Telco security landscape and strategies: Europe

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 December 2024

Authors

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

Contents

Executive summary

The evolving telecoms landscape in Europe

The telecoms industry is the cornerstone of digital transformation across Europe. By 2026, 5G mobile technology is forecast to reach more than 50% of total mobile connections, with the transition to 5G standalone (SA) adding further impetus to 5G monetisation efforts. Private 5G deployments are gaining traction across Europe, offering opportunities to create new revenue streams and serve additional enterprise customers.

A fast-changing landscape of cybersecurity threats

With digital transformation comes an increased threat of cyberattacks. Over the next three years, cybersecurity threats are expected to intensify – in particular, phishing/smishing and ransomware. Supply chain attacks also pose a significant risk to the safety of European digital infrastructure. A comprehensive security regulatory framework at both the regional and national levels together with the development of industry standards and certificates can support operators in enabling a safer digital environment.

Network security and future investments

Phishing/smishing, ransomware and supply chain attacks remain a priority focus for operators in Europe. They are ready to defend their network assets against such types of attack. They are deploying innovative solutions to bolster network defences – for example, phishing simulation tasks as part of staff training.

Generative AI (genAI) represents a key technology for network modernisation, enabling real-time threat detection and response. However, to unlock the potential of genAI for network security, more investment is needed in edge computing.

Industry tools and collaboration

Industry collaboration is essential to protect against the rapidly evolving threats. As a global organisation unifying the mobile ecosystem, the GSMA provides various forms 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. The risk impact is also now greater, 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 last 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.

Previous reports have focused on Latin America, Asia Pacific, Northern Africa (broadly defined as countries north of the Sahel) and Southern Africa (south of the Sahel). This report focuses on Europe.

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

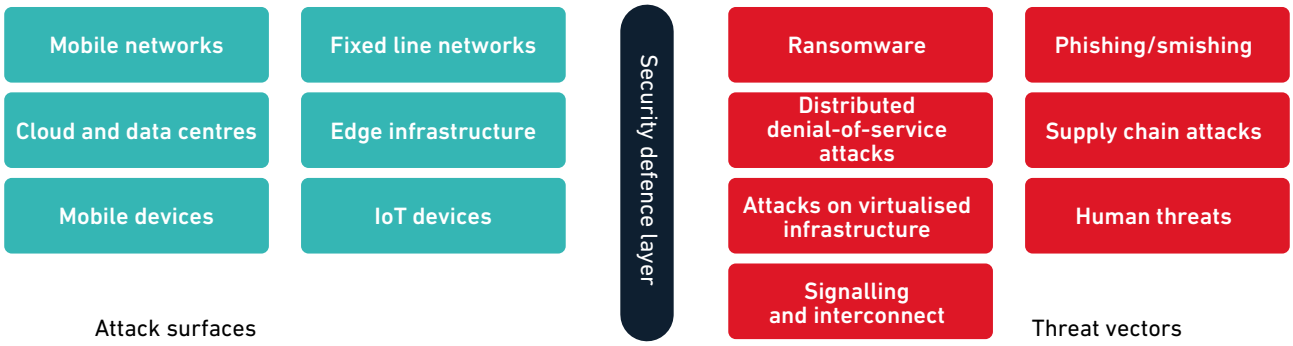
This research used a mixed methodology, with data inputs drawn from multiple sources:

- a new survey of telecoms operators across the world (N=120)
- 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

2

The telecoms environment and its bearing on security

2.1 5G adoption and the monetisation imperative

In Europe, attention is shifting to 5G monetisation, as operators seek returns on their significant capital outlays. The transition to 5G standalone (5G SA) is providing further impetus to monetisation efforts by introducing new capabilities, including improved support for network slicing. Private 5G deployments are also gaining traction in Europe, offering opportunities to create new revenue streams and serve additional enterprise customers.

