Telco security landscape and strategies:

Northern Africa

Innovating to protect

GSMA Intelligence

GSMA

GSMA Intelligence

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA: @GSMA

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

gsmaintelligence.com

info@gsmaintelligence.com

Published October 2024

Authors

Tim Hatt, Head of Research and Consulting
James Joiner, Lead Analyst
Silvia Presello, Lead Analyst

Contents

Executive summary

Northern Africa's mobile evolution

The telecoms industry in Northern Africa continues to undergo significant transformation, driven by the rapid uptake of 4G services in recent years. 4G adoption in the region reached 35% of total mobile connections at the end of 2023. This will reach 45% in 2025, overtaking 3G as the most widely adopted mobile network generation in Northern Africa.

The shift to 4G (and eventually 5G) will underpin increased use of online services in the region. This provides new opportunities to drive digital transformation and socioeconomic advancements. However, the rapid pace of change combined with ongoing challenges with online safety and digital skills makes the region an attractive target for fraud and cyberattacks. Understanding, mapping and mitigating security threats (both existing and upcoming) in an objective, speedy and effective manner is therefore essential.

Operator perceptions of security readiness

The GSMA Intelligence survey on telecoms operator security highlights that around 80% of Northern African operators rate their mobile network defences as strong or very strong, in line with the global average. However, within that total, only 22% of operators rate those network defences as very strong, compared to a global average of 38%. This suggests that confidence in mobile network defences can be further increased in the region.

The level of confidence among Northern African operators in their security defences varies according to type of attack. Operators are confident in their ability to defend against ransomware and smishing/phishing attacks, with more than 85% considering themselves ready or somewhat ready. However, this confidence wanes when it comes to other threats. For instance, less than a third of operators feel ready or somewhat ready to defend against signalling and interconnect attacks, or those targeting virtualised interfaces. This is a key takeaway for telecoms security vendors looking to support operators in developing more robust security defences.

Investing in network security

Operators in Northern African have invested in a range of security tools to protect their customers and operations. SMS and voice firewalls are a key part of an operator's defence against fraud and malware attacks, while operators are investing in Signalling System #7 (SS7) and Diameter signalling firewalls to safeguard their interconnect and signalling networks. Leading operators in the region are also combining their network operations centres (NOCs) and security operations centres (SOCs) to improve coordination and streamline threat detection and response as the IT and network domains converge.

These innovations are being implemented alongside non-technical measures. For example, operators have established a range of security controls targeted at employees, including comprehensive security training, staff vetting, additional administrator controls and operating a 'least privilege regime'. Operators are also helping develop cybersecurity skills and awareness among customers. These steps are important as people can often be the weakest link in the security risk profile.

Industry tools and collaboration

Industry-wide collaboration is essential to protect against heightened threat levels. As a global organisation unifying the mobile ecosystem, the GSMA provides a wide range of support to its members. Examples include the following:

- **Network Equipment Security Accreditation Scheme (NESAS)** – This audits and tests network equipment vendors and their products against a security baseline. It can help avert fragmentation of regulatory security requirements by providing a globally recognised, robust security baseline that all stakeholders can adopt and adhere to.
- **Mobile Cybersecurity Knowledge Base (MCKB)** – This provides guidance on mobile security risks and mitigation measures. It combines the cybersecurity knowledge of the mobile ecosystem (including mobile operators, vendors and regulators) with input from public sources such as 3GPP, ENISA and NIST.
- **GSMA Baseline Security Controls** – Part of the MCKB, these provide a comprehensive set of security measures for mobile networks and can form the baseline for any mobile network security risk assessment.
- **Telecommunication Information Sharing and Analysis Centre (T-ISAC)** – This enables operator members to communicate cyber risk data, including new indicators of compromise, in real-time. It also allows operators to share best practices with each other in a trusted environment.

1

Research in context: security in 2024

1.1 Purpose

The security threat landscape across telecoms and the broader technology industry continues to evolve at a rapid pace. Security threats are an assumed constant in the digital world. This has been the case since the PC era of the 1980s. However, risk levels are higher now.

Trends such as moving towards software-defined mobile networks, AI and digitisation across the economy have increased the attack surface and lowered technical barriers to launch attacks. Risk impact is also now higher, with cyberattacks having severe consequences including brand damage, data breaches, system outages and loss of business. Overall, the world is becoming a more dangerous place, with cyberattacks seen as an effective – if sometimes clandestine – means for malign actors to exact economic damage or compromise national security.

This is the second in a five-part series on security innovations in the telecoms industry. The report series aims to:

- evaluate the threat landscape for telecoms operators
- track where and why things have changed in the threat landscape – for better or worse
- discuss innovation and best practice in solutions to mitigate or repel threats
- examine potential future scenarios and how to get ahead of the curve.

The first report focused on Latin America and established a view on operator perceptions of their own security readiness, vulnerabilities and routes to pre-empting new attack vectors. This report focuses on Northern Africa, broadly defined as countries north of the Sahel, though with some in the Sub-Saharan region of the African continent.[1]

Security is very much a common good. This research series is therefore intended to be a resource for operators, their suppliers and partners, and governmental agencies cognisant of the foundational role mobile networks play in modern economies.

1.2 Approach and timelines

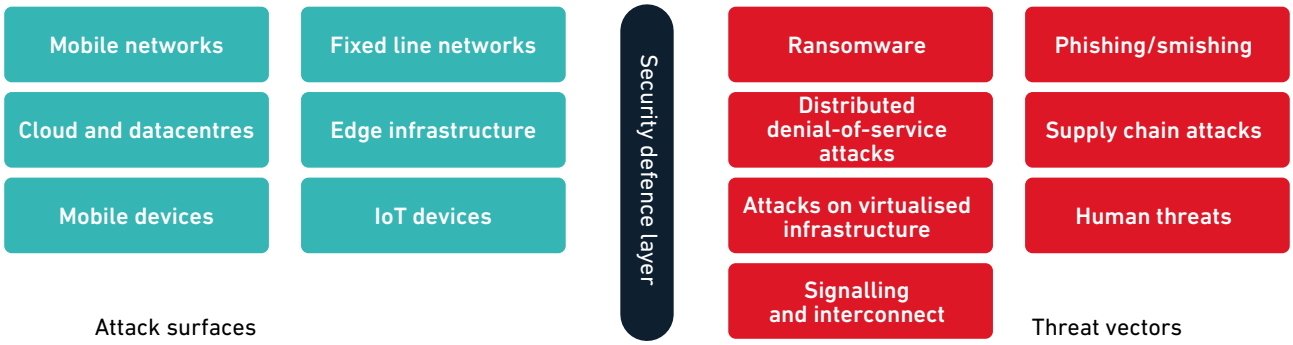
The research uses a mixed methodology. Data is drawn from multiple sources:

- a new survey of telecoms operators around the world (n=100)
- reported data from the GSMA Intelligence database
- an index to quantify security readiness against various attack vectors
- specialist, third-party sources.

The metrics are explained in Chapter 2, while definitions and examples of attack vectors are provided in the Appendix. GSMA Intelligence also interviewed telecoms operators and other security players in the region to produce a set of case studies. These highlight technology innovation and engineering to bolster security in mobile networks, the compute stack and end-user devices.

Figure 1

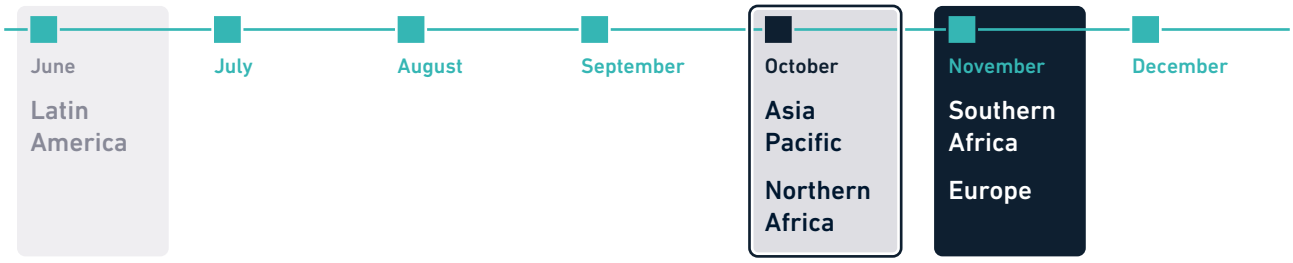
A simplified view of security attack surfaces and threat vectors



Source: GSMA Intelligence

Figure 2

Timeline for report series (2024)



Source: GSMA Intelligence

1 A full list of countries is provided in the Appendix.

2 The telecoms environment and its bearing on security

2.1 The operating environment in Northern Africa

The customer base for mobile internet in Northern Africa has grown significantly, driven by continued rollout of 4G networks and buoyant consumer demand. The latter has been helped by falling smartphone and data tariff costs relative to income and the growing availability of content in what are primarily mobile-only internet markets.

By the end of 2023, the number of mobile connections in the region had reached almost 1 billion. Smartphone penetration stood at 90% of total mobile connections. Approximately half the mobile customer base still relies on 3G networks, but there is a gradual shift to 4G.

The adoption of 5G in the region is limited. It is forecast to account for just 1% of total mobile connections by the end of 2024. The lack of 5G adoption reflects infrastructure gaps and a challenging spectrum situation for operators. However, this is expected to improve with 5G spectrum assignments scheduled for several countries in the region, including Ethiopia and Morocco.

As regional/national digital transformation and cybersecurity strategies are released or updated,[2] the requirement to deploy 5G services will gain momentum. With more 5G spectrum auctions expected to take place in the coming years, 5G deployments and take-up will accelerate, though at a slower pace than in other parts of the world. GSMA Intelligence forecasts that 5G adoption will reach just over 20% of mobile connections by 2030, compared to a global average of 56%.

