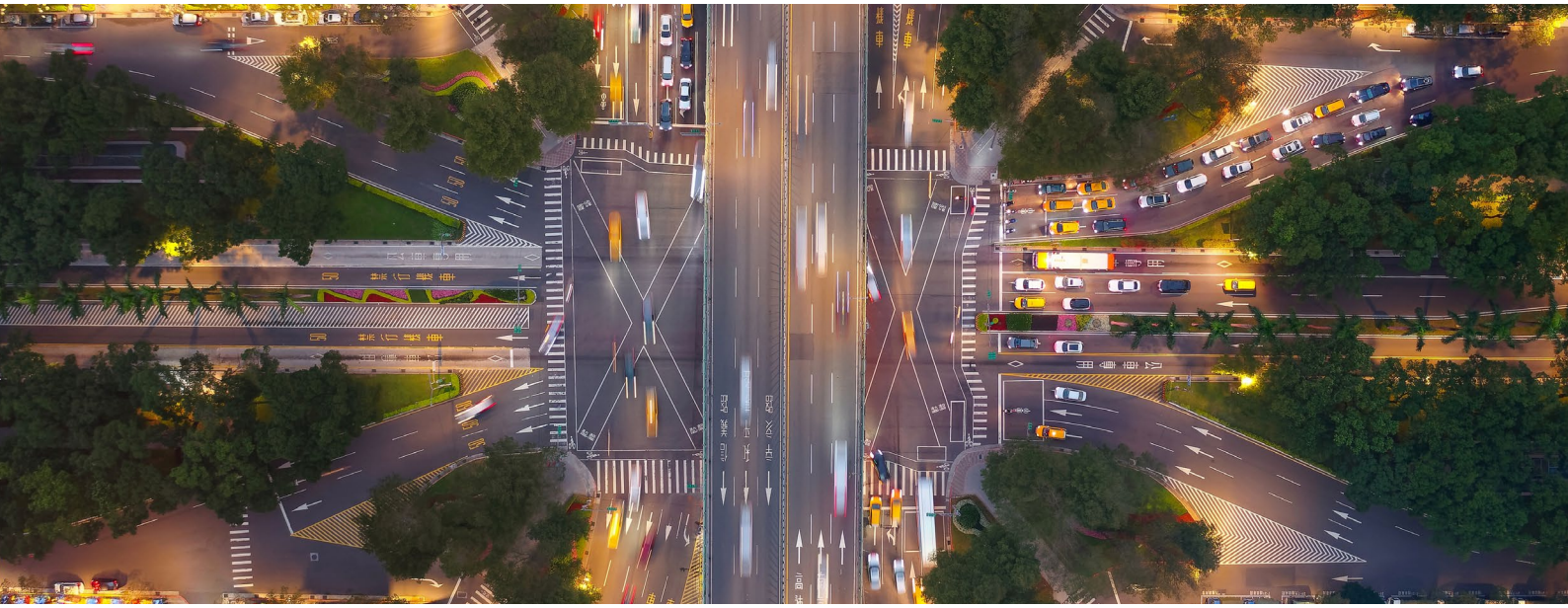
- **Interconnect threats:** Roaming and third-party interconnections create blind spots where attackers exploit signaling weaknesses across borders.

2. Operator maturity and gaps

- **Detection and response:** Many operators lack real-time monitoring for signaling attacks, relying on outdated or reactive measures.
- **Vendor dependence:** Operators often rely on vendors for security controls, but inconsistent implementations leave gaps in protection.

3. Regulatory and industry blind spots

- **Policy lag:** Many national cybersecurity strategies still overlook signaling security, treating it as a "telco issue" rather than a national security priority.
- **Stress testing and compliance:** Few regulators mandate rigorous signaling attack simulations, leaving networks untested against real-world exploits.



2.2 Current defensive measures against signaling attacks

Mobile signaling security requires layered defenses to combat evolving SS7, Diameter, and GTP threats. Figure 2 below assesses current industry protections to identify critical gaps between perceived risks and actual safeguards.

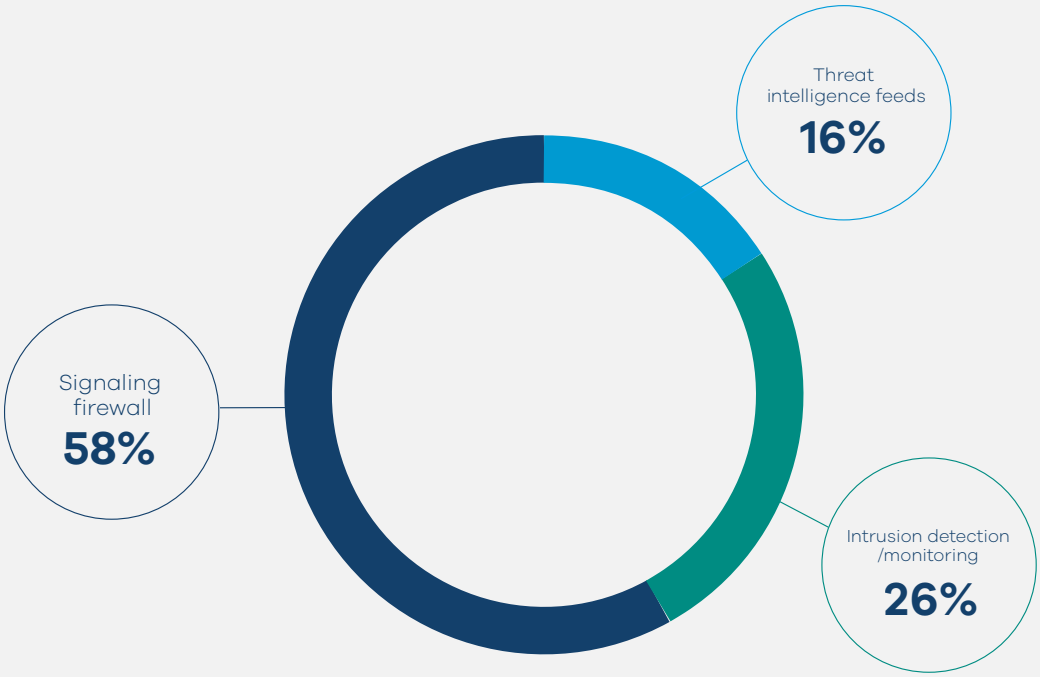


Figure 2: Adoption of key signaling security measures

Signaling firewalls dominate deployments (58%), reflecting industry recognition of basic perimeter defenses against SS7, Diameter, and GTP attacks. However, intrusion detection/monitoring lags (26%), exposing gaps in real-time threat visibility.

- **Critical weaknesses persist:** Few organizations use threat intelligence feeds (16%), leaving the rest blind to evolving tactics.
- **Firewalls are not equal to comprehensive security:** While 58% adoption of signaling firewalls is positive, these alone cannot stop advanced attacks (e.g., SS7 location tracking).

2.3 Maturity in detecting and responding to signaling attacks

Assessing organizational maturity in detecting signaling attacks reveals how prepared telecom operators are to identify and respond to critical threats. It highlights risk exposure, guides investment in defenses, and informs regulatory priorities. Low maturity signals systemic vulnerabilities that adversaries can exploit. Understanding maturity is essential for building resilient and secure telecom infrastructure.