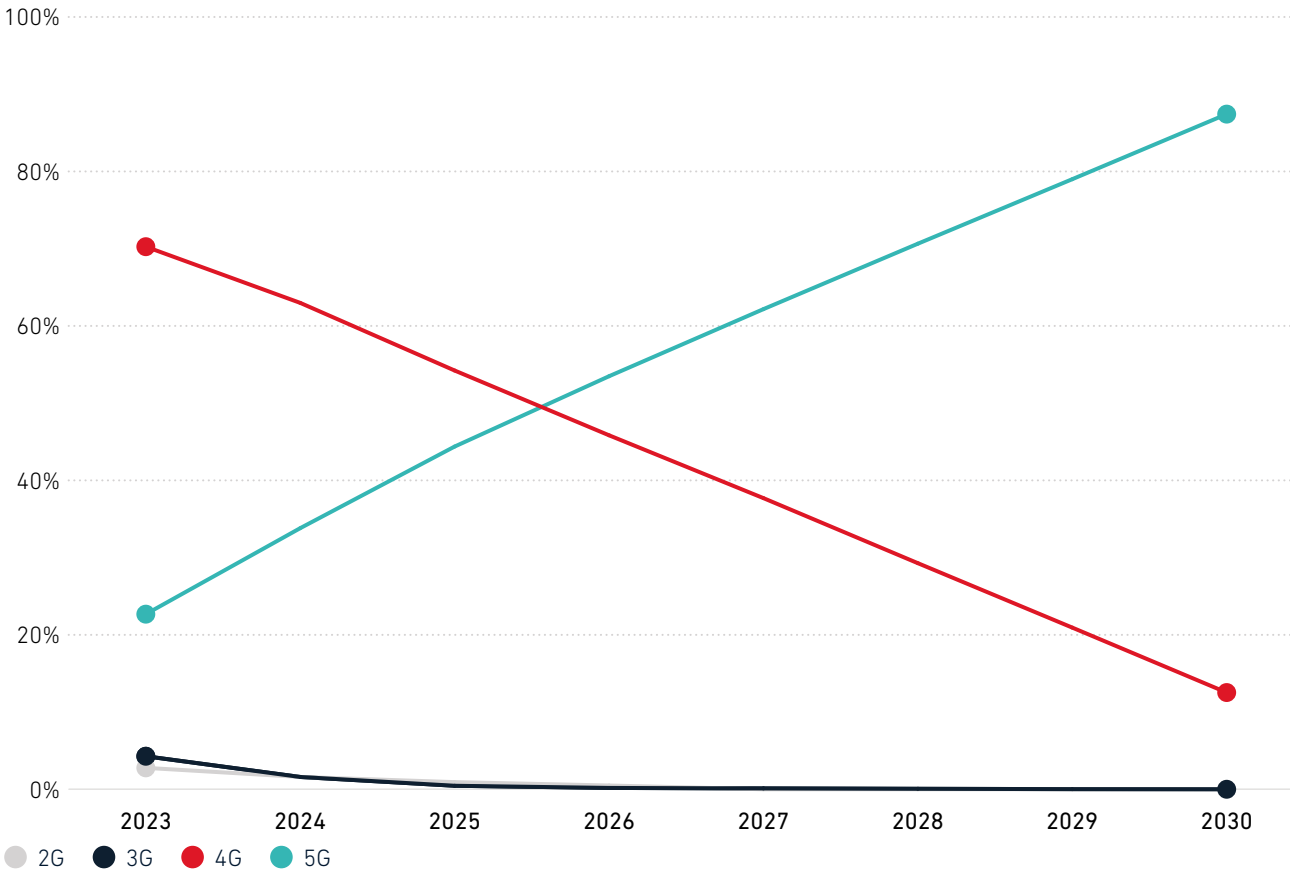
5G is set to dominate in terms of percentage of total connections by 2026. It is forecast to reach 87% of total mobile connections in Europe by 2030. Most countries in the region will see 5G adoption rates surpassing the global average of 54% of total mobile connections. Leading markets such as Germany and Finland are forecast to exceed 90%.[1]

Meanwhile, 2G and 3G networks are being phased out. For example, in the UK, all network operators have pledged to turn off 2G and 3G networks by 2033. Across Europe, 3G is likely to be switched off before 2G.

Figure 3

5G will be the dominant mobile technology in Europe by 2026

Percentage of total mobile connections



Source: GSMA Intelligence

1 The Mobile Economy Europe 2023, GSMA Intelligence, 2023

Table 1

Country-level subscriber and technology trends for key markets in Europe

	Finland		France		Germany		Italy		Poland		Spain	
	2023	2030	2023	2030	2023	2030	2023	2030	2023	2030	2023	2030
Mobile subscriber penetration	92%	93%	86%	88%	87%	89%	89%	90%	87%	89%	88%	90%
Smartphone adoption	87%	92%	86%	94%	82%	93%	79%	88%	78%	89%	80%	86%
Technology mix												
2G	1%	—	1%	—	3%	—	4%	—	5%	—	4%	—
3G	2%	—	8%	—	—	—	4%	—	9%	—	7%	—
4G	61%	6%	72%	10%	61%	5%	76%	14%	75%	24%	71%	9%
5G	36%	94%	18%	91%	36%	95%	15%	86%	11%	76%	18%	91%

Note: totals may not add up due to rounding

Source: GSMA Intelligence

The EU and cybersecurity strategy

Cybersecurity policies and General Data Protection Regulation (GDPR) are key components of Europe's strategy to protect its digital infrastructure and the personal data of citizens.

The EU Cybersecurity Act, which came into force in 2019, established a framework for the certification of ICT products and services to achieve a common level of cybersecurity across the EU by strengthening the role of the European Union Agency for Cybersecurity (ENISA). ENISA helps member states address common cybersecurity issues, supporting the reporting process for cybersecurity and implementation of the EU's Network and Information Systems (NIS2) Directive.

The NIS2 Directive aims to set cybersecurity goals across member states. It is a legally binding act of the European Union that establishes a set of cybersecurity objectives that all EU member states must fulfill. Each member state is free to choose how the required objective is fulfilled. The goal of the NIS2 Directive is to improve the status of cybersecurity across the EU by increasing harmonisation of cybersecurity requirements and obligations. It also encourages member states to introduce new areas such as vulnerability management, supply chain and cyber hygiene to their national cybersecurity strategies. The NIS2 Directive states that responsibility for determining penalties for non-compliance lies with the individual member states, not the EU. Under the directive, operators may be asked to provide the materials and information needed to assess the security of their network and information structure.