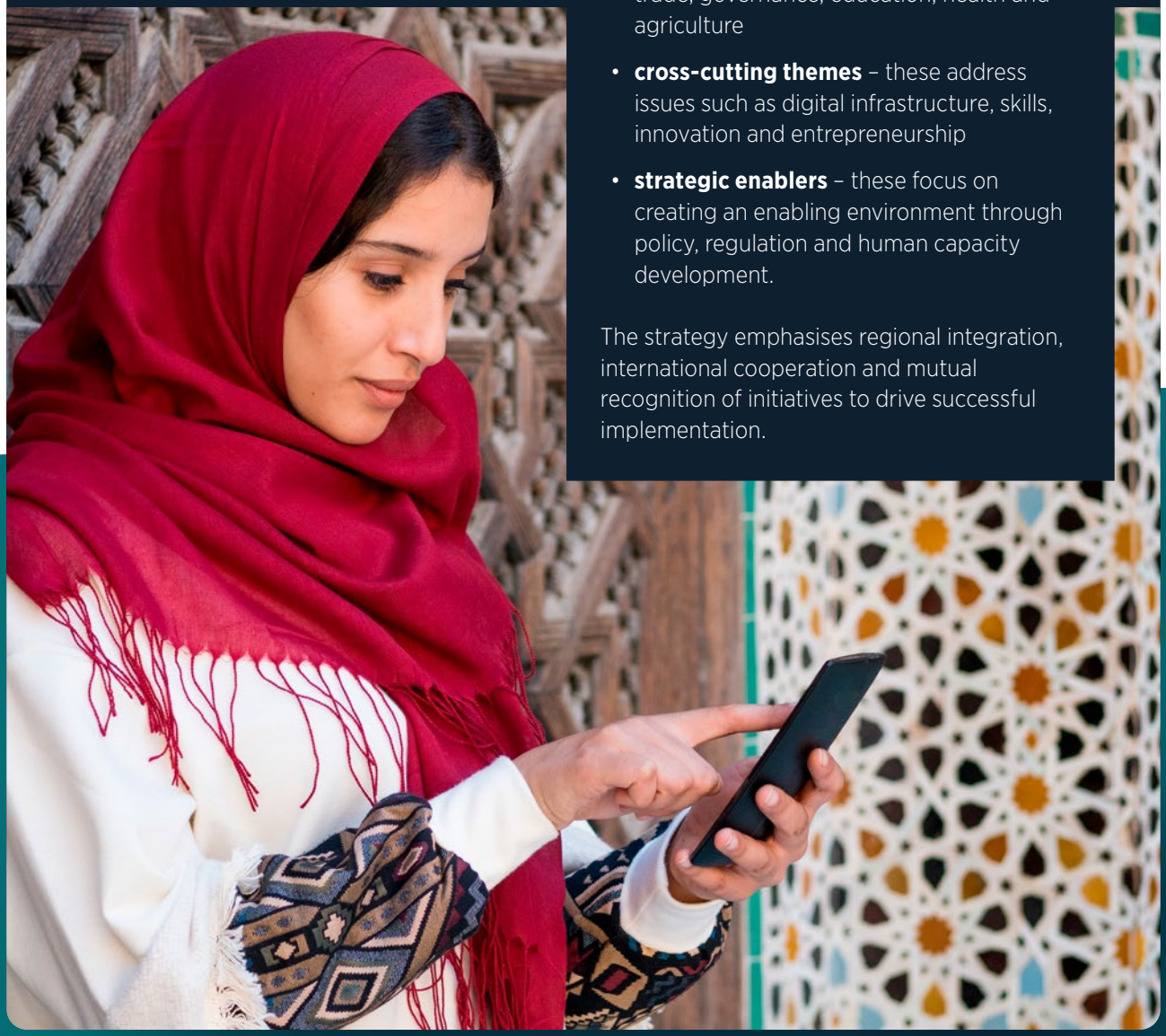
The Digital Transformation Strategy for Africa (2020–2030)

The African Union (AU) has developed the Digital Transformation Strategy for Africa to guide the continent towards an integrated and inclusive digital society and economy. The strategy aims to improve quality of life for Africans by harnessing digital technologies and innovation.

Key components include:

- **foundation pillars** – these encompass critical areas such as digital content and applications, digital ID, emerging technologies, cybersecurity, privacy, research and development, digital industry, trade, governance, education, health and agriculture
- **cross-cutting themes** – these address issues such as digital infrastructure, skills, innovation and entrepreneurship
- **strategic enablers** – these focus on creating an enabling environment through policy, regulation and human capacity development.

The strategy emphasises regional integration, international cooperation and mutual recognition of initiatives to drive successful implementation.

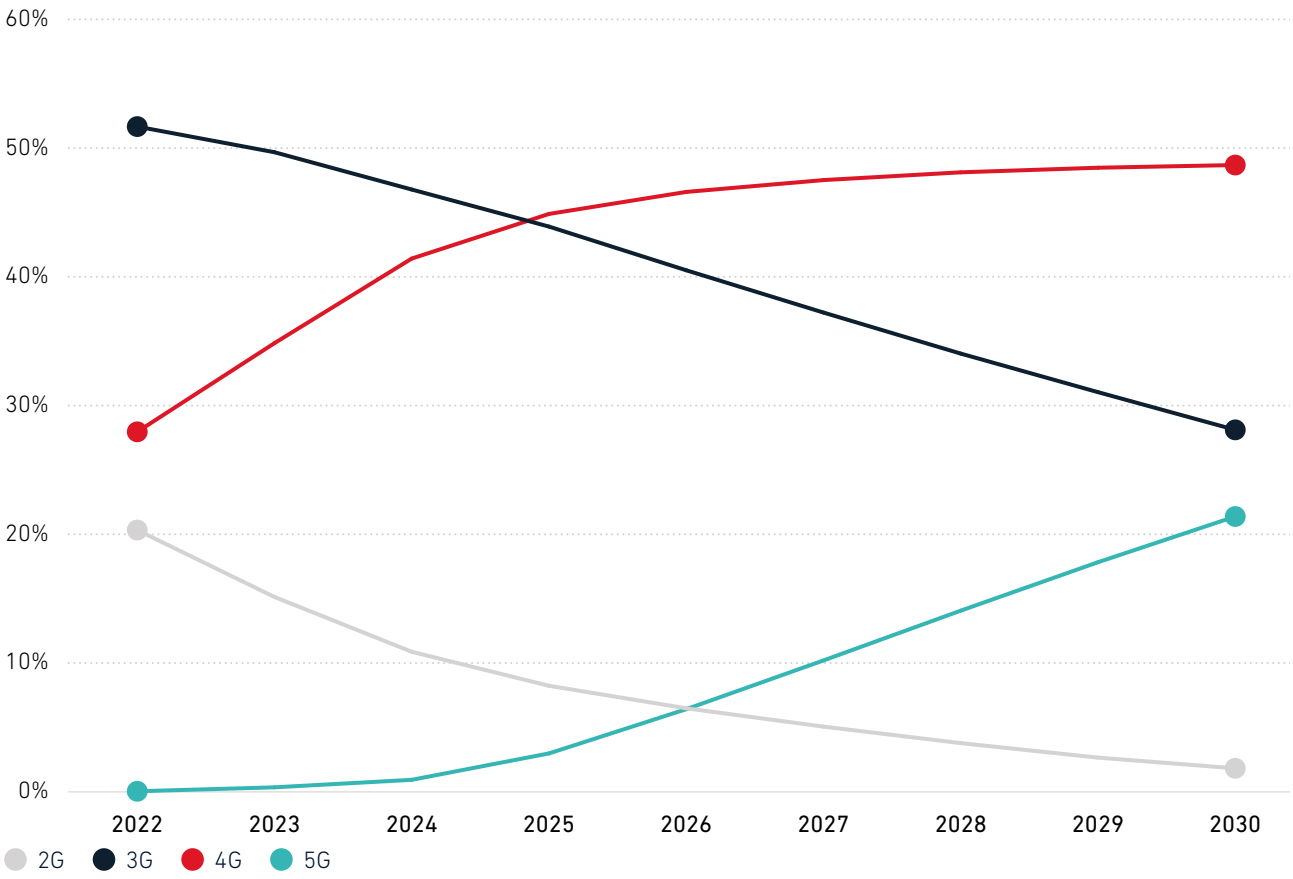


2 Morocco, Ethiopia and the Democratic Republic of Congo are among the Northern African countries updating their digital strategies.

Figure 3

Previous generation technologies continue to dominate in Northern Africa, with 5G reaching 21% by 2030

Percentage of total mobile connections



Source: GSMA Intelligence

Table 1

Country-level subscriber and technology trends for key markets in Northern Africa

	Algeria		Democratic Republic of Congo		Egypt	
	2023	2030	2023	2030	2023	2030
Mobile subscriber penetration	71%	78%	33%	43%	70%	76%
Smartphone adoption	85%	91%	31%	61%	85%	91%
Technology mix						
2G	12%	2%	30%	5%	9%	2%
3G	16%	4%	51%	40%	46%	22%
4G	72%	52%	20%	52%	44%	44%
5G		42%		4%		32%

	Ethiopia		Morocco		Tunisia	
	2023	2030	2023	2030	2023	2030
Mobile subscriber penetration	40%	50%	74%	80%	79%	84%
Smartphone adoption	36%	80%	84%	90%	85%	91%
Technology mix						
2G	2%	1%	23%		27%	8%
3G	57%	20%	22%	10%	10%	4%
4G	41%	69%	55%	24%	63%	48%
5G	1%	10%		67%		40%

Note: totals may not add up due to rounding
Source: GSMA Intelligence

From a security perspective, financial services are a key focus area for operators in the region. Mobile money, wallets and financial services are a mainstay offering of operators. These can work on 3G and 4G smartphones and have proven to be a sustainable revenue line. Since M-Pesa's launch in 2007, mobile money services have expanded to reach a large number of customers. M-Pesa accounted for around 40% of Safaricom's revenues in 2023. Revenue from M-Pesa amounted to $835 million in the 2023 financial year, ahead of voice revenues at $578 million and mobile data revenues at $382 million.[3]

Operators have primarily conducted their mobile money operations through fully owned subsidiaries, offering banking services to those without access to traditional banking. The value of mobile money transactions reached around $350 billion in 2023.[4] The rapid growth of mobile money services has also led to expansion into other financial products such as bill payments, savings, loans and insurance products.

3 Annual report and financial statements, Safaricom, 2023
4 The State of the Industry Report on Mobile Money, GSMA, 2024

3

The security landscape: rapidly evolving threats

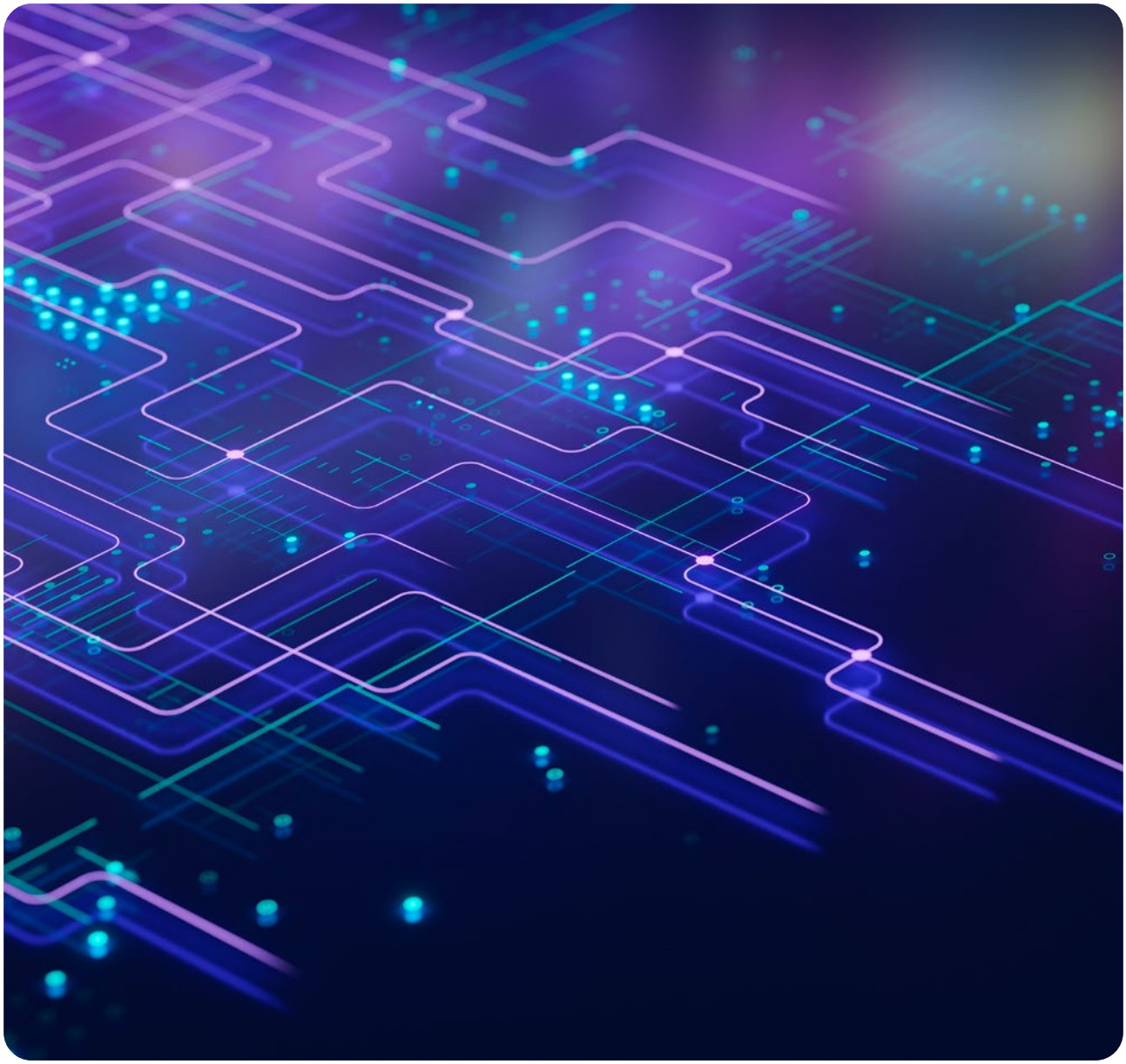
3.1 Understanding the cybersecurity threat

To establish and operate cyber defences, it is crucial to have a clear understanding of the security threats and the network assets that make up the attack surface. This report series considers a range of network assets, including mobile and fixed networks, edge computing, cloud data centres, IoT and mobile devices. Cybersecurity attacks on these are complex, wide-ranging and constantly evolving. As new technologies emerge (such as software-defined mobile networks and AI), malicious actors continue to adapt. New threats and sources of attack are emerging around the world.