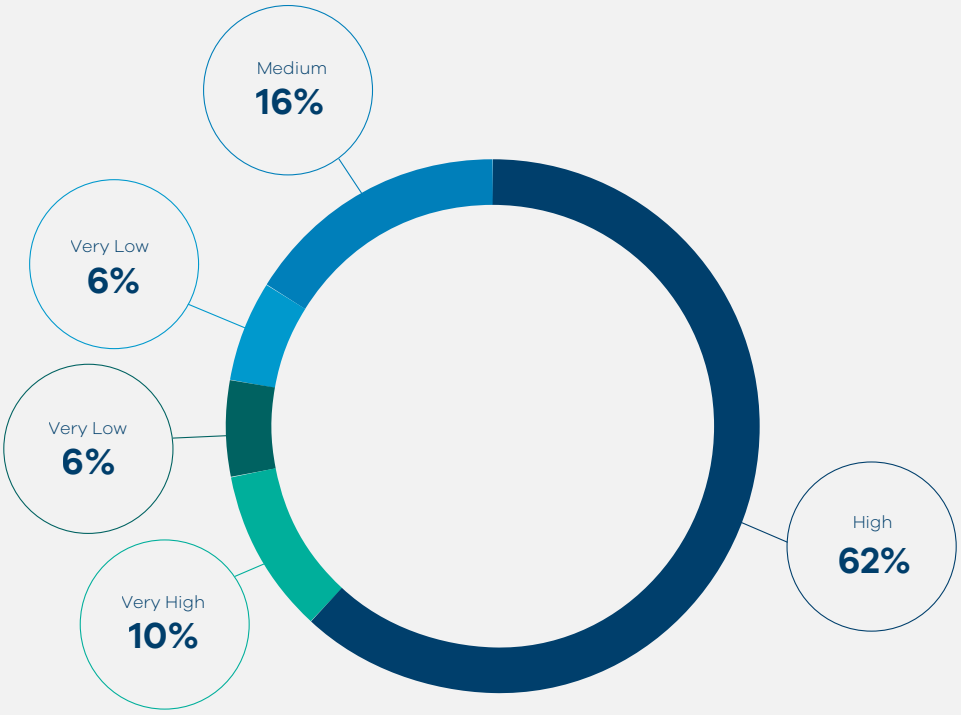


Figure 3: Maturity levels in detecting/responding to signaling attacks

Organizational maturity in detecting and responding to signaling attacks remains inconsistent, despite the growing sophistication of threats targeting SS7, Diameter, and GTP vulnerabilities. Our survey reveals that while 62% of organizations rate their capabilities as "high", only 10% claim "very high" maturity, leaving nearly 28% of respondents admitting to "medium", "low", or "very low" preparedness. This disparity highlights critical gaps in the telecom sector's defenses, where a significant minority remain dangerously exposed to signaling-based breaches.

The data exposes a concerning divide:

- **High/Very High maturity (72%) reflects progress among major operators, likely driven by regulatory pressure and high-profile attacks**
- **Medium/Low/Very Low (28%) suggests smaller providers or lagging enterprises lack the resources or urgency to address signaling threats**

Organizations self-assessing as medium maturity or below require immediate intervention through government-enforced frameworks, cross-carrier threat intelligence sharing, and investment in AI-driven signaling firewalls. Complacency is not an option when signaling attacks undermine national security, financial systems, and critical institutions.

Regulators must mandate annual signaling security audits, ensuring all providers meet stringent detection and response benchmarks. The 28% unprepared cannot remain the weakest link in global telecommunications.

2.4 Barriers in improving signaling security

Addressing key issues helps in improving signaling security for stakeholders to understand technical, regulatory, and operational obstacles such as legacy system vulnerabilities, lack of global standards, limited operator awareness, and cost constraints. By identifying these barriers, stakeholders can develop targeted policy recommendations, strengthen collaboration, and prioritize investments that enhance signaling security.

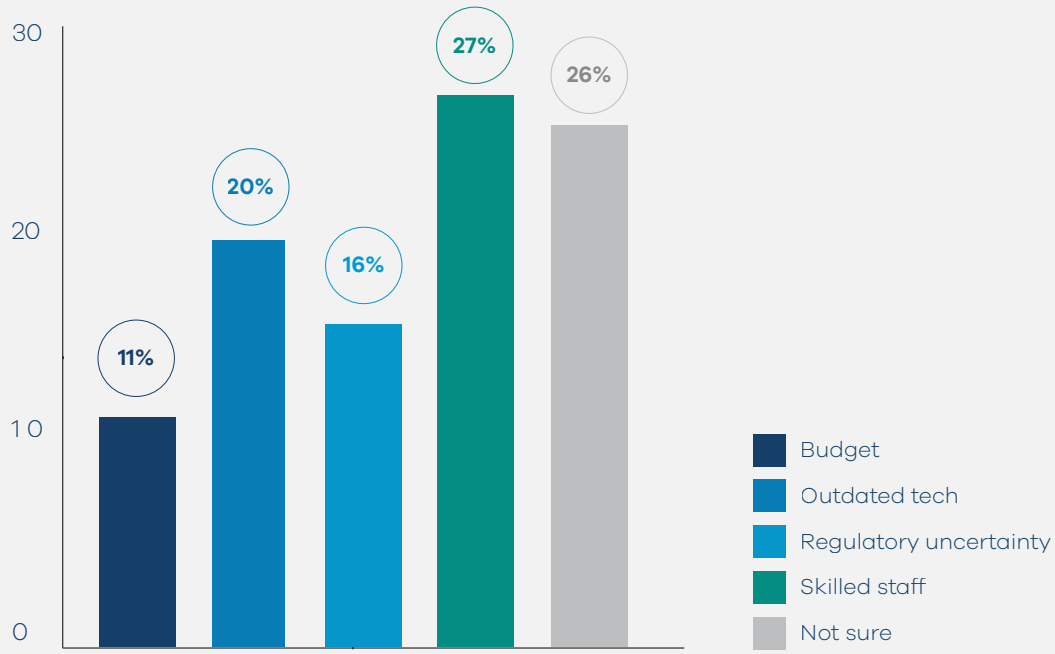


Figure 4: Top challenges in strengthening signaling security

The transition to secure signaling protocols faces systemic roadblocks that demand urgent attention from industry and regulators alike. The survey reveals a fragmented landscape where 27% of organizations cite a lack of skilled staff as the top barrier, a critical shortage in an era of increasingly sophisticated attacks. Close behind, 26% admit they are not sure what impedes progress, exposing dangerous gaps in strategic awareness. Meanwhile, 20% blame outdated technology, 16% point to regulatory uncertainty, and 11% identify budget constraints as key obstacles.

These barriers form a self-reinforcing cycle:

- **Skill gaps delay modernization, forcing reliance on outdated tech that cannot block new attacks**
- **Regulatory uncertainty paralyzes investment, leaving budget disputes unresolved**
- **The "not sure" cohort signals a troubling lack of awareness in addressing known vulnerabilities**

Barriers to signaling security are not just operational challenges; they are national security risks. With 73% of respondents citing tangible obstacles (skills, tech, regulation, or budget), the industry cannot afford incremental fixes. A coordinated overhaul is needed to replace legacy systems, clarify policies, and cultivate the expertise required to defend critical networks.

The cost of addressing these barriers pales in comparison to the cost of a major signaling breach, whether in stolen data, disrupted services, or eroded trust.

2.5 Visibility into interconnect and roaming-based signaling threats

While barriers highlight why operators struggle to modernize signaling defenses, the consequences are most visible in interconnect and roaming environments where threats traverse borders unchecked. Limited skills, outdated systems, and unclear policies leave operators exposed precisely where traffic is hardest to control. To understand the stakes, we must now examine the visibility gap in interconnect and roaming-based signaling threats.

Interconnect signaling, the lifeline of global roaming and cross-carrier communication, remains dangerously impermeable for many telecom operators. While mobile signaling systems such as SS7, Diameter, and GTP facilitate seamless connectivity, they also open doors to roaming fraud, location tracking, and network infiltration.