To complement the NIS2 framework, in March 2024, the European Parliament approved the Cyber Resilience Act (CRA), which addresses two main issues. Firstly, it is targeted at the inadequate level of cybersecurity inherent in many products. Secondly, it addresses the inability of consumers and business to determine which products are cybersecure. The objectives are to create conditions for the development of secure products with digital elements by ensuring hardware and software are placed on the market with fewer vulnerabilities; and create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.[2]

Many European countries have developed and implemented their own national cybersecurity policies to address unique challenges and bolster their digital defences. For example, Germany's IT Security Act 2.0 introduced stringent requirements for critical infrastructure operators, mandating regular security audits. Similarly, France's National Cybersecurity Strategy aims to enhance the country's cyber defences through increased investment in cybersecurity infrastructure and a focus on workforce upskilling.

2 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

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 network assets that make up the attack surface. This report series considers a range of network assets, including fixed and mobile networks, edge computing, cloud data centres, IoT and mobile devices.

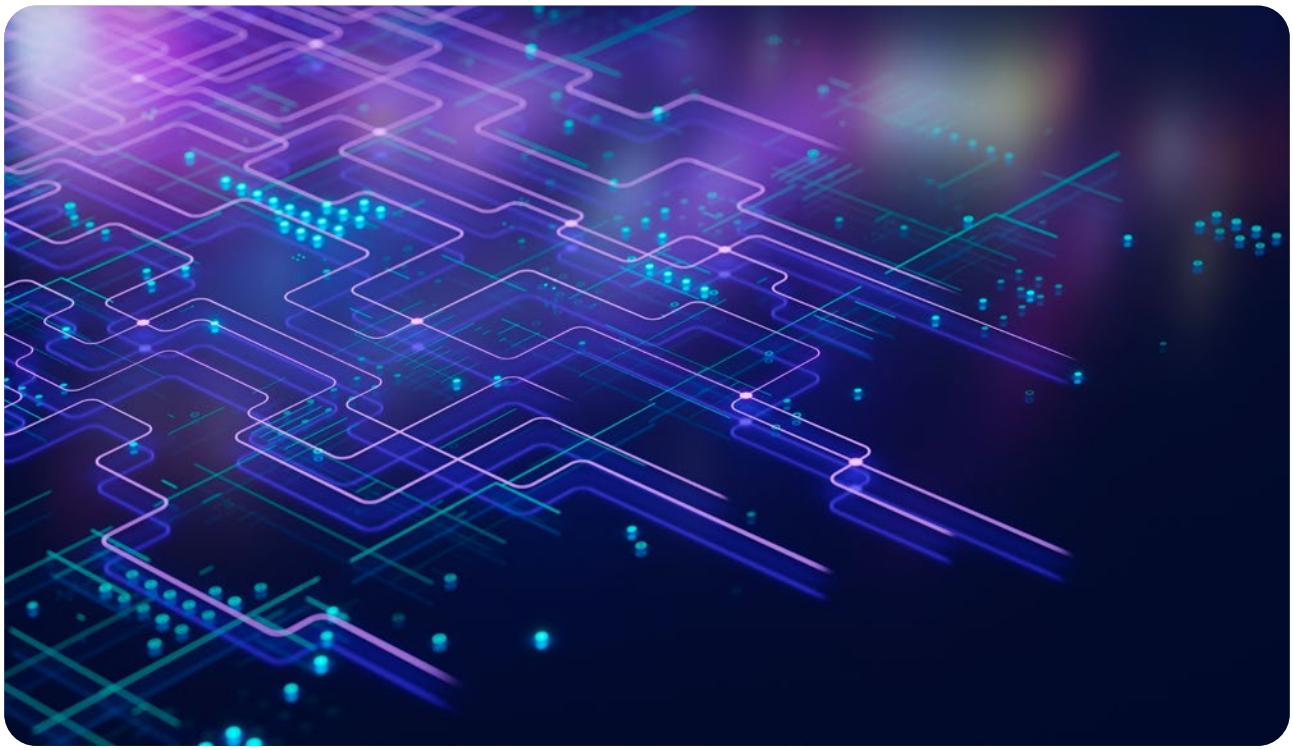
Cybersecurity attacks on these are complex, wide-ranging and constantly evolving. As new technologies emerge (such as software-defined mobile networks and AI), malicious actors continue to adapt. New threats and sources of attack are emerging around the world.

Cyberattacks can inflict severe damage on operators, including customer/financial loss and reputational impact. 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 such as 'living off the land' or 'lone wolf' attacks.

In Europe, threat actors include criminal organisations with considerable funding and resources. These groups often belong to transnational crime cartels that operate at least partially online. Reflecting this reality, 95% of surveyed operators in Europe identify structured criminal groups as the primary source of cybersecurity threats in the region. The dark web continues to be a key enabler for cybercrime, allowing offenders to share knowledge, tools and services. AI and machine learning-based tools and services are increasingly being exploited by cybercriminals, fuelling the growth and competitiveness of the 'cybercrime-as-a-service' market.