Mobile operators are frequently targeted by cyberattacks and must accept that no one is invulnerable. Cyberattacks can inflict severe economic damage. It is therefore crucial to understand, monitor and counter the evolving threats. The threats facing operators and others include established vectors such as ransomware, malware and distributed denial-of-service (DDoS) attacks, as well as more nuanced attempts via 'living off the land' or 'lone wolf' attacks.

The GSMA Intelligence survey on security of telecoms operators in Northern Africa reveals that:

- operators perceive the network security risk environment to be at critical levels
- the cyber-threat level across IoT and devices (mostly smartphones) is concerning, with around half of operators rating the threat level over IoT very high and around three quarters rating the threat level over mobile devices high or very high
- the threat level for cloud data centres is rated slightly lower, likely reflecting that security responsibilities are shouldered by their hyperscaler owners rather than these not being a target per se.



3.2 Operator perceptions of threat levels

Security threat level by domain

Operators perceive there to be a significant threat level for IoT and mobile networks (see Figure 4). This is exacerbated by the challenge of integrating legacy mobile network systems with IoT applications. Legacy mobile network systems may have vulnerabilities, and integrating these with IoT applications introduces new attack vectors and potential security risks. Implementing robust security measures such as authentication and access control to protect the integrated system from unauthorised access and data breaches can help mitigate risk. GSMA Baseline Security Controls can form the baseline of any mobile network security risk assessment.[5]

Operators are increasing IoT coverage to cater to an array of vertical use cases, including digital payments, smart cities, smart health and smart agriculture. For instance, Ethio Telecom, in partnership with the Addis Ababa city administration in Ethiopia, is installing a wide area network (SD-WAN network) to interconnect different administrative offices and institutions of the city with the main data centre.

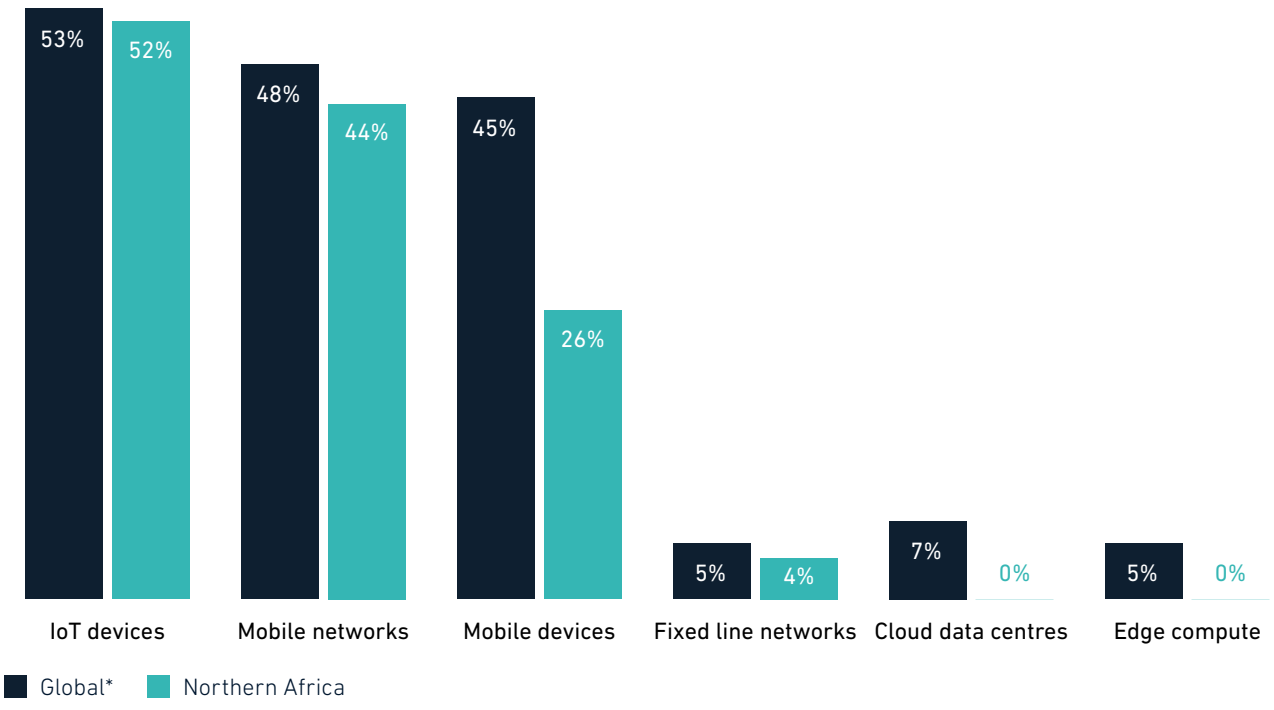
As digitisation continue to expand, the urgency grows to phase out legacy mobile networks and fortify cybersecurity measures, given the growing number of attack entry points from smart devices to edge nodes. Device attacks can manifest at the hardware or software levels, presenting risks for device OEMs, operators and a range of industries.

Figure 4

Around half of operators rate the threat level as very high across IoT devices

Considering the current cybersecurity landscape of 2024 in your primary country of operation, how would you rate the overall threat level across the following assets?

Percentage of operators ratings as very high



*Global results reflect latest survey responses.
Source: GSMA Intelligence

5 For more information on GSMA Baseline Security Controls, see Chapter 5

Security threat level by vertical

The financial and healthcare sectors are viewed by operators in the region as highly susceptible to attack, with 80% of operators acknowledging this vulnerability. The effectiveness rating among operators for their products and services to counter/prevent threats in these sectors is lower than global counterparts. This underlines the need for innovation from operators and for them to take a proactive and resilient, multifaceted approach that enhances security risk management (see Section 3.3).

Though related to a system glitch rather than an attack, the recent example of state-owned Commercial Bank of Ethiopia highlights how important security risk management processes can be. The bank experienced a system failure during an upgrade designed to improve the bank's IT system. Through the implementation of a quick and effective risk management strategy, it managed to recover most of the funds lost due to the failure.[6]

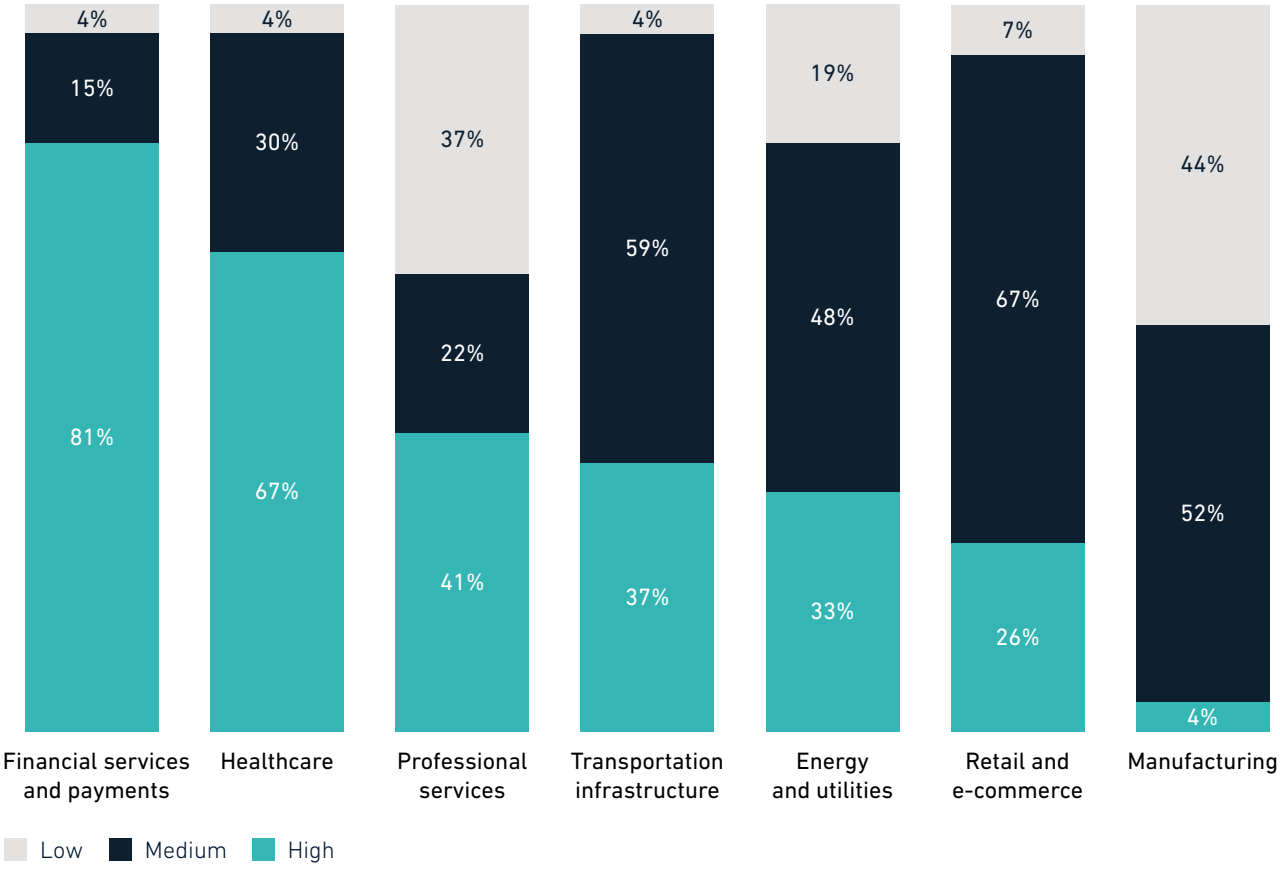
Across Northern Africa, the average annual loss due to mobile money fraud per provider is estimated at $1.06 million.[7] Mobile money users are particularly vulnerable to fraud due to lower levels of digital literacy and the complexity of the service ecosystem, with numerous stakeholders.

Figure 5

The financial and healthcare sectors are rated by operators as being highly susceptible to cyber threats

Considering the 2024 cybersecurity threats in your primary country of operation, how would you rate the overall security level across the following verticals?