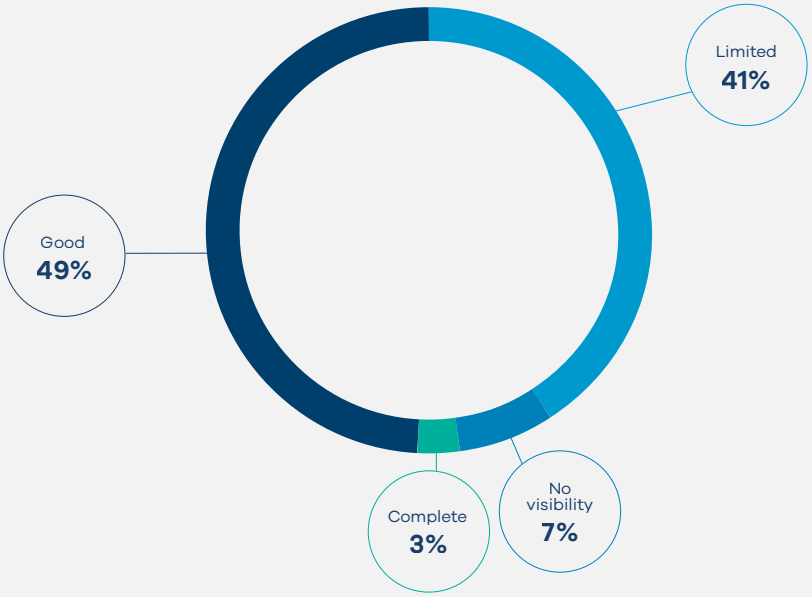


Figure 5: Level of visibility into interconnect signaling threats

Our survey exposes a critical visibility gap: only 3% of organizations claim complete visibility into interconnect threats, while a staggering 49% operate with merely good visibility, leaving nearly half (48%) with limited or no visibility at all. This means one in two operators cannot reliably detect malicious signaling traffic entering their networks from global partners.

The data reveals a fractured defense posture:

- **Complete/Good visibility (52%) reflects progress among large carriers with advanced monitoring, but even good visibility may not suffice against evolving threats**
- **Limited/No visibility (48%) suggests smaller operators or regional players are blind to inbound attacks, making them ideal targets for adversaries**

Telecom alliances and government bodies must treat interconnect visibility as a collective security imperative. The 48% operating in the dark cannot remain the soft target of global telecommunications.

It is therefore imperative to enforce Zero Trust principles for interconnect traffic, requiring authentication and encryption for all signaling exchanges. No provider should route traffic without full threat visibility.

2.6 Vendor effectiveness in mitigating signaling security risks

It is essential to assess industry confidence in vendor solutions because this reveals potential gaps in trust, accountability, and performance among telecom operators and their suppliers. The responses highlight whether vendors are meeting security expectations or if stronger oversight and contractual safeguards are needed. By addressing this, the industry can push for greater transparency, vendor accountability, and improved risk mitigation strategies in signaling security.

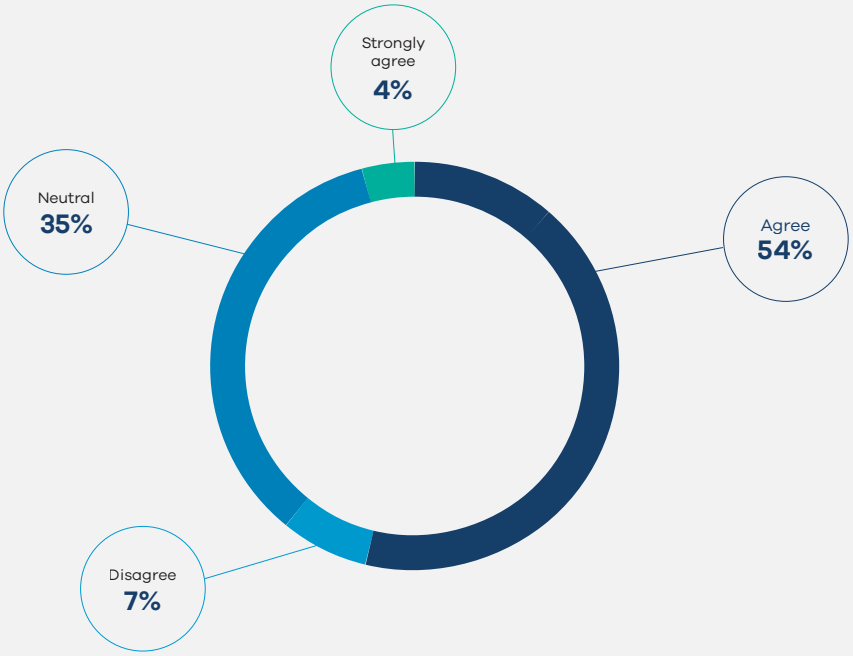


Figure 6: Confidence in vendor's signaling risk mitigation

Vendor solutions are the first (and often only) line of defense against signaling attacks targeting military, government, and financial systems. Organizations that cannot verify vendor effectiveness are blind to intrusions until it is too late. The effectiveness of vendor solutions in mitigating signaling protocol risks remains a critical yet divisive issue in telecom security: while 54% of organizations agree that their current vendor provides adequate protection against SS7, GTP, and Diameter-based attacks, a notable 35% remain neutral, indicating uncertainty or lack of visibility into vendor capabilities. More alarmingly, 7% openly disagreed, suggesting gaps in security postures despite reliance on third-party solutions.

When 42% of telecom professionals are either unsure or dissatisfied with their vendor's signaling protections, it exposes a dangerous reliance on potentially inadequate defenses.

3. Cyber Resilience of Critical ICT Infrastructure

3.1 Assessing readiness and closing resilience gaps

The security of critical ICT infrastructure is threatened by deep-seated vulnerabilities in the global telecommunications network, which are frequently exploited with significant consequences. This chapter explores the nature of these foundational risks, evaluates the industry's current state of readiness, and identifies the key national policies and technical controls required to strengthen cyber resilience.

3.2 The Pervasive Impact and Visibility Gap of Signaling Threats

Signaling-based threats are not a theoretical risk but a tangible reality impacting the core of the telecommunications industry. Survey responses (Figure 8) confirm that a significant majority (53.9%) of organizations have experienced a direct impact on their network resilience or service continuity, ranging from minor disruptions to significant events. Perhaps more telling is the critical visibility gap revealed by the data; the largest single response category was "Not sure" (46.2%). This suggests that many organizations lack the necessary monitoring and detection capabilities to identify these often-stealthy attacks, meaning the true scope and frequency of such incidents are likely underestimated across the industry.

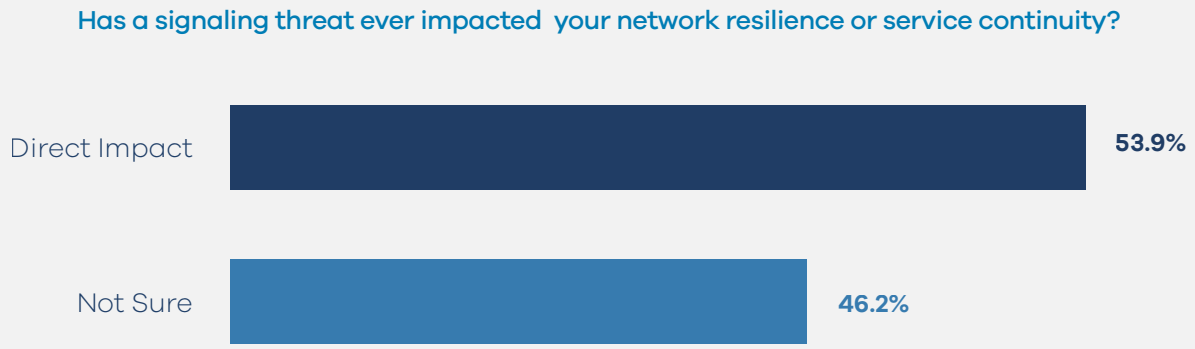


Figure 7: Impact of Signaling Threats on Network Resilience and Service Continuity

3.3 Critical Disparity in Contingency Plan Maturity

The survey results reveal a critical disparity between the existence of contingency plans and their operational readiness. While most organizations have some form of plan, a closer look (Figure 9) reveals a significant preparedness paradox. Only a minority (35%) have a "Comprehensive plan tested regularly," indicating a proven capability to respond to an attack. This leaves majority of the industry relying on "Partial" plans or having no specific plan at all. This widespread dependence on incomplete or untested strategies creates a dangerous false sense of security, leaving organizations vulnerable in a real-world crisis.