The GSMA Intelligence security survey of telecoms operators in Europe reveals the following:

- The perceived threat level is highest for mobile and IoT devices. However, 70–80% of operators surveyed rated their defences for these assets as either strong or very strong.
- According to the majority of operators surveyed, the financial and healthcare sectors are the verticals most exposed to potential cybersecurity threats.
- Phishing/smishing, ransomware and supply chain attacks are the top three threats impacting mobile networks.
- Despite stringent regulation and significant investments from operators, cybersecurity threats are rapidly evolving and are set to rise over the next three years.
- Collaborating with industry stakeholders to develop and implement security management and technical measures is crucial to ensure cyber resilience.
- Collaborating with regulatory authorities and cybercrime agencies is important to counter the cybersecurity threat.
- Investment in and deployment of AI-powered network security solutions is key to enhancing network defences. However, more edge compute is needed.



3.2 Operator perceptions of threat level by domain

Operators perceive there to be a significant threat level for mobile and IoT devices (see Figure 4). However, operators also have confidence in their readiness to defend against security attacks on mobile and IoT devices. Some 80% of operators rate their defences as either strong or very strong for mobile devices, while 70% rate their defences as either strong or very strong for IoT devices, which is well above the global average (see Figure 5). In general, European operators are more confident in their network defence capabilities than their global counterparts in terms of devices, fixed line networks and cloud assets

By establishing robust standards for data protection and cybersecurity, frameworks such as GDPR, NIS2 and the CRA have helped fortify Europe's digital landscape and spur a culture of compliance.

Operators in Europe have bolstered security for IoT devices by advancing network security technologies, enhancing integration between IoT devices and private mobile networks, and implementing zero-trust network principles. Operators involved in the development of IoT products and services can take advantage of the GSMA IoT Security Guidelines FS60[3] to increase their cyber defences.

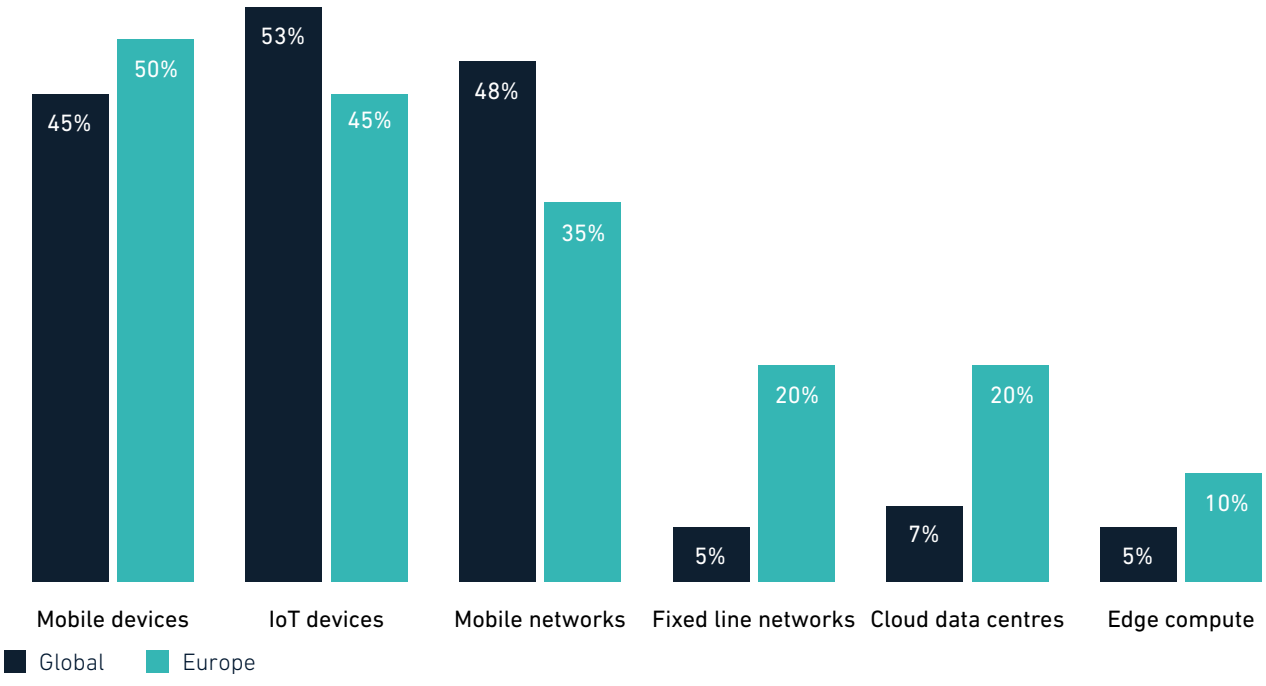
Since 2008, ENISA has provided training materials to raise awareness of cybersecurity and encourage behavioural change among end-users. Operator efforts and cooperation with ENISA have been key in supporting cybersecurity and enabling a safer digital environment. The collaboration has positively impacted operators' view of defences for non-core network assets such as IoT and mobile devices.