Percentage of operators that rated the threat level high, medium or low



Source: GSMA Intelligence

6 "Commercial Bank of Ethiopia Recovers 78% of 801.4m birr lost in a system glitch: President Abe Sano", Addis Standard, 2024
7 2024 the year ahead: Main telecom mobile industry fraud and security challenges for mobile operators in Africa, Unitel, 2024

Strength of operator defences

Operators in Northern Africa have a significant level of confidence in their mobile network defences, with 81% rating them as either strong or very strong, in line with the global average of 82% (see Figure 6). However, only 22% of these operators rate their defences as *very* strong, compared to a global average of 38% (see Figure 7). By focusing on particular areas, operators in the region can work to improve confidence levels and ensure their network defences are as robust as possible:

- **Identify weak spots** – Assessing specific vulnerabilities or areas where network defences can be enhanced.
- **Invest in security** – Increasing investment in cutting-edge security technologies and practices can help improve confidence levels. Security solutions include encryption, authentication and access control.
- **Develop training and awareness** – Better training and greater awareness among network operators on the latest threats and defence mechanisms can help boost confidence in the robustness of network defences.
- **Collaborate and adopt best practice** – Sharing best practice and collaborating with global partners can help operators improve the security framework and reach higher confidence levels.
- **Leverage industry-wide tools** – Operators can leverage the Network Equipment Security Assurance Scheme (NESAS) and Mobile Cybersecurity Knowledge Base (MCKB) to help enhance their security defences capabilities.[8]

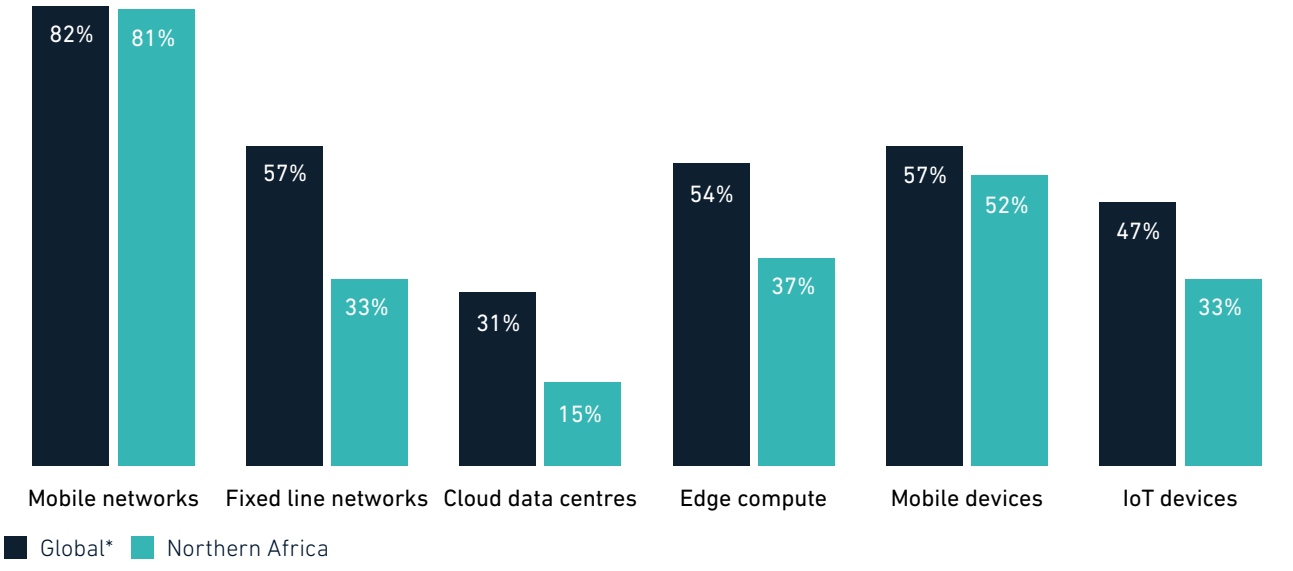
Confidence is lower when it comes to edge infrastructure and devices, and lower still for cloud and data centres. Some of the perceived weakness can be explained by a lack of control; others are responsible for data centre operations or device manufacturing. Nevertheless, the operator view of defences for these assets in Northern Africa is weaker than counterparts in other regions, suggesting more fundamental vulnerabilities to address.

Figure 6

Operators are confident in the strength of their own defences for mobile networks

Considering the 2024 cybersecurity threats in your primary country of operation, how would you rate your company's readiness against security attacks for the following assets?

Percentage of operators that rate their defences as **strong** or **very strong**



*Global results reflect latest survey responses.
Source: GSMA Intelligence

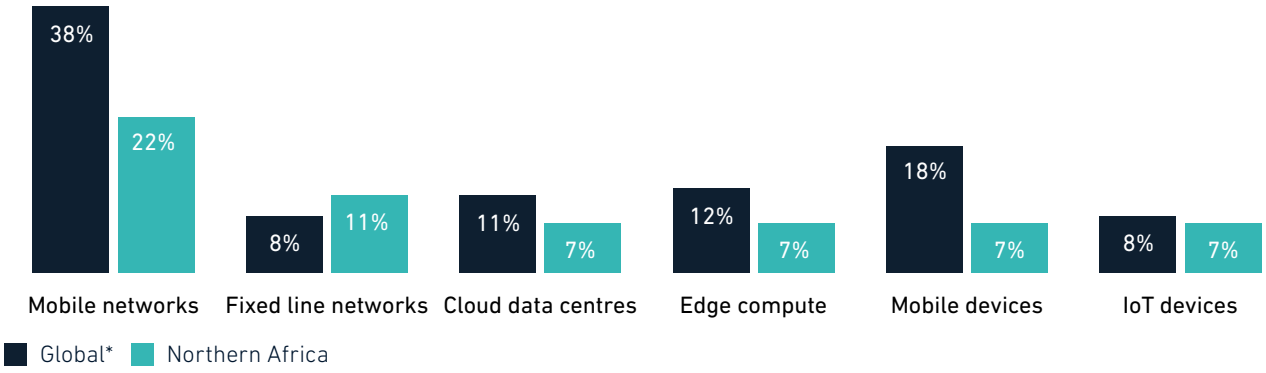
8 For more information on these tools, see Chapter 5.

Figure 7

Only 22% rate mobile network defences as *very* strong

Considering the 2024 cybersecurity threats in your primary country of operation, how would you rate your company's readiness against security attacks for the following assets?

Percentage of operators that rate their defences as **very strong**



*Global results reflect latest survey responses.
Source: GSMA Intelligence

Security threat level by vector

Threat vectors include established routes such as ransomware and phishing but have also evolved into a wider panoply of options using advanced techniques. Operators in Northern Africa view ransomware and phishing/smishing (phishing via SMS) as the top two threats facing their mobile networks, with supply chain attacks slightly lower down the list but still concerning (see Table 2).

Ransomware, supply chain attacks and phishing/smishing represent a clear challenge for operators over the next three years. Phishing/smishing remain common attack vectors for account takeover fraud (ATO), which is a significant and growing concern in the telecoms sector due to its impact on mobile money. This suggests the pipeline of fixes is insufficient and/or that attackers are evolving their practices more quickly.

Table 2

Phishing/smishing attacks pose a challenge to operators

Considering the 2024 cyber threat landscape in your primary country of operation, and based on your knowledge, what are the major sources of cybersecurity threats? Percentage of operators that rank vector in top three of all attack vectors

Thinking about the cyber threats in your primary country of operation, how do you anticipate the hazard level for the following cyber threats will be in three years compared to now? Percentage of operators that rank the risk as being higher over the next three years minus the percentage that rank the risk as lower.

	Global*	Northern Africa	Net threat rise in Northern Africa over next three years
Ransomware	78%	85%	67%
Phishing/smishing	88%	93%	96%
Supply chain attacks	51%	59%	70%

*Global results reflect latest survey responses.
Source: GSMA Intelligence

Preparedness: behind or ahead of the curve?

Looking at viable security risks helps understand where the industry sees itself as being behind or ahead of the curve (see Figure 8).

Although ransomware and smishing/phishing are major cyber threats in the region, operators have confidence in their ability to defend against such attacks. For example, 93% of operators view themselves as either very ready or somewhat ready to defend against phishing/smishing. Some 85% of operators view themselves very ready or somewhat ready to defend against ransomware. A key question is whether and how operators will be able to keep up with the threats of ransomware and phishing/smishing as they evolve and become more nuanced. This will require cooperation, use of industry tools such as MCKB, network security hardening policies, and improvements in capacity building and risk response.

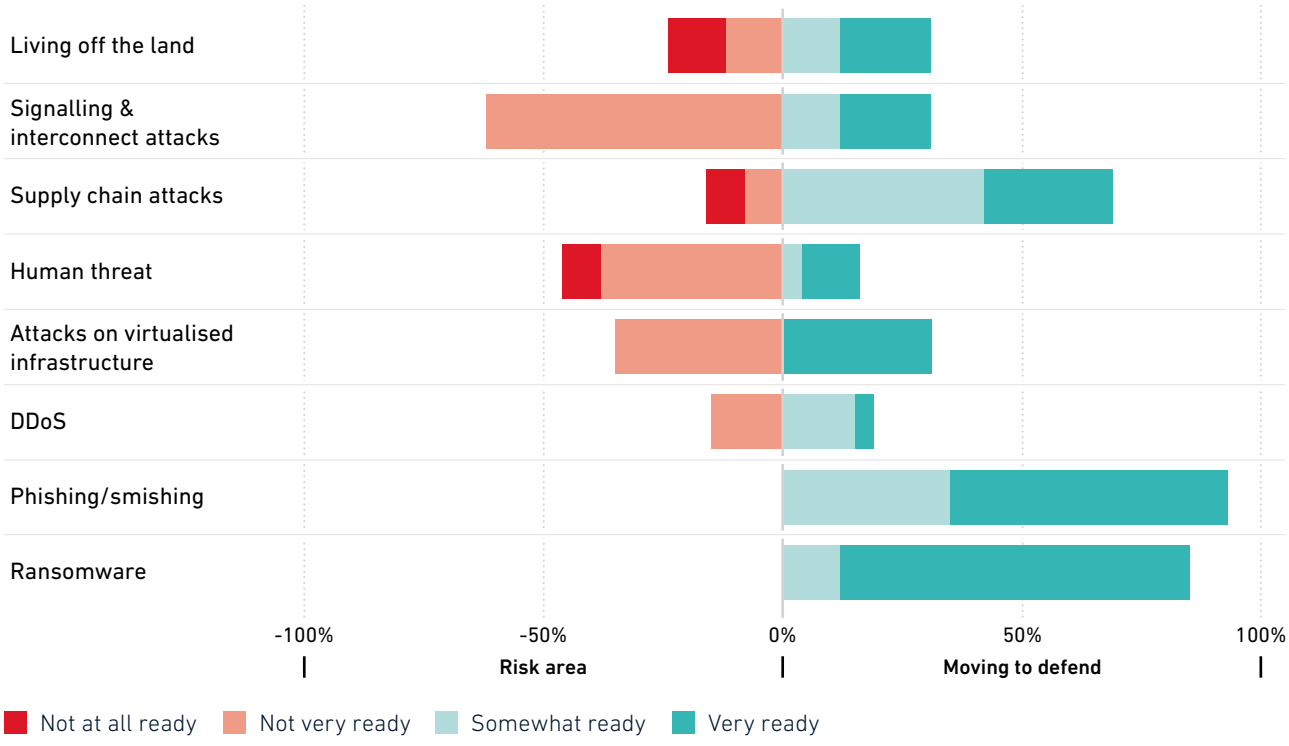
For potential attacks on the supply chain, around 69% of operators view themselves as ready. However, 16% view the supply chain as a vulnerability, with 8% claiming they are not ready at all. Signalling and interconnect, human attacks and attacks on virtualised infrastructure are viewed as even greater risks. To some extent, the threats seen as net risks (such as signalling or virtualised infrastructure) reflect the fact that operators do not fully control these levels of the technology stack. However, this does not exonerate operators from a responsibility to protect, or (at the very least) limit exposure to the reputational damage that could stem from a breach of partner infrastructure. The challenge is to coordinate with suppliers on common approaches and strategies to monitor and respond to any attacks, given that the effects of a breach will impact all stakeholders. In-sector cooperation between operators is also important, with toolkits such as T-ISAC[9] helping meet this objective.