Does your organization have contingency plans and redundancy for signaling network failures or attacks?

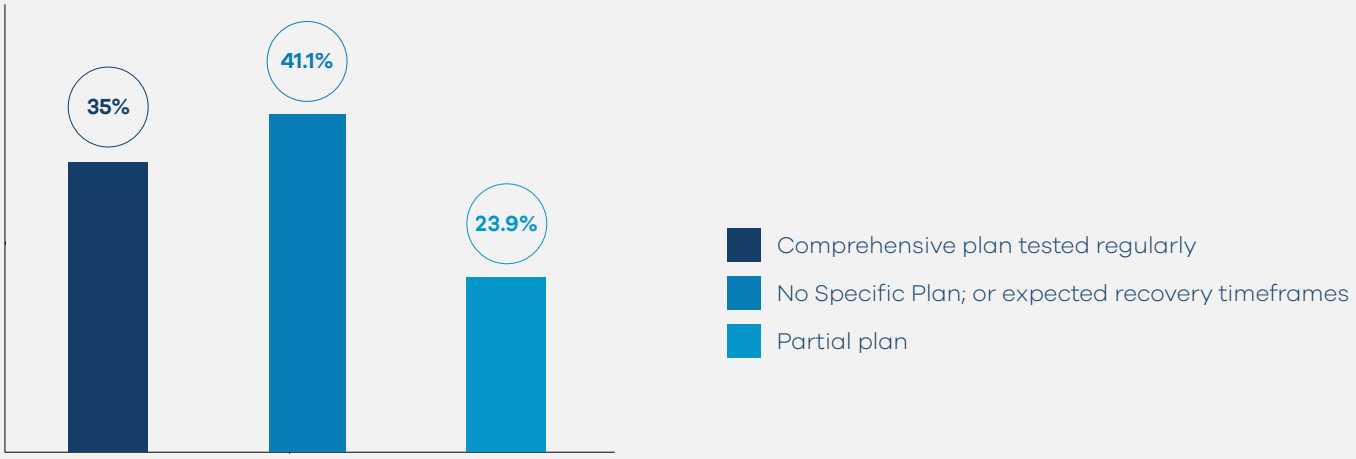


Figure 8: Maturity of Contingency Plans for Signaling Failures or Attacks

3.4 The Infrequent Cadence of Operational Stress Testing

Effective cyber resilience is not achieved through planning alone; it must be validated through rigorous and frequent testing. The survey data on operational readiness (Figure 10), however, shows that this is not standard practice. A mere 19.7% of organizations conduct stress tests on a frequent (quarterly or more) basis. In contrast, a combined 80.3% of respondents admit they test rarely or never. This infrequent validation of security controls and incident response plans means that for most organizations, resilience remains a theoretical concept rather than a proven, operational discipline.

Do you regularely stress-test your network for signaling-based attacks?

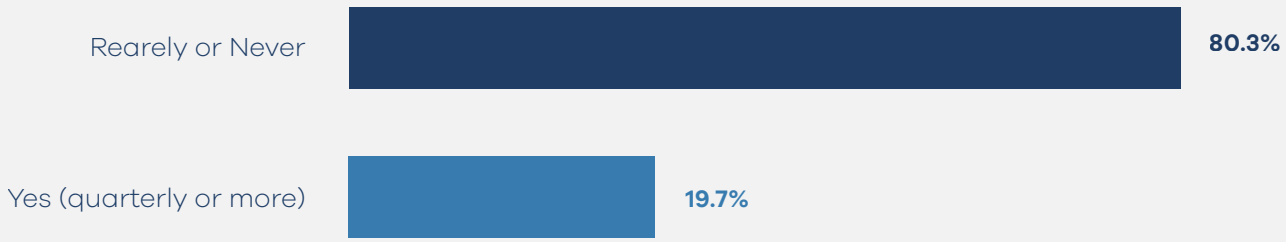


Figure 9: Top Priority Measures to Improve National Signaling Resilience

3.5 An Industry Mandate for National Policy Action

When looking toward the future of telecom security, there is a clear and strong industry consensus that regulatory action is required to elevate the security posture of national critical infrastructure. The survey responses in the below figure show a unified call for specific, mandated technical controls. "Mandated firewalls" emerged as the top priority with 58% support, closely followed by "Signaling encryption standards" and "National Threat sharing" at 48.7%, 42% respectively. Also, "Operator Audits" comes in picture as a considered measure with 31.6% This indicates a collective belief that voluntary measures are insufficient and that a higher, mandatory security baseline is essential for effectively protecting the entire digital ecosystem

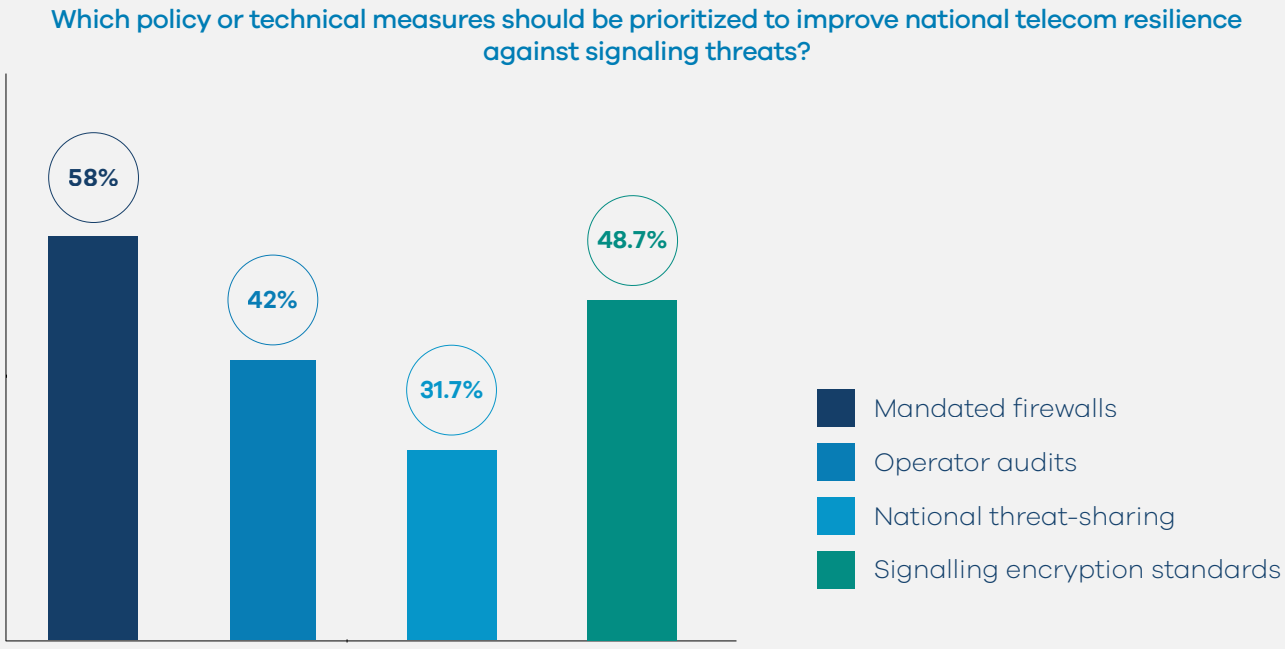


Figure 10: Top Priority Measures to Improve National Signaling Resilience

4. 5G Rollout and Its Cybersecurity Implications

The global rollout of 5G is not just an upgrade in speed and capacity; it is a complete architectural overhaul of mobile networks. Unlike previous generations, 5G introduces cloud-native core networks, software-defined networking, and service-based architectures. These advances deliver operational agility and scalability, but they also fundamentally reshape the cyber threat landscape.