Figure 4

Half of operators in Europe rate the threat level as very high for mobile devices

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

Percentage of operators rating **very high**



Source: GSMA Intelligence

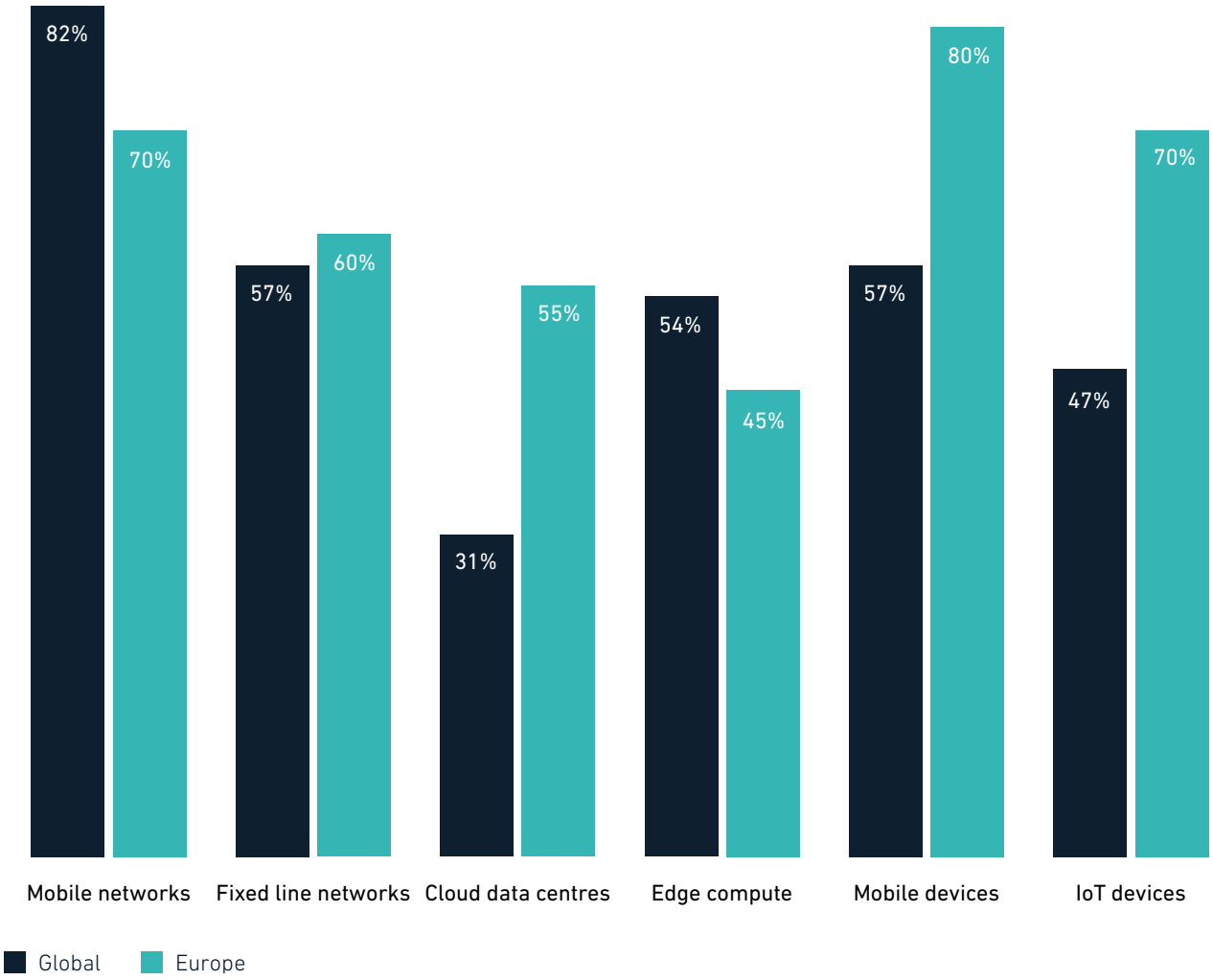
3 For more information, see GSMA IoT Security Guidelines Overview.

Figure 5

80% of operators rate their defences for mobile devices as either strong or 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 products and services?

Percentage of operators rating as **strong** or **very strong**



Source: GSMA Intelligence

3.3 Operator perceptions of threat level by vertical

Social engineering tactics and ransomware using email, SMS and calls can pose a significant threat to enterprise verticals, particularly financial services and healthcare. The financial services and payments sector is viewed by operators in Europe as most susceptible to attack, with 90% of operators acknowledging this vulnerability (see Figure 6). Attackers can gain access to sensitive financial data and exploit it for fraudulent activities. Similarly, in the healthcare sector, the ongoing digital transformation and handling of sensitive patient data make it a prime target for social engineering and ransomware attacks.

Operators can play a crucial role in supporting these verticals by providing robust cybersecurity solutions to mitigate such threats. Around 75% of European operators consider their security products and services to be highly effective in countering and preventing cyber threats related to financial services and payments (slightly below the global average of 85%). In healthcare, 70% of European operators believe their security measures to counter cyberattacks are strong or very strong (above the global average of 53%).