Figure 8

Operators are ready for established threats but far less so for emerging ones and human threats

Evaluate your company's readiness across the following threats vectors in your primary country of operation.

Percentage of operators assigning readiness level to attack type



Source: GSMA Intelligence

9 See T-ISAC

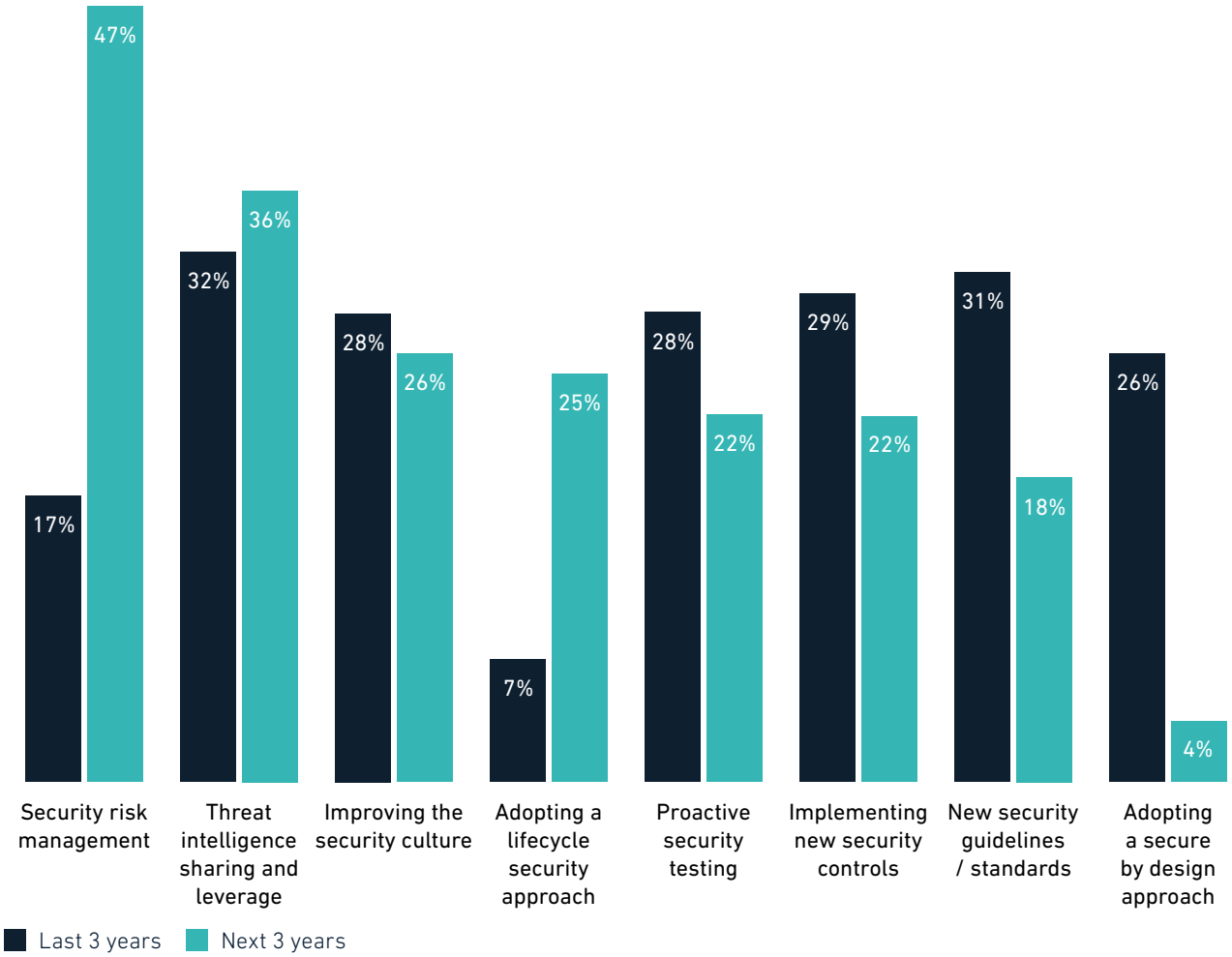
3.3 Operator perceptions of network security innovations

Figure 9 shows some of the interventions available to operators to improve network security. There is little consensus on what has been the most important tool for defending network assets over the past three years, with a range of solutions and tactics required to adequately defend mobile networks. Some operators (32%) claim that threat intelligence sharing and leverage has been the most effective, while others (31%) believe new security guidelines and standards have had the greatest impact on network robustness. Looking ahead to the next three years, the most widely held view is that security risk management and threat intelligence sharing & leverage are the top priorities to ensure mobile networks and related infrastructure are robust and resilient.

Figure 9

Security risk management and threat intelligence sharing are seen as key to future security for operators in Northern Africa

Which areas within security and telecommunications networks do you believe have had the greatest impact over the last three years and, separately, require most innovation in the next three years to create more robust and resilient networks?



Note: respondents were asked to rank 1st, 2nd and 3rd. Chart shows overall weighted scores, calculated as Ranked 1st * 1.00 + Ranked 2nd *0.66 + Ranked 3rd * 0.33
Source: GSMA Intelligence

With security risk management a priority for operators going forward, it is unsurprising that operators have identified the need for support in enhancing network visibility & monitoring and vulnerability management. The latter is a key element within the broader framework of security risk management. It typically involves multiple stakeholders across the supply chain working together to identify, fix, mitigate or compensate for vulnerabilities before they can exploited.

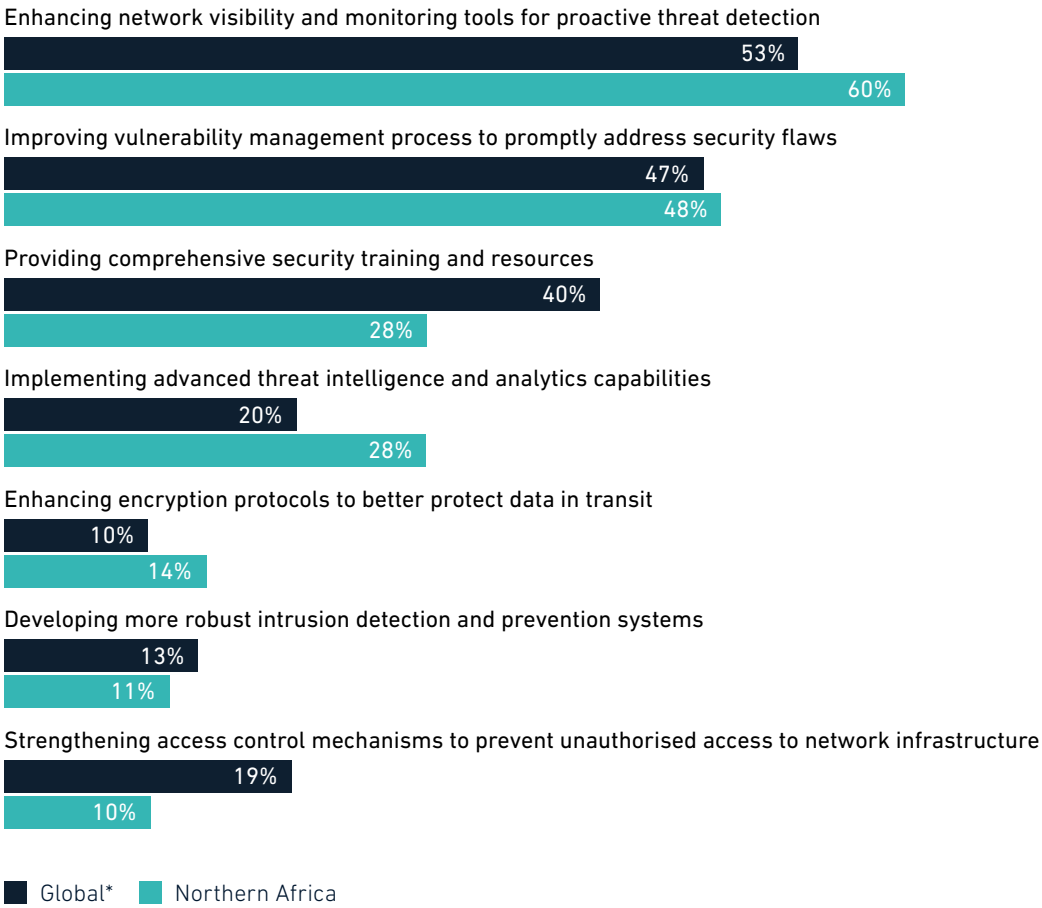
One mechanism for vulnerability management in the mobile industry is the GSMA's coordinated vulnerability disclosure (CVD) programme.[10]

Figure 10

Improving network visibility & monitoring and vulnerability management are the areas where operators need the most support

Considering your primary country of operation, which areas do you most need support to enhance mobile security?

Percentage of operators rating area in top three



Note: respondents were asked to rank 1st, 2nd and 3rd. Chart shows overall weighted scores, calculated as Ranked 1st * 1.00 + Ranked 2nd *0.66 + Ranked 3rd *0.33.
Source: GSMA Intelligence

10 See the GSMA's CVD programme

4 Ensuring security readiness

4.1 Measures to counter the threat

The cyber-threat landscape in Northern Africa is complex and fragmented, with countries at different levels of social and economic development. Low-income countries are often targets of attackers, who adopt a strategy of infiltrating systems in such countries before moving to higher-value targets.

As well as economic and social conditions, low levels of digital literacy and cybersecurity awareness, cyber attackers are incentivised by a lack of robust legal and regulatory cybersecurity and data protection frameworks. This ranges from how to handle breaches and personal data, to identification of what constitutes illicit activities in cyberspace, and the definition of the necessary procedural tools to investigate, prosecute and enforce such legislation. It is critical that regulators and governments in those countries of Northern Africa that are more exposed to cyberattack (e.g. Ethiopia and Algeria) enact measures to increase the robustness of their cybersecurity and data protection legal frameworks.

Table 3

Ethiopia and Algeria need to address the growing cybersecurity gap versus leading countries in the region

	Cybersecurity score (out of 100)	Rank (out of 184 countries)
Egypt	95.48	23
Morocco	82.41	50
Algeria	33.95	104
Ethiopia	27.74	115

Note: Each country's cybersecurity score is an aggregate score of five pillars – legal measures, technical measures, organisational measures, capacity development, and cooperation.
Source: ITU, Global Cybersecurity Index 2020[11]

Operators in Northern Africa can take several security measures to help counter cyberattacks:

Technology segregation segregates internal operational technology services from external access. It slows down hacking by making the discovery of vulnerable systems more difficult. It is particularly appropriate for protecting systems and applications against hackers, and is effective against ransomware gangs.

Configuration hardening is the process of reducing the level of vulnerabilities posed by a system's configuration. It increases the degree of effort needed to gain an initial hacking foothold in the target organisation and is particularly appropriate for protecting IT systems from advanced persistent threat (APT) attacks, ransomware gangs and telco fraudsters. It could also help reduce the cost of introducing external tools by tapping into the security defences already in place in operator networks and systems.