In particular, the signaling layer once primarily governed by SS7, Diameter, and GTP now relies on web-based protocols (e.g., Hypertext Transfer Protocol [HTTP]/2 over Service-Based Interface [SBI]) and containerized microservices, significantly broadening the attack surface and introducing new classes of threats.

This chapter assesses the cybersecurity ramifications of 5G adoption, particularly in relation to signaling security, vendor ecosystems, cloud-native deployment models, and interoperability with legacy infrastructure. The signaling plane has become a critical control vector in 5G, capable of being exploited for DoS, subscriber tracking, session hijacking, and unauthorized network access. Yet, many stakeholders remain underprepared to identify, detect, or mitigate these risks due to gaps in visibility, standardization, and interworking security.

4.1 Global 5G deployment status and security maturity

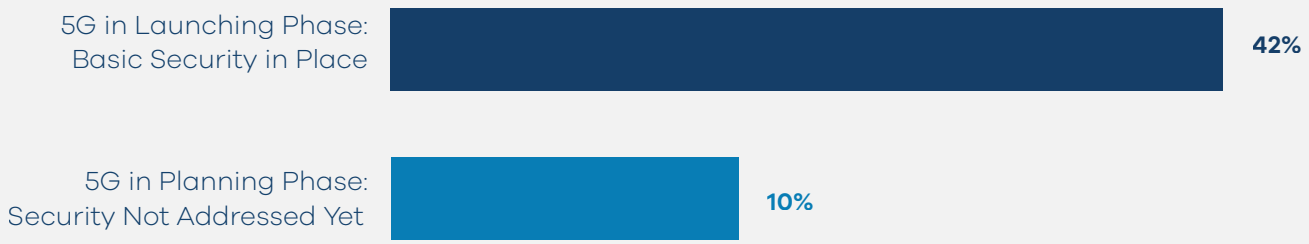


Figure 11: Global 5G deployment readiness

The survey findings provide a glimpse of global readiness when it comes to 5G deployment and its accompanying cybersecurity posture.

According to the survey results, 42% of organizations are still in the rollout phase with only basic security mechanisms in place, indicating that transitional architectures are still being used that blend 4G and 5G technologies. Their current protections rely heavily on legacy defenses and often lack visibility into new 5G-specific risks.

This group of organizations is particularly vulnerable for several reasons:

- **They are still exposed to older, well-known security gaps**
- **Their technology stacks are often built using multiple vendors, which makes coordination and standardization more difficult**
- **They may fall behind regulatory expectations, especially in regions where security requirements are still evolving**

For these operators, there is a clear need for support from both vendors and regulators to strengthen their cybersecurity posture during the rollout phase.

Most concerning is that 10% of surveyed entities are planning their 5G deployments without any current security considerations, representing a clear systemic blind spot. The lack of a consistent security baseline among global 5G adopters poses challenges to international trust and ecosystem resilience.

As 5G underpins critical services – from autonomous transport to smart energy grids and national defense applications – any gaps in its security implementation could have cross-border ripple effects. In this context, regulatory evolution is not optional; it must become a strategic priority. In addition,multi-stakeholder collaboration is essential. Governments, telecom operators, cloud vendors, and equipment manufacturers must work together to define minimum security standards, enable threat intelligence sharing, and embed signaling-layer protection into network design. Initiatives such as national 5G security frameworks, certification schemes, and international alignment on signaling protection must be accelerated.

In short, organizations that proceed without structured security planning could inadvertently become entry points for sophisticated cyber threats. Bridging this gap is critical to ensure that the global 5G ecosystem develops in a secure, trusted, and resilient manner.

4.2 Key security challenges in 5G deployment

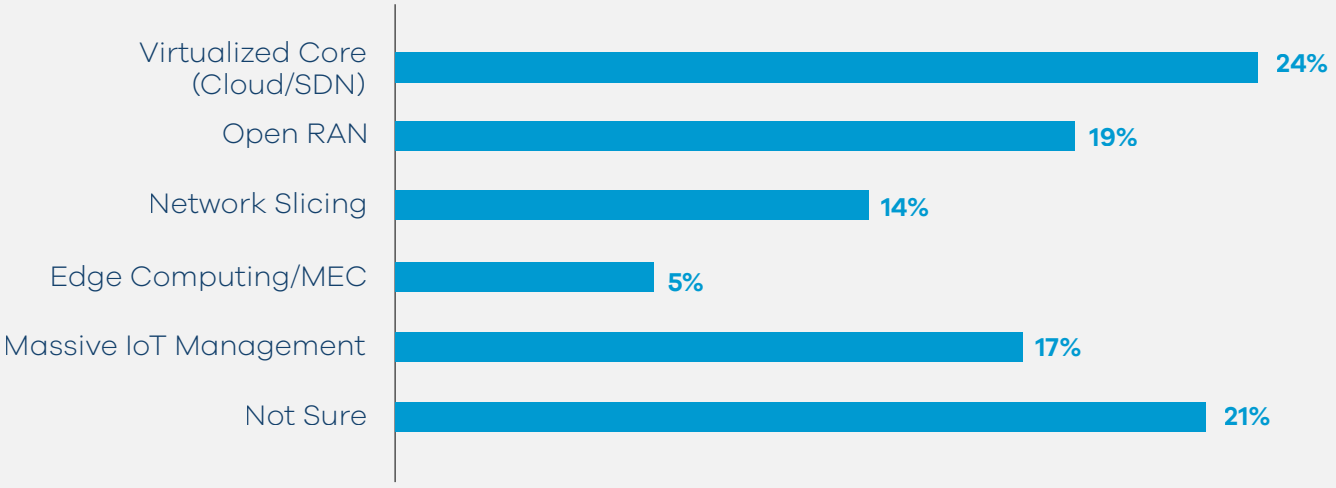
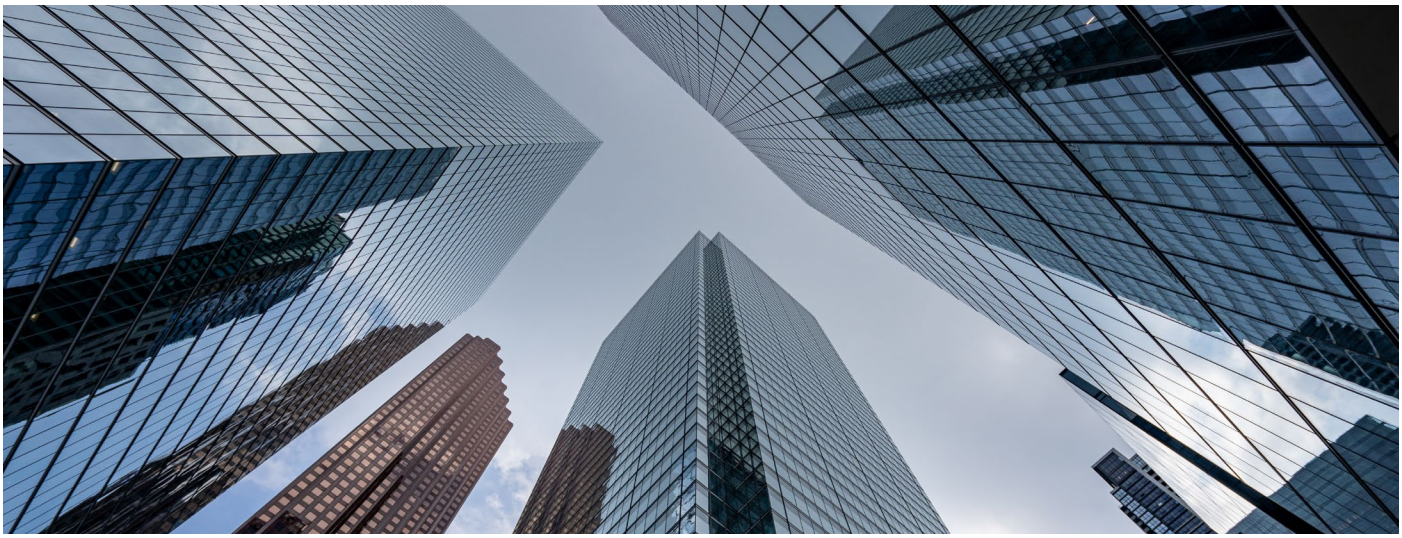