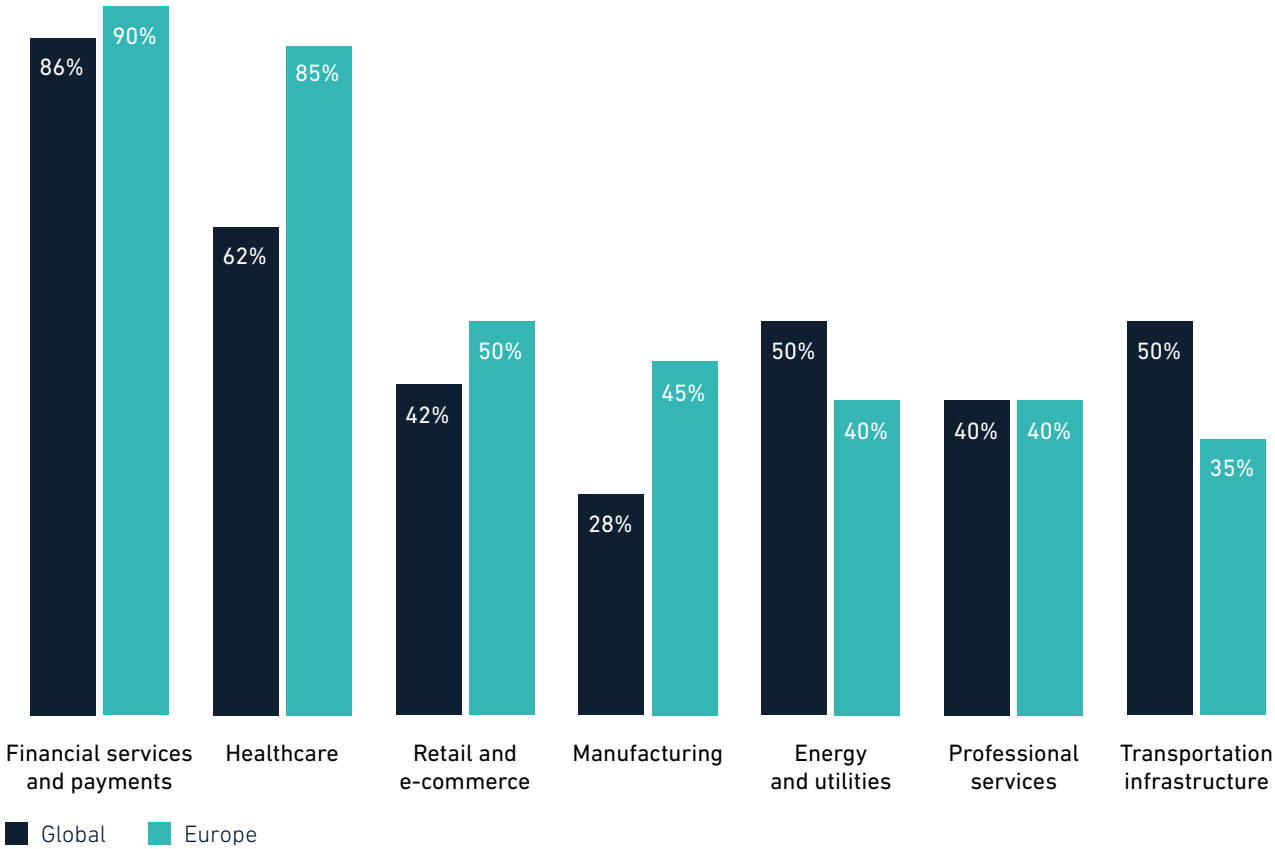
In today's digital world, the implementation of security measures is paramount across all industries. While deploying security products and services is essential, verticals need to also pay particular attention to security implementation, factoring in regulatory compliance, risk control measures and solution testing.

Figure 6

Financial services & payments and healthcare are rated as the top verticals exposed to cybersecurity threats

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

Percentage of operators rating as **high**



Note: Survey results for Ghana and Nigeria are not included in the data for Southern Africa, as they have been included in the data for Northern Africa.
Source: GSMA Intelligence

3.4 Operator perceptions of threat level by vector

Operators in Europe view phishing/smishing (phishing via SMS) and ransomware as the top two threats facing their mobile networks, with supply chain attacks slightly lower down the list but still concerning (see Table 2).

Over the next three years, 85% of operators expect an increase in phishing/smishing, while 70% anticipate an increase in ransomware incidents. Low entry barriers and the relative ease of deploying phishing/smishing campaigns via as-a-service infrastructure make these types of attack hard to eradicate. GenAI has increased the effectiveness and impact of phishing/smishing attacks by making them harder to distinguish and appear more legitimate. In terms of ransomware, the advent of bitcoin and other cryptocurrencies makes it possible to extort huge ransoms from large companies and organisations.

Some 60% of operators expect an increase in supply chain attacks over the next three years, reflecting the number of suppliers and possible attack vectors. Supply chain attacks can have devastating consequences for operators, such as reputational damage, downtime and financial/ customer loss. Supply chain attacks are also a significant cyber threat due to the large number of victims affected. For example, the supply chain attack that affected 3CX, a VoIP provider that was using corrupted software of another company, distributed malware to hundreds of thousands of its customers.[4] Securing the supply chain against cyberattacks is a complex task, requiring industry cooperation and equipment/ vendor assessment. The GSMA Network Equipment Security Assurance Scheme (NESAS)[5] helps operators mitigate some of the risks impacting the supply chain.

Table 2

Phishing/smishing is the top threat impacting mobile network in Europe

Considering the 2024 cybersecurity threat landscape and based on your expertise, please rank the top three major threats impacting mobile networks in your primary country of operation.

How do you anticipate the hazard level for the following cyber threat will be in three years compared to now?