Regular patching of systems and applications reduces the likelihood that standard exploits will work against target systems. It is effective at protecting IT systems against threats from ransomware gangs and malicious insiders. It also provides protection against APT attacks.

Reduced technology complexity means a technology stack is designed for easy maintenance and allows security efforts to focus on a well understood set of technologies. This security measure is relevant when looking across all threat actors.

Email protection is aimed at configuring email systems securely. It increases protection from fraudulent emails with malware or social engineering intent. It is effective against ransomware.

Secure access protects legitimate access by making passwords harder to guess. It is highly effective for threats from malicious insiders and is effective at countering APT attacks and ransomware threats.

11 For the latest rankings and scores, see the Global Cybersecurity Index, released in September 2024.

5 Innovation from telecoms operators

5.1 Leveraging industry-level tools and resources

Securing the supply chain

Selecting and testing vendors and products is key to network security. A common way of demonstrating product security is to build products that are independently assessed under globally recognised product security assurance schemes, such as the GSMA's NESAS, which audits and tests network equipment vendors and their products against a security baseline, defined by industry experts through the GSMA and 3GPP. This approach to network security offers benefits to the entire ecosystem (including regulators, mobile operators, hyperscalers and equipment vendors), as highlighted in Figure 11.

Figure 11

The NESAS framework provides a universal industry standard for network security

Source: GSMA

The NESAS framework underscores the importance of applying regulations, where necessary, consistently across all providers within the value chain in a service- and technology-neutral manner. Schemes such as NESAS can be particularly useful in regions like Northern Africa, where many countries are yet to deploy 5G, and policymakers are still establishing rules for assigning 5G spectrum and deploying 5G networks.

Securing the 5G era

5G offers the mobile industry an unprecedented opportunity to raise network and service security levels. 5G standards development has adopted 'secure by design' principles, leading to the following:

- **use of mutual authentication** – confirming sender and receiver have an established trust and the end-to-end relationship is secured
- **a presumed "open" network** – removing any assumption of safety from overlaid products or processes
- **acknowledgment that all links could be tapped** – mandating encryption of inter/intra network traffic, ensuring the encrypted information is worthless when intercepted. Although this is common practice in solutions for other services, such as online banking, it is a major paradigm shift in existing mobile telecoms practices. As a consequence, 5G networks should afford the consumer more protection than 2G/3G/4G networks.[12]

However, operators must also be aware that the adoption of new network technologies introduces new potential threats for the industry to manage. While the transition to 5G SA will allow the full security features of 5G specifications to be realised, it will also pave the way for a cloud-native, service-based architecture that will introduce new security challenges. This underlines the importance of operators investing in their threat monitoring, detection and response capabilities.

12 For more information, see the GSMA's Securing the 5G era

Building a mobile cybersecurity knowledge base

As mobile operators launch 5G while maintaining earlier generations of mobile technologies, communications networks will face new security threats and challenges. Understanding, mapping and mitigating existing and upcoming security threats in an objective, rapid and effective manner has become essential.

To help operators and others in the mobile ecosystem, the GSMA has conducted comprehensive threat analysis involving industry experts from across the ecosystem (including mobile operators, vendors and regulators) and input from public sources such as 3GPP, ENISA and NIST. It has mapped these threats to appropriate and effective security controls.

The GSMA has collated this analysis in the GSMA Mobile Cybersecurity Knowledge Base to provide useful guidance on mobile security risks and mitigation measures. The Knowledge Base aims to make available to GSMA members the combined knowledge of the mobile ecosystem to increase trust in mobile networks and make the interconnected world as secure as possible. Over time, the Knowledge Base will be enhanced and extended to respond to the evolving cybersecurity threat landscape.

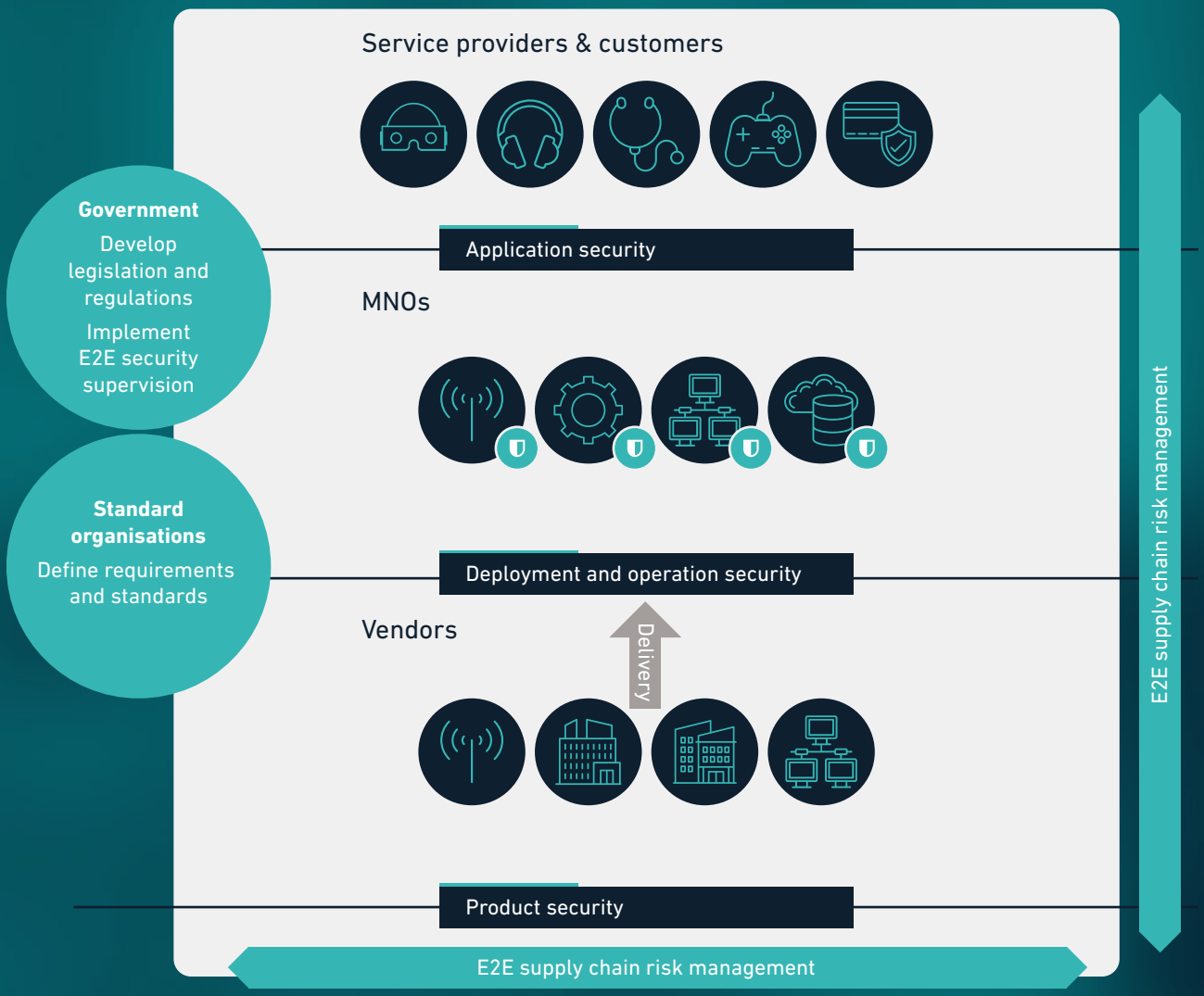
The Knowledge Base facilitates and encourages collaboration to protect networks and services against disruption and unauthorised access, as well as the prevention and mitigation of risks. It will help enhance mobile security competencies and capabilities and will strengthen the work of operators, enterprises, oversight agencies and regulators. At an operational level, the Knowledge Base offers clear instructions for taking step-by-step actions to build security assurance while considering the full range of risks surrounding end-to-end networks.

The Knowledge Base also provides operators with a mobile cybersecurity model, which is a framework designed to enhance the security of mobile networks and services by addressing cybersecurity risks across multiple areas. The mobile security model consists of three main layers:

- **Application security** – The scope of the application security layer includes mobile device users as well as vertical industries that provide and use a range of applications. Application security requires multiparty collaboration between mobile operators, equipment vendors and application developers to ensure the security of mobile networks and the users and services they support. Application security extends beyond mobile operators' networks and therefore beyond the responsibility of mobile operators.
- **Deployment and operation security** – The deployment and operation security layer is commonly managed, controlled and operated by mobile operators, but some elements might also be outsourced to specialist service providers. During the network design phase, mobile operators perform a comprehensive and continuous risk assessment which takes into account network components, network functions provided by vendors and the network architecture to ensure effective management of security threats.
- **Product security** – Product security is the responsibility of vendors, such as device providers or network equipment suppliers. Network element security assurance is a key tool, providing a basis to evaluate whether network devices and components have been designed and implemented in accordance with defined security requirements. Security assurance programmes should adhere to globally recognised and unified standards to ensure their operation is cost effective and sustainable for the ecosystem. For example, the Network Equipment Security Assurance Scheme (NESAS), jointly defined by 3GPP and the GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry.

Figure 12

Cybersecurity is a shared responsibility



Source: GSMA[13]

13 See Network Equipment Security Assurance Scheme (NESAS)

Establishing business controls

The measures required to enhance security are not always technical; they may involve reporting or communication procedures crucial to upholding business objectives on security. As part of the Mobile CyberSecurity Knowledge base, the GSMA has developed baseline security controls to help operators understand and develop their security posture to a foundation (base) level.[14] Key measures include the following:

- **Driving board-level engagement** – Where organisations fail to recognise security at the board level, there is likely to be a gap in the way the organisation understands their success, risk posture, priorities and future investment on programmes. This gap introduces unnecessary security and fraud risks.
- **Formally recognising security as a responsibility** – Organisations should have a role formally recognising security as a responsibility. This is often fulfilled by the chief information security officer (CISO). Alternatively, it can be any person of a senior standing. Their role must be able to influence and direct enterprise-level investment and change.
- **Establishing organisational policies** – Organisations should construct specific policies in relation to security. These should map to the overarching security strategy and principles of the organisation. Essentially, policy should underpin the organisation's security objectives.
- **Developing business continuity management (BCM) plans.** BCM improves the resilience of an organisation by developing an organisation's ability to detect, prevent, minimise and deal with the impact of disruptive events. In the aftermath of an incident, the BCM plan enables critical activities within the organisation to continue. In the longer term, it can help the business to recover and return to business as usual.
- **Aligning with internationally recognised standards –** Operators should align their cybersecurity practices and compliance regimes with internationally recognised standards (e.g. aligning BCM with ISO/IEC 22301) and cybersecurity frameworks (e.g. NIST Cybersecurity Framework).

Several operators in Northern Africa have made significant progress establishing business controls for managing security. For example, Airtel Africa has implemented a comprehensive security programme to identify risks to its business operations. Data security is listed as the top material issue in its annual sustainability report, driving board-level engagement in security initiatives. Furthermore, the operator has formally recognised security as a responsibility, appointing a Group CISO and CIO in 2022. It has also ramped up its efforts to align with internationally recognised security standards, having achieved ISO 27001 (Information Security Management System) and ISO 22301 (Business Continuity Management System) certifications for all 14 of its markets in 2022.

MTN has aligned its privacy and data protection policies with ISO 27001, as well as various other policies and frameworks, including the NIST Cybersecurity Framework, General Data Protection Regulation (GDPR) and Protection of Personal Information Act (POPIA).[15] To ensure it complies with these guidelines and regulations, MTN has appointed an information officer and deputy information officer to guide data privacy and establish clear procedures for reporting personal information breaches.