Figure 12: 5G deployment challenges

Note: Numbers might not sum up to 100 due to rounding



4.3 Architectural complexity of 5G pinpointing the greatest security challenges in 5G deployments

As 5G networks reshape the foundation of mobile connectivity, they also introduce a radically transformed architectural landscape – distributed, virtualized, and software-driven. The survey identified which aspect of this new architecture introduces the greatest cybersecurity challenge, reflecting broad concern across multiple architectural domains and highlighting the multifaceted nature of securing 5G.

A plurality of respondents (24%) pointed to the virtualized core, including cloud-native functions and SDN, as the most pressing security challenge. This finding aligns with industry observations that virtualization and cloudification expand the attack surface, introduce complex dependencies, and demand a level of agility in threat response that many traditional telecom security frameworks are not yet equipped to handle. Cloud platforms, when misconfigured or poorly segmented, can become conduits for lateral movement by threat actors.

Open RAN (19%) emerged as the second most cited challenge given its reliance on open interfaces, disaggregated components, and a multi-vendor environment. While Open RAN offers vendor diversity and cost benefits, it also raises new concerns around supply chain security, trust boundaries, and lack of standardized security oversight - particularly in less mature implementations.

Massive IoT management (17%) and network slicing (14%) are also seen as significant security pain points. The proliferation of IoT devices introduces heterogeneity and scale, making centralized control and consistent policy enforcement difficult. Meanwhile, network slicing, though intended to isolate use cases securely, can create new inter-slice vulnerabilities if not managed with rigorous orchestration and policy frameworks.

Interestingly, only 5% of respondents selected edge computing/MEC, which could reflect either a perception of maturity in edge security or a lack of deep visibility into its associated risks. Notably, 21% of respondents were unsure which aspect of this new architecture introduces the greatest cybersecurity challenge, signaling a broader need for security education and shared technical understanding across the telecom ecosystem.

These findings are echoed by independent research from Forrester, which recently reported that 36% of global technology decision-makers responsible for networks, telecom, edge, and IoT identified security as their top concern in deploying private 5G networks. Among that 36%, concerns centered on threats from external/internal hackers, malicious radio frequency (RF) jamming, lack of control of end devices, accidental RF interface, and risk of installation.

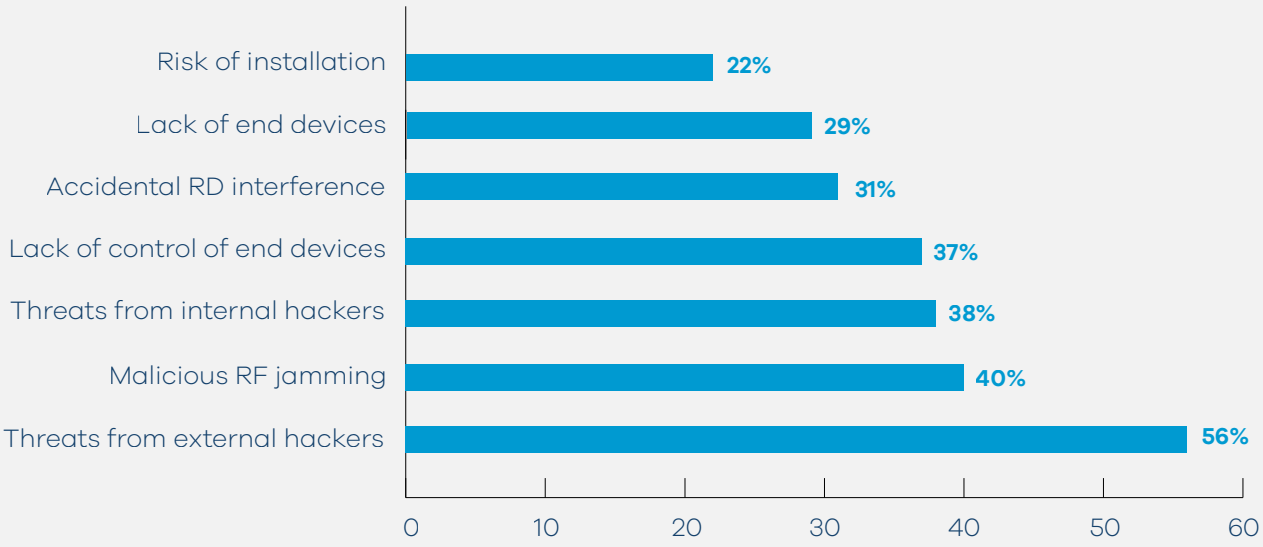


Figure 13: 5G deployment security concerns among 36% of global technology decision-makers

These results highlight that regulators and national cybersecurity authorities should prioritize guidance and enforcement in these high-risk areas, especially as more critical services and government functions become dependent on 5G. Addressing these architectural challenges proactively is key to ensuring service continuity and long-term ecosystem resilience in the 5G era.

Moreover, this indicates a critical need for:

- **Cross-functional education for security and network architects**
- **Development of industry-wide security risk heatmaps**
- **Inclusion of cybersecurity perspectives in 5G procurement and design decisions**

4.4 Supply chain risks in 5G deployment

Figure 14: Supply chain risks in 5G deployment

Most telecom leaders acknowledge the risks tied to 5G supply chain vulnerabilities – 83% show some level of concern. However, only a small portion (17%) is highly concerned, signaling a gap between awareness and tangible risk mitigation.

This disconnect may be due to:

- **Limited insight into what is happening beyond immediate suppliers**
- **Overconfidence in vendor compliance or certifications**
- **Assumptions that government bans or restrictions can sufficiently manage the risk**

The largest group (36%) describes itself as "slightly concerned," implying the issue is known but not urgent. This mindset is risky.

Modern 5G networks rely heavily on global software and hardware ecosystems. Small, hidden vulnerabilities, whether in a software library, a firmware update, or an offshore development team, can quietly create major weaknesses.