	Global*	Europe*	Net threat rise in Europe over next three years**
Phishing/smishing	68%	60%	85%
Ransomware	49%	45%	70%
Supply chain attacks	32%	40%	60%

*Calculated as rank 1st *1 + Rank 2nd *0.66+ Rank 3rd*0.33
**Percentage of operators that rank the risk as being higher over the next three years minus the percentage that rank the risk as lower.

Source: GSMA Intelligence

4 Source: "The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks", Wired, April 2023
5 For more information, see GSMA Network Equipment Security Assurance Scheme.

Nuisance and fraudulent calls in Europe

Nuisance and fraudulent calls are a global issue. Specialist in fraud and spam calls, Hiya, flagged more than 19 billion spam calls in the first half of 2024.[6] Robocalling and caller ID spoofing make the problem worse.

In Europe, a mobile user receives on average one fraudulent call and three nuisance calls per month. The countries most exposed to spam calls are Spain and France.

Addressing caller ID spoofing can greatly reduce fraudulent calls. Authorities and operators in Finland have been working to tackle the problem. The response is based on a simple technical solution of filtering and information exchange among operators on whether a specific mobile subscription is currently abroad or not.

Table 3

Mobile users in Europe receive an average of one fraud call and three nuisance calls per month

	Monthly per user			Regional distribution*		
	Fraud calls	Nuisance calls	Spam calls	Fraud calls	Nuisance calls	Spam calls
Spain	2	9	11	19%	12%	13%
France	1	10	11	9%	13%	13%
Italy	0	9	9	0%	13%	11%
Poland	1	5	6	14%	7%	8%
Sweden	1	4	5	12%	5%	6%
Europe (average of all countries)*	1	3	4			

*Extrapolated
Source: Hiya

Preparedness: behind or ahead of the curve

Looking at the viable security risks helps understand where the industry sees itself as being behind or ahead of the curve (see Figure 7).

Although phishing/smishing and ransomware are major threats in the region, most operators have confidence in their ability to defend against such attacks. For example, 90% of operators view themselves as somewhat or very ready to defend against phishing/smishing. Some 55% of operators view themselves somewhat or very ready to defend against ransomware. A key question is whether and how operators will be able to keep up with threats of ransomware and phishing/smishing as they evolve and their intensity increases. This will require cooperation, threat intelligence sharing, use of industry tools such as NESAS and MCKB, implementation of internal security policies (ranging from staff vetting to incident response strategies) and investments to enhance IT skills and cybersecurity awareness.

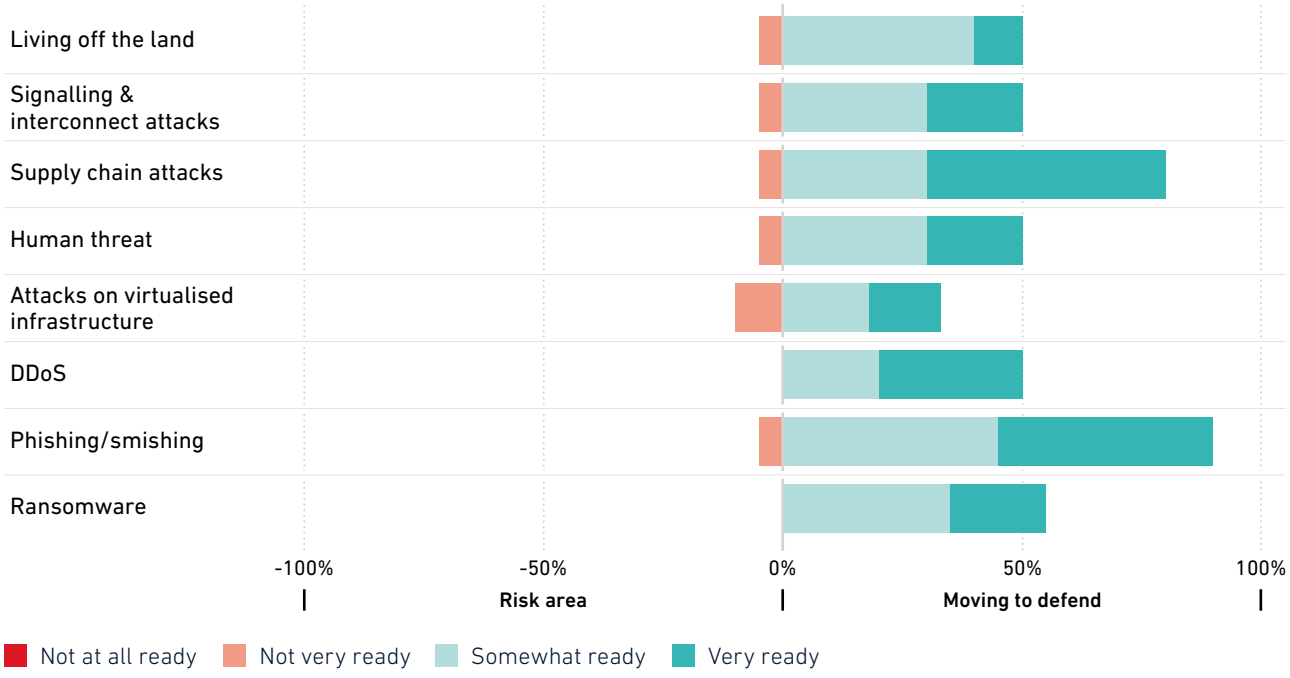
Most operators in Europe are ready to address less common types of cyber threats, such as living off the land and signalling & interconnect attacks. Approximately 80% of operators are ready to defend against supply chain attacks. By being ready, operators can ensure more resilient and reliable services.

Figure 7

Most operators are ready to counter cyber threats

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

Percentage of operators assigning readiness level to attack type (excluding operators rating as neutral)



Source: GSMA Intelligence

3.5 Operator perceptions of network security spend and the impact of legislation

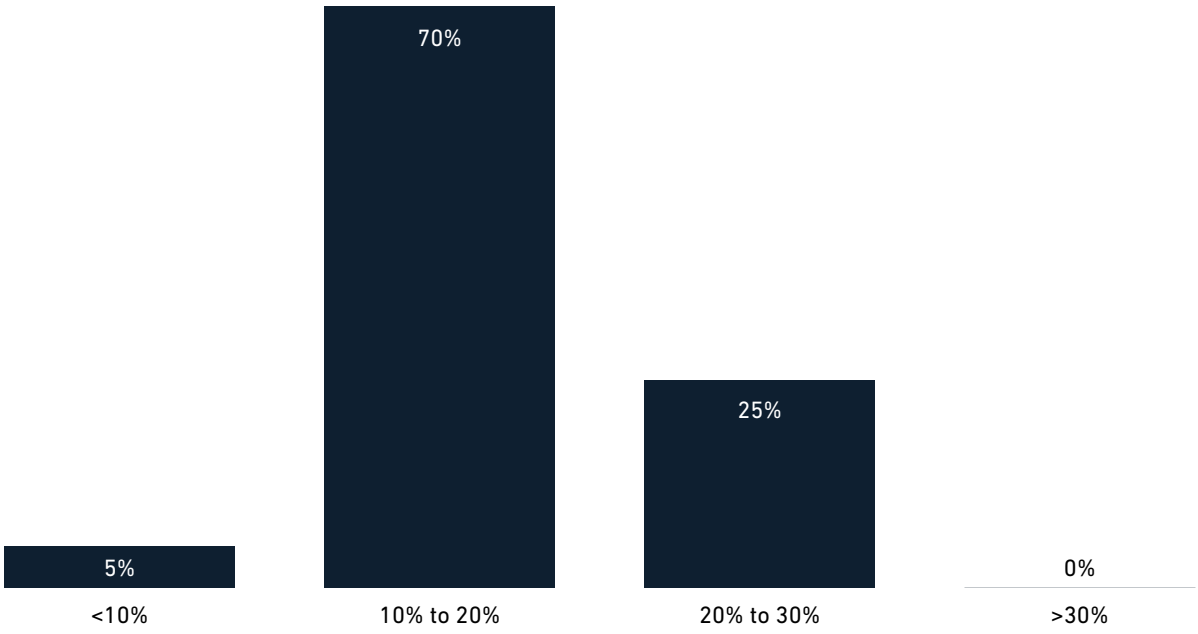
The digital age demands robust network security. Policymakers in Europe have responded by enacting stringent legislation aimed at bolstering cybersecurity. The efficacy of these regulations has been subject to debate, especially in the context of the significant financial burden faced by operators. GSMA Intelligence data shows that 70% of operators spend between 10% and 20% of their network opex on cybersecurity, while 25% of operators spend between between 20% and 30% (see Figure 8). This includes ongoing spend on security for mobile, fixed and cloud network assets.

Recent years have seen a flurry of legislative measures designed to enhance cybersecurity in Europe. While the frameworks aim to create a safer digital environment, they frequently impose rigorous compliance requirements on operators. This translates into substantial financial commitments, including hardware and software upgrades, regular cybersecurity compliance audits, employee training, hiring of skilled cybersecurity professionals, implementation of robust incident response teams, and investments in systems to manage potential breaches. The fast-changing threat landscape means defensive measures must constantly evolve, often outpacing legislation.

Figure 8

Some 70% of European operators spend 10–20% of their network opex on cybersecurity

According to your knowledge and thinking about cybersecurity threats in your primary country of operation, what is your approximate company spend on security (as a percentage of network opex) for your own network infrastructure? This would include mobile, fixed and cloud.



Source: GSMA Intelligence

Figure 9

Operators in Europe see regulations for network security becoming more stringent over the next three years

Over the next three years, how do you see government regulations for network security evolving in the countries your company operates in?

Source: GSMA Intelligence

Looking ahead to the next three years, all operators surveyed in Europe see government regulations for network security becoming more or significantly more stringent. This indicates an increasing focus on network security, which will likely drive innovation as telcos and their partners seek to develop more robust and efficient solutions to meet evolving requirements. A stricter regulatory environment will enable a safer digital landscape, which is essential to avoid financial and customer losses, damage to reputation, and theft/loss of sensitive data. By ensuring robust cybersecurity, operators can cultivate trust among consumers and enterprises. This solid foundation will help spur digital transformation, unlocking revenue opportunities.

3.6 Operator perceptions of AI's ability to bridge the security gap

Some 65% of operators in Europe believe AI will enhance network security (below the global average of 72%). While there is significant optimism around AI's potential to bolster security, there remains some scepticism or uncertainty around