Improving intelligence sharing

Contributing to relevant sharing communities is another way in which operators can defend against security threats. The sharing of information between mobile operators is most commonly done via the GSMA's Telecommunication Information Sharing and Analysis Centre (T-ISAC), which enables GSMA operator members to communicate cyber risk data, including new indicators of compromise, in real-time. Additionally, T-ISAC allows its members to share best practice with each other in a trusted environment, bolstering the security of operators and their partners.[16]

The GSMA's Fraud and Security Group has an intelligence sub-group that reviews and shares a range of reported security and fraud attack types. This regular sharing of attack techniques allows new modus operandi to be identified and evaluations to be made on the effectiveness of deployed security and fraud controls. The GSMA also facilitates the Fraud and Security sub-group focusing on local fraud campaigns through threat intelligence sharing.

14 For more information on business controls, see the GSMA's FS.31 GSMA Baseline Security Controls
15 MTN FY23 Transparency Report
16 GSMA members can join T-ISAC

A barrier to intelligence sharing has been the lack of a framework to classify and deconstruct the various tactics and techniques used by adversaries. However, in April 2024, the GSMA published a new tool for the telecommunications security industry. The Mobile Threat Intelligence Framework, MoTIF, is a GSMA member-developed framework designed to classify the threat actors active over telecoms networks. It provides a language to describe the activity of threat actors attacking mobile industry targets by explaining their tactics and techniques in a formal, machine-readable way. The framework should significantly improve communication among operators, expediting the transfer of knowledge.

5.2 Navigating the human risk

Humans can be the weakest link in the security risk profile. Operators have therefore established a range of security controls targeted at employees, including staff vetting, additional administrator controls and operating a 'least privilege regime'. They are also taking appropriate steps when onboarding new staff. For example, every new Ooredoo Algeria employee is enrolled in an internal cybersecurity awareness programme that familiarises them with cybersecurity risks. Staff are then required to pass a test at the end of the programme.[17]

Operators are also collaborating with universities to develop local workforces with cybersecurity skills. For example, when Orange Cyberdefense opened a new hub in Morocco (its first in Africa) to meet local demand for cybersecurity solutions, it recruited staff through partnerships with major French engineering schools.[18] The experts based in Morocco have access to all the expertise, methodologies and best practices from Orange Cyberdefense and work in close collaboration with the Orange teams in Morocco.

Despite operator initiatives playing an important role in upskilling staff, there remains a shortage of cybersecurity professionals in Northern Africa. The challenge of hiring new experts is likely to deepen as demand for cybersecurity skills grows across the sector. This is driving educational institutions and governments to develop new courses targeted at university graduates and those at the early stages of their professional careers. For example, Egypt's National Telecommunication Institute (NTI) announced a partnership in April 2024 with Arab Security Consultants (ASC), a distributor of the International Council of E-Commerce Consultants (EC-Council), to bolster collaboration in network security and cybersecurity. The agreement aims to establish the EC-Council Academy at NTI, delivering training in EC-Council's network security courses and technologies to NTI students and graduates. Over a three-year period, the initiative hopes to train up to 1,000 people each year.

There is also an emphasis in Northern Africa on developing cybersecurity skills and awareness among the wider public. Orange has launched a free, high-level certification training programme in partnership with online learning provider, Coursera. The programme is aimed at equipping young people in Africa and the Middle East with key skills in essential areas such as AI and cybersecurity. It will be available through Orange Digital Centres (ODCs), which are physical hubs of innovation and learning that Orange has established throughout its footprint. There are now 26 ODCs worldwide, including several in Northern Africa (Côte d'Ivoire, Egypt, Ethiopia, Guinea, Mali, Morocco, Senegal and Tunisia).

ODCs also provide a physical space for hosting workshops to share digital best practices in areas such as personal data security and protecting children online. These workshops have helped Orange reach 1.8 million beneficiaries between 2021 and 2023 through its free digital training programmes. Other operators have established their own digital skills training programmes for customers, often in partnership with third-party specialists. For example, Telecom Algeria has partnered with Shirudo to offer customers a free online game that educates customers on how to protect themselves from phishing, malware, ransomware and other cybersecurity threats.

17 Ooredoo Algeria 2022 Annual Report
18 "Orange Cyberdefense accelerates its international expansion with new Moroccan presence to cover French-speaking African countries", Orange, June 2020

5.3 Tackling fraud and malware attacks

Minimising SMS and voice fraud

The rise in fraud initiated through telecoms channels such as SMS and voice calls, coupled with new regulatory requirements, is driving operators to invest in fraud protection solutions. SMS firewalls are a key part of an operator's defence against fraudulent SMS traffic. For example, Orange has deployed a third-party SMS firewall to reduce fraud and spam in Morocco. Such solutions work by filtering and blocking fraudulent traffic, including grey-routing, phishing and smishing.

SMS firewalls can also boost application-to-person (A2P) messaging revenues by segmenting SMS traffic in real time, enabling operators to apply the correct pricing for each type of traffic.[19] Conversely, neglecting to shield subscribers from fraudulent SMS activities risks eroding consumer confidence in operator messaging services, which can have a negative impact on operator A2P revenues if enterprises switch to OTT-based services rather than business messaging via SMS.

Operators are also investing in solutions to prevent voice fraud. Many operators are leveraging voice firewalls to evaluate voice traffic and block calls to minimise the impact of vishing on end users. Voice firewalls are frequently employed alongside complementary solutions such as branded caller display, which allows organisations to display their brandname or logo on the recipient's phone. Notably, voice fraud prevention solutions are evolving beyond dependence on number history analytics and validity checks to thwart fraudulent calls. Leading solutions are increasingly using AI/ML to analyse every dimension of a call in real-time, enabling a swift response to emerging threats.

CASE STUDY FROM EGYPT

Telecom Egypt reduces incoming scam calls after deploying voice firewall solution

Challenge: According to a 2023 report by the Global Anti-Scam Alliance (GASA), phone calls are the most common method for scam attempts worldwide. Egypt, like many other countries, suffers from voice call scams that employ spoofing to deceive subscribers regarding the caller's true identity.[20] Scammers use this tactic to conceal their identities and convince recipients that the call is from a trustworthy source. This tactic is frequently used to impersonate banks or authorities, initiating the early stages of financial fraud schemes or personal data theft.

Solution: To protect its subscribers, Telecom Egypt has deployed a voice firewall to detect and block any spoofed calls coming onto the network, ensuring that only genuine calls reach the subscribers thereby preventing scams at the first stage, before potential victims are reached.

Impact: When the firewall solution was initially deployed, more than 8% of all calls on Telecom Egypt's network were identified as fraudulent and immediately blocked. The firewall solution has effectively deterred scammers from targeting the network, driving a reduction of more than 90% in incoming calls featuring spoofed caller IDs.[21]

19 See for example, "Ooredoo Algeria: Double-digit increase in A2P SMS traffic and revenue with Infobip SMS Firewall solution" Infobip
20 Caller ID spoofing means the number displayed to a subscriber when receiving a call is not the number from which the call is being made.
21 "Telecom Egypt Reports 90% Reduction in Incoming Scam Calls after Deploying Enea's Voice Firewall, Deterring Fraudster", Enea, June 2024

Countering fraudulent SIM swapping

SIM swap is a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one. However, it has provided an opportunity for fraudsters to obtain and utilise the replacement SIM card to gain access to users' financial and wider service accounts.

Mobile operators are taking several steps to counter fraudulent SIM swapping. Common strategies include having an equal level of customer validation for new and existing customers, increasing the amount of training given to retail staff, and implementing multifactor authentication. Partnerships with SIM card vendors can help operators more easily enact these measures.

Operators are also looking to implement GSMA Mobile Connect and GSMA Open Gateway APIs to improve user authentication. Ethio Telecom, e& and Zain Group are among the operators with a presence in Northern Africa to have joined the GSMA's Open Gateway initiative. However, the first commercial launch of GSMA Open Gateway APIs in the region is still pending, with operators in South Africa and other countries already demonstrating the power of the SIM Swap and Number Verification APIs for fraud prevention and security.

CASE STUDY FROM ETHIOPIA

Operators drive awareness on measures end users can take against fraud

Challenge: Ethiopia has lower levels of formal financial inclusion than its East African neighbours. Less than half of the adult population have an account at an institution. The revised National Financial Inclusion Strategy (NFIS 2021–2025) aims to increase financial inclusion from 46% to 70% of all adults by 2025, in part by scaling digital payments through mobile money services.[22]

However, financial inclusion will not happen without action to allay safety and security concerns among individuals. GSMA Consumer Survey respondents and focus group participants commonly cited safety and trust as key barriers to account ownership and usage.

Solution: Mobile money providers Ethio Telecom and Safaricom are investing in educational campaigns to increase digital financial literacy and promote safe transaction practices. These campaigns can reach customers through online channels and marketing collateral displayed by mobile money agents. Best-practice guidance includes keeping your PIN private, choosing a strong PIN for your account, verifying phone calls and messages purportedly from mobile money providers, and not handing over phones to mobile money merchants.

In addition, Safaricom has introduced anti-fraud initiatives in other markets that enable users to block fraudulent attempts to swap their SIM cards. The operator has also signed up major banks to its new SIM-Swap-Check anti-fraud service, which allows them to check when a customer's SIM card was last swapped. Similar solutions could be introduced in Ethiopia, following Ethio Telecom's commitment to launch Open Gateway APIs.

Impact: At the end of 2023, Ethio Telecom reported that its Telebirr m-money service had reached 41 million customers, following its launch in May 2021. Meanwhile, Safaricom reached 4.5 million total registered M-Pesa customers in Ethiopia in March 2024 – eight months after its debut in the country.[23] The speed at which these services have grown shows the untapped demand for financial solutions in Ethiopia. The steps taken by mobile operators to drive awareness of safety and security measures have played an important role in boosting financial inclusion.

22 Mobile Money in Ethiopia: Advancing Financial Inclusion and Driving Growth, GSMA, 2023
23 FY24 Investor Presentation , Safaricom, May 2024

Thwarting malware and ransomware attacks

Malware and ransomware represent significant threats to the mobile industry, its customers and supply chains – particularly as the time it takes to exploit a vulnerability has moved from weeks to days, and as skilled, motivated groups are including newfound exploits in their toolkits. Against this backdrop, operators are working to accelerate their ability to patch and mitigate vulnerabilities. This is supported by AI/ML and other technologies that allow more frequent and increasingly automated patching.

Further defence can be provided by partnering with consumer security software vendors. Consumer-facing solutions can be split into two categories: network-based solutions and endpoint solutions. Network-based solutions analyse information about traffic on the network to block – or advise users against accessing – dangerous websites. Meanwhile, endpoint solutions use a range of processes and solutions to protect a network's endpoints (e.g. smartphones, tablets and laptops).

Endpoint solutions can include antivirus and anti-malware software, as well as password management, identity monitoring features and parental controls. Operators are increasingly forming partnerships with third-party providers to offer these capabilities to customers. Maroc Telecom is one of the operators in Northern Africa offering a parental control solution to protect children from inappropriate content on the internet, while Telecom Algeria also provides its customers with this capability along with a range of security tools.

CASE STUDY FROM ALGERIA

Telecom Algeria offers its customers a range of security tools

Challenge: With increasing incidences of malware, ransomware and other threats, the need for a robust and comprehensive security solution is critical. Mobile operators have an important role to play in encouraging their customers to embrace security tools.

Solution: Telecom Algeria has partnered with an IT-security solutions vendor to offer comprehensive security packages to its customers.[24] The operator's consumer proposition provides protection against online risks, covering common infection sources such as email and offering features such as malware and ransomware protection. The solution also includes parental control features that can filter inappropriate content, restrict access to specific websites and manage device usage time to ensure children's online safety.