Without proactive attention, this could lead to:

- **Invisible vulnerabilities embedded in network components**
- **Delayed detection of malicious code or unauthorized access**
- **Higher costs to fix systemic issues after deployment**

4.5 Biggest concerns regarding 5G signaling threats

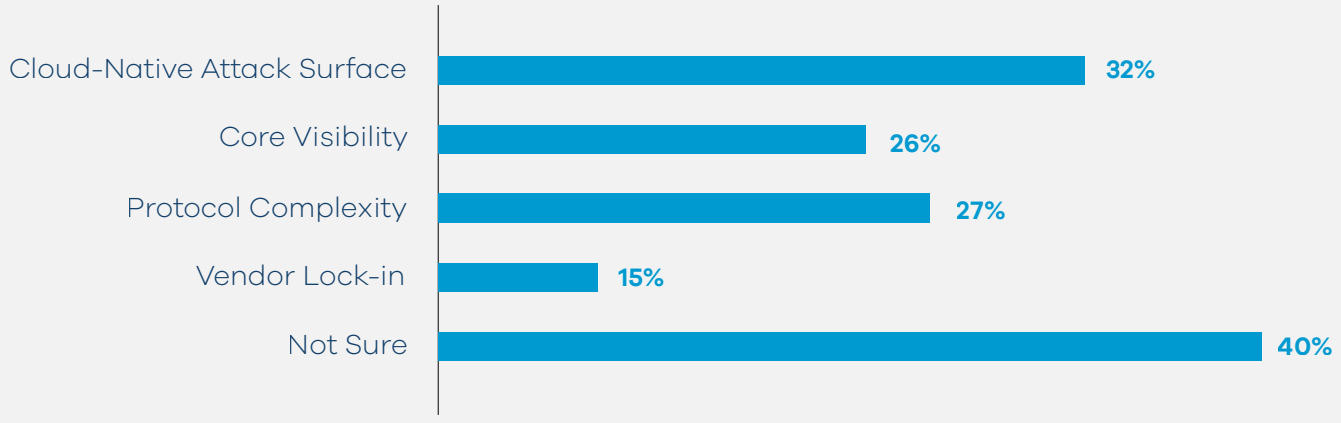


Figure 15: Biggest concerns regarding 5G signaling threats

5G signaling introduces a new class of cybersecurity challenges due to its reliance on cloud-native infrastructure, distributed architectures, and complex protocols.

To explore industry perspectives on where these threats are most acute, our survey asked participants to identify their biggest concern regarding 5G signaling threats. The results reveal a fragmented landscape of understanding and readiness, with no single threat vector dominating the narrative but a few clear areas of heightened concern.

The most striking insight is that 40% of respondents indicated they are not sure what their biggest signaling-related concern is. This indicates a significant awareness gap in the ecosystem and suggests that education, simulation, and red-teaming exercises are urgently needed to help organizations identify and understand where their most vulnerable points may lie.

Among those who identified specific concerns, 32% cited the expanded cloud-native attack surface as the biggest threat. The adoption of microservices, containerized network functions (CNFs), SBA, and distributed cloud environments has redefined traditional signaling boundaries, exposing previously internal signaling pathways to external attack vectors. Misconfigurations, weak inter-service authentication, and unsecured APIs are all potential entry points for attackers.

Protocol complexity was selected by 27% of participants as a major concern, highlighting the steep learning curve associated with 5G signaling layers and the challenges in securing dynamic and loosely coupled protocol stacks. Unlike legacy SS7 or Diameter signaling systems, 5G signaling leverages multiple protocol layers, each with its own set of stateful interactions, error handling, and security assumptions. When improperly implemented or monitored, these protocols can become fertile ground for fuzzing attacks, state misalignment, or session hijacking.

Vendor lock-in, though selected by a smaller portion of participants (15%), still reflects a strategic risk for organizations looking to maintain control over their 5G evolution. Proprietary signaling implementations, opaque software stacks, or limited security telemetry from vendor components can hamper effective threat detection and response, especially in highly sensitive environments like defense, critical infrastructure, and public safety.

Together, these findings point to the need for multi-layered 5G signaling security strategies that address both the technical and organizational dimensions of risk. CSPs, regulators, and vendors alike must collaborate to develop standards, threat models, and interoperability frameworks that reduce ambiguity and strengthen defense across the 5G signaling ecosystem.

4.6 Expert insights from the field

As part of the research for this flagship report, an interview was conducted with a senior expert working closely with MNOs in the domain of signaling security. His observations provided practical, field-level insights that complement the broader survey data and literature review, adding depth to the analysis.

From a vendor perspective, the expert noted a persistent reluctance among telecom equipment providers to implement critical security measures such as endpoint detection and response (EDR) solutions, integration with security information and event management (SIEM) platforms, and the provision of signaling-level logs from network elements (NEs). This lack of transparency and integration, he stressed, represents a significant barrier to effective monitoring and threat detection. According to the expert, addressing these gaps will likely require intervention at the regulator or standardization-body level to ensure vendors are mandated to provide such capabilities.

Regarding operator-level recommendations, the interviewed expert emphasized the importance of embedding AI-driven, protocol-aware monitoring across all 5G planes. Such monitoring would enable real-time visibility, automated incident response, and enhanced compliance across multi-vendor, cloud-native network environments. Additionally, he identified a critical shortage of telecom cybersecurity professionals, highlighting the need for targeted certification programs to cultivate a skilled workforce capable of defending next-generation networks against advanced threats.

5. Recommendations

The vulnerabilities in mobile signaling protocols are among the most critical yet overlooked threats to global telecommunications.

Survey evidence, reinforced by external research, shows 88% of experts recognize signaling threats as serious national security concerns, yet nearly half of operators have limited or no visibility at all of interconnect vulnerabilities and only 58% deploy basic defenses.

This is not a theoretical risk. Signaling attacks enable mass surveillance, financial fraud, and infrastructure disruption. The industry must shift from reactive compliance to proactive resilience, with targeted action from all stakeholders.

5.1 For MNOs

MNOs remain on the front line of signaling security. As the stewards of subscriber trust and guardians of national communications infrastructure, their readiness to detect, mitigate and adapt to evolving threats is critical. The following actions are designed to strengthen operational resilience and ensure signaling security remains a board-level priority.

1. Embed security from the start

- **Build signaling-layer protections into network architecture from the planning phase, not as retrofits**
- **Treat Security Edge Protection Proxy (SEPP), SBA controls, and cloud-native protections as mandatory, not optional**

2. Strengthen operational defenses

- **Conduct signaling-specific threat modeling and red-team exercises (e.g., rogue Network Function [NF] registration, tunnel hijacking)**
- **Deploy AI-driven monitoring, API gateways, and behavioral analytics to baseline signaling behavior**
- **Mandate telemetry exports from all network functions, regardless of vendor**

3. Accelerate 5G security maturity

- **Transition to standalone (SA) architectures with integrated security**
- **Harmonize governance across multi-vendor environments to eliminate weak links**

4. Implement supply chain and vendor oversight

- **Demand Software Bill of Materials (SBOM) from all suppliers**
- **Monitor vendor components in live networks for abnormal behavior**
- **Participate in telecom-specific information-sharing groups for early warning on threats**

5. Engage third-party governance

- **Adopt modular, multi-vendor architectures to retain flexibility and avoid reliance on a single supplier. Modular solutions enable scalable additions or replacements of components, reducing vendor lock-in risks while ensuring seamless operation**
- **Implement robust third-party risk management (TPRM) tailored for telco environments such as mapping dependencies, enforcing contractual safeguards (e.g., software escrow), continuous monitoring, and stress-testing vendor resilience**

5.2 For vendors

Vendors shape the security capabilities embedded in network equipment and software. Their design choices, patch cycles, and interoperability commitments directly influence the security posture of the global telecom ecosystem. These recommendations focus on fostering secure-by-design principles and accelerating innovation to address emerging attack surfaces.

1. Deliver secure-by-design commitments

- **Embed signaling-layer protection directly into products, avoiding "bolt-on" third-party fixes**
- **Provide documented proof of security checks and component provenance**

2. Ensure open and interoperable security

- **Support open telemetry standards (e.g., OpenTelemetry, NetFlow, packet captures [PCAPs])**
- **Offer full mapping of internal signaling states and inter-NF flows**
- **Ensure detection thresholds and mitigation logic are transparent and configurable**

3. Reduce integration friction

- **Deliver solutions that integrate smoothly across hybrid or transitioning networks**
- **Build tamper-proof firmware and hardware update processes**

5.3 For regulators

Policymakers and regulators set the tone for compliance, resilience, and cooperation. In a landscape where signaling threats transcend borders, their role in defining common baselines and mandating incident reporting is essential. The following guidance aims to bridge governance gaps and align industry practices with national and global security goals.

1. Establish national signaling security baselines

- **Mandate signaling-level monitoring, threat reporting, and regular audits as part of licensing**
- **Require maturity assessments for signaling security in spectrum allocation and rollout approvals**

2. Enforce security transparency and accountability

- **Launch certification frameworks for signaling security implementation**
- **Mandate SBOM disclosure and supply chain security verification for all critical telecom gear**

3. Strengthen national and cross-border defenses

- **Promote vendor diversity and interoperability to reduce single-vendor dependence**
- **Require operator participation in threat intelligence sharing and inter-operator penetration tests**
- **Fund national training programs on 5G control plane security**

5.4 For academia and industry alliances

The global cybersecurity community–spanning researchers, standardization bodies, and information-sharing groups–provides the connective tissue for a proactive defense posture. Collaboration across public and private sectors can help identify threats early and disseminate countermeasures effectively. The recommendations below focus on sustaining a collective defense model and advancing research into next-generation signaling threats.

1. Advance research on evolving signaling threats

- **Expand research and development on securing Open RAN, network slicing, massive IoT management, and 6th Generation cellular network technology (6G)**
- **Develop behavioral analytics models and AI-driven threat detection for signaling layers**

2. Foster collaborative intelligence

- **Maintain active cross-border signaling threat exchanges**
- **Share anonymized incident data to reduce dwell time and improve collective response**

5.5 Five-Point Policy Roadmap to strengthen critical ICT infrastructure

The Five-Point Policy Roadmap presented here distills the evidence into a set of concrete, actionable steps that policymakers can adopt to strengthen national cyber resilience. Each point links directly to gaps identified in our survey and expert interviews, ensuring the roadmap reflects both strategic priorities and frontline realities.
This roadmap is not just a technical prescription — it is a governance blueprint designed to reduce systemic vulnerabilities, improve cross-border trust, and safeguard the digital services that societies and economies now depend on daily.

Securing critical ICT infrastructure, particularly telecom signaling systems, requires a clear, actionable policy framework that aligns technical defenses with national security priorities.

This roadmap distills complex security needs into five targeted policy actions designed to close existing gaps, future-proof networks against emerging threats, and foster greater public-private cooperation. Each point is both a strategic direction and a practical step toward a more resilient cyber ecosystem.

1. License-grade signaling firewalls and anomaly detection
Require SS7, Diameter, and GTP firewalls with minimum 30-day log retention in telecom licenses.

2. End-to-end encryption for inter-operator links
Enforce GSMA SECURE (Diameter over IPsec) and 5G SEPP (mutual TLS) adoption; target 40% coverage by 2026 and 100% coverage by 2028.

3. 24-hour incident reporting
Fast, anonymized threat sharing should be a regulatory requirement.

4. Annual regulator-observed red-team stress tests
Perform simulated attacks under supervision to validate failover and response readiness.

5. Board-level composite resilience index (CRI)
National resilience targets should be tied to executive accountability, with public reporting.

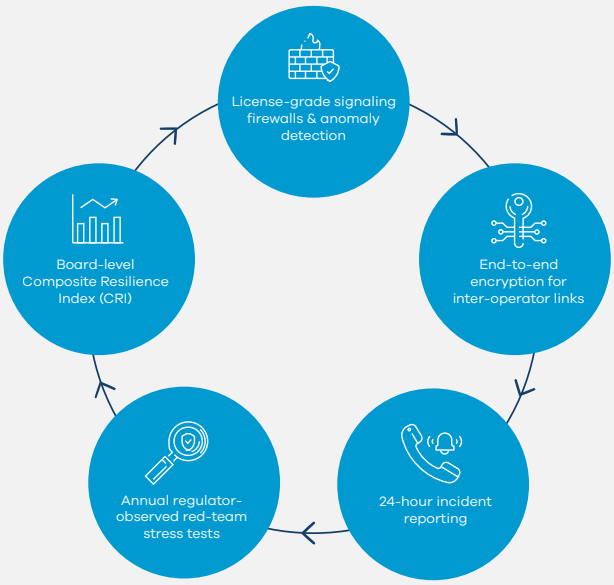


Figure 16: Five-Point Policy Roadmap to harden critical ICT infrastructure

The choice is clear: secure the signaling layer now or face irreversible breaches to national and economic stability.

The evidence is conclusive and the blueprint exists – the remaining gap is urgency.

Conclusion

This flagship report calls for greater executive awareness, policy inclusion, and investment in signaling-layer resilience. As mobile networks become central to national infrastructure – powering everything from cyber identity systems to emergency services – nations must ensure this foundation is secure.

Ignoring signaling security is no longer a viable option. Strategic, non-technical leaders have a crucial role to play in closing this gap by integrating signaling risks into national strategies, establishing oversight mechanisms, and fostering international cooperation to protect the trust that underpins our global cyber future.

The findings of this flagship report underscore a pressing reality: signaling security remains both a foundational enabler of trust in mobile communications and a critical vulnerability within evolving telecom ecosystems. Our survey results reveal a significant gap between awareness and action, with many stakeholders acknowledging the risks but lacking the governance, investment, or cross-industry collaboration required to address them comprehensively.

This report calls on industry leaders, policymakers, and solution providers to move beyond reactive measures toward a shared strategic vision for signaling security. The accompanying recommendations and audience-specific actions provide a practical path forward, but success will depend on sustained commitment, transparent information-sharing, and proactive investment. The near future will define whether mobile networks remain trusted critical infrastructure or whether their foundational trust is eroded. The choice, and the responsibility, rests with all of us.

Bibliography

1. Industrial Cyber. Moody's Cyber Heat Map Flags Extreme Cyber Risks for Critical Infrastructure, Impacting Telecommunications and Airlines. June 7, 2023.
2. Khaleej Times. No More OTPs: UAE Banks to Switch to App Verification Starting Today. July 25, 2025.
3. Juniper Research. Data Roaming Fraud to Accelerate, Reaching $8bn Globally by 2028, as Bilateral 5G Roaming Agreements Exacerbate Losses. July 2023.
4. Hackers Arise. Chinese State-Sponsored Hackers Inside the US Mobile Telecom System: Mobile Telecom Companies Vulnerable to SS7 Vulnerability. Accessed September 2025.
5. European Union Agency for Cybersecurity (ENISA). Interconnect Security: Security Measures for SS7 and Diameter. Heraklion, Crete: ENISA.
6. European Union Agency for Cybersecurity (ENISA). Telecom Security Incidents 2024. Heraklion, Crete: ENISA, 2025
7. The White House. National Cybersecurity Strategy. Washington, DC: The White House, 2023.
8. GSMA Intelligence. GSMA Intelligence Data & Analysis. Accessed September 2025.
9. GSMA. FS.36: 5G Interconnect Security. London: GSMA, 2021.
10. 3GPP. TS 33.522: 5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP). 3rd Generation Partnership Project (3GPP), 2022
11. Cisco Press. SS7 Security and Fraud. Accessed September 2025.

GLOBAL CYBERSECURITY FORUM

stc