Telecom Algeria also offers security packages geared towards small businesses. The operator's Desktop & Server Security Suite delivers centralised protection for all network devices, securing the PCs and mobile devices of employees. In addition, the Mail Security Suite offers smart antivirus protection for active traffic, ensuring optimal data security for businesses.

Impact: Telecom Algeria's range of security packages underlines the operator's commitment to enhancing the online security of its customers. They can purchase Telecom Algeria's security packages through Idoom Market, Telecom Algeria's online store, or at physical retail outlets, with flexible licensing options from 12 to 36 months. The straightforward activation process ensures users can quickly and efficiently secure their devices.

24 https://www.algerietelecom.dz/en/produits/drweb-prod215

5.4 Safeguarding against operational attacks

Reinventing the security operations centre

Many operators in Northern Africa have opened security operations centres (SOCs) to provide continuous prevention, protection, detection and mitigation of cyber threats. In some cases, operators have converged their network operations centre (NOC) and SOC to improve collaboration across security teams and streamline threat detection and response. This is becoming increasingly important as telecoms networks migrate to cloud-based network elements and infrastructure.

Investments in SOCs are geared at improving threat visibility across the network and other sources, while increasing automation to help SOC teams cope with the influx of information. For example, Ooredoo has announced plans to integrate endpoint detection and response (XDR) technology into its suite of cybersecurity offerings.[25] The solution leverages AI and ML to proactively detect, prevent, investigate and remediate cyber threats in real-time. The MSSP agreement will cover all Ooredoo's operating companies, with the service being gradually launched across the entire footprint in 2024.

CASE STUDY FROM TUNISIA

Tunisie Telecom converges its SOCs

Challenge: Before 2023, Tunisie Telecom faced challenges managing three separate SOCs dedicated to its telecoms network, enterprise IT and cloud services. This siloed approach hindered effective collaboration and timely response to emerging cyber threats across the organisation's diverse perimeters.

Solution: In 2023, Tunisie Telecom initiated a strategic project to converge its three SOCs into a unified General SOC (G-SOC). Under the direction of the G-SOC Director, 80% of the company's security tools were federated, consolidating monitoring and incident response capabilities. The convergence included establishing a dedicated Threat Management Administrator role to centralise threat intelligence collection, curation and dissemination. This initiative aimed to streamline operations, optimise resource allocation and foster a cohesive cybersecurity strategy across all perimeters.

Impact: This strategic initiative not only strengthens Tunisie Telecom's cybersecurity posture but also positions the company to adapt swiftly to evolving cyber threats. The SOC convergence underscores Tunisie Telecom's commitment to safeguarding its infrastructure, protecting customer data and maintaining trust and reliability in the digital age.[26]

25 "Ooredoo Group Upgrades Cybersecurity for B2B Customers, Partners with SentinelOne", SentinelOne, June 2024
26 For more information, see "HardenStance's Telecom Threat Intelligence Summit 2023 (TTIS 2023) Day 1", YouTube, August 2023

Protecting interconnect and signalling networks

Operators are investing in safeguarding their interconnect and signalling networks, primarily by deploying Signalling System #7 (SS7) and Diameter signalling firewalls. For 5G, the implementation of security edge protection proxy (SEPP) has the potential to further improve roaming security. In addition to these technical solutions, there are ongoing efforts to improve signalling threat intelligence sharing among operators and vendors. The GSMA has also published guidance for its members on how to reduce the risks associated with interconnect signalling, particularly in relation to deploying and using SS7 and Diameter signalling firewalls.

Deploying defensive DDoS tools

Defensive DDoS tools form an important part of network defence and should keep pace with the increasing range and methods of attack. A defence to DDoS attacks is to drop packets by routing them to a 'sinkhole' (i.e. the traffic routing is changed such that the packets are dropped rather than allowing onward connection to the target network). Orange, Vodafone Egypt and Inwi are among the operators to offer a DDoS protection to service to enterprises, whereby traffic destined for the customer's network is monitored and attacks are mitigated before they reach the customer's network link. These types of solution can help operators grow their enterprise revenues while enhancing overall network security.

More operators in Northern Africa will introduce security services for enterprise customers in the coming years. For example, Airtel Africa is aiming to become a provider of security services to institutions in its countries of operation by 2025.[27] As part of this effort, it is exploring opportunities to engage with partners for specialised solutions such as denial of service, application security and monitoring services.

CASE STUDY FROM MOROCCO

Orange Maroc provides DDoS security solutions to enterprise customers

Challenge: DDoS attacks aim to overwhelm internet services with more traffic than they can handle, making them unavailable to legitimate users. To support their enterprise customers against these types of attack, mobile operators can provide DDoS protection services, whereby traffic destined for the customer's network is monitored and attacks are mitigated before they reach the customer's network link.

Solution: Orange Maroc offers two solutions to protect its customers against DDoS attacks:

- **Cloud solution** – Traffic is redirected to Orange Maroc's cleaning centres, where illegitimate traffic is filtered out, providing robust protection against volumetric attacks. Customers can opt for either systematic traffic cleaning or on-demand cleaning based on their specific needs.
- **Customer site solution** – DDoS protection is installed directly at the customer's site(s), safeguarding against application-level attacks on customer traffic. This solution is ideal for environments with multi-operator access, ensuring comprehensive and localised protection.[28]

Impact: DDoS protection is a crucial defence for enterprise customers against cybersecurity threats. Meanwhile, providing cybersecurity solutions such as DDoS protection services to enterprises is a significant driver of revenue growth for operators. In 2023, Orange Cyberdefense, the operator's dedicated cybersecurity services entity, reported an 11% increase in revenue. Orange aims to achieve €1.3 billion in cybersecurity revenue by 2025.[29]

27 Airtel Sustainability Report 2022
28 For more information, see https://entreprise.orange.ma/Solutions-Business/Solutions-avancees/Business-DDoS-Security
29 Orange Integrated Annual Report 2023–2024

Appendix

Defining the Northern Africa region

The following countries are classified as being part of the Northern Africa region: Algeria, Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Democratic Republic of the Congo, Egypt, Ethiopia, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Libya, Mali, Mauritania, Morocco, Niger, Nigeria, Senegal, Sierra Leone, Sudan, Togo and Tunisia.

This does not conform to the United Nations geoscheme; it is an arbitrary designation to separate countries broadly on or above the Sahel, from those to the south (which will be part of a future report in this series).[30]

Defining security threat vectors and their implications

Malware and ransomware

Malware and ransomware represent significant, ongoing threats to the mobile industry, its customers and wider supply chains. The mobile industry (along with others) has to significantly accelerate its ability to patch and mitigate vulnerabilities to avoid negative consequences.

Ransomware attacks can impact access to essential network resources and data, internal servers and communications systems. They can result in the unauthorised extraction of data from IT systems.

30 Ghana and Nigeria are included in both the Northern and Southern Africa editions of this report series.

Malware can be engineered to perform remote code execution and spread broader fraudulent attacks through smishing messages and other fraud schemes, including SMS sent to high-cost destinations and abuse of direct carrier billing.

Commercial spyware is a form of malware that is designed to steal confidential data from the device or appliance it is running on or to access real-time service on the device. Commercial spyware can access a range of personal information and other data to enable threat actors to gain authorised access to the services that these credentials are intended to protect. These types of cyberattacks can lead to financial and sensitive data loss.[31]

Why it matters

The high rate of incidence and severe nature of malware and ransomware attacks mean this threat continues to be a major security consideration for mobile operators and other enterprises.

Attacks on virtualised infrastructure

This refers to attacks on virtual machines and container solutions. As product and function-related software can now run on a range of non-proprietary platforms, operators must ensure that whatever combination of hardware and software they use stays secure.

Why it matters

With the rollout of 5G, the industry is migrating to cloud-based network elements and infrastructure. This virtualised infrastructure can be implemented through virtual machines and containers. As the technology matures, it is important to consider security issues and develop efficient defence mechanisms against potential vulnerabilities in the network architecture. These types of attack can lead to data loss, downtime and damage to a company's reputation.

SIM swapping

A SIM swap attack is a form of identity theft in which the attacker persuades a mobile operator to switch a victim's phone number to a new device to gain access to bank accounts, credit card numbers and other sensitive information. The first step in a SIM swap attack is for attackers to phish for as much information about the victim as possible. After this step, the attacker gains access to the victim's text messages, phone calls and accounts that may be linked to the phone number.

Why it matters

SIM swapping is a relatively new type of attack that is becoming more popular due to the increasing reliance on mobile-based authentication methods. This type of attack can severely damage the reputation of mobile operators and result in subscribers losing trust in operator services.

Distributed denial-of-service attack (DDoS)

Distributed denial-of-service attacks (DDoS) aim to overwhelm internet services with more traffic than they can handle, making them unavailable to legitimate users.

Why it matters

DDoS attacks have been launched via a variety of protocols, including the application layer, network layer (e.g. IP), transport layer (e.g. UDP) and via signalling routes. Services are emerging that seek to make launching a DDoS attack easier, with potentially negative consequences for mobile network operators, including operational disruption and downtime.

31 Mobile Telecommunications Security Landscape, GSMA, 2024

Signalling and interconnect attacks

Signalling and interconnect attacks refer to cyberattacks that exploit the use of legacy SS7 and newer Diameter protocols. An attacker gains access to the SS7/Diameter interconnect network and can perpetrate an attack against any mobile network and subscribers in the world if their home network does not provide protection. The attacks include privacy violations (location tracking, intercepting calls and SMS messages) and fraud.

Why it matters

Such attacks can potentially affect millions of mobile subscribers, with severe consequences for the reputation and financials of mobile network operators.

Human threat

The human threat includes both inadvertent events (e.g. falling for phishing emails) and deliberate compromises. These can take different forms, with some involving social engineering, such as a malicious insider abusing existing access and exfiltrating sensitive data, or exhorting customer-service agents into providing customer data.

Why it matters

Human mistakes are not just limited to junior staff; executives can also fall prey to such attacks. Neglecting the human factor can result in considerable financial loss, reputational damage and loss of customer trust.

Living off the land

A living-off-the-land (LOTL) attack is a type of cyberattack where a hacker uses legitimate tools and features already present in the target system to avoid detection and carry out a cyberattack. In this type of attack, cyber criminals leverage the operating system's built-in capabilities, administrative tools and batch files to control the system and steal sensitive information.

Why it matters

This has become a popular attack technique among hackers as it is difficult for security systems to detect. It can be challenging to differentiate the attack from regular system activity since the attackers use legitimate tools, slowing response times. For this reason, the impact of LOTL attacks can be significant, ranging from sensitive data theft to complete system compromise. These attacks can result in the loss of sensitive data, operation disruption and downtime, financial loss and damage to an organisation's reputation.

Spam and fraud calls

Spam is defined as unwanted calls, including fraud and nuisance calls. While some spam is a nuisance, fraud calls are intended to steal money or personal information. The most common phone scams globally include bank scams, Amazon and mobile provider impersonators, medical care scams, tax and insurance scams, and those related to solar energy.[32]

Why it matters

Governments need to pass regulations to limit spam and fraud calls, and operators need to comply with these. Unwanted calls degrade consumers' confidence and trust in the voice channel, reducing the likelihood of them answering calls. It is therefore in the operator's best interests to protect subscribers from aggressive nuisance calls in addition to illegal fraud calls.[33]

32 Global Call Threat Report, Hiya, 2023
33 Global Call Threat Report, Hiya, 2023

gsmaintelligence.com

GSMA
Intelligence

gsmaintelligence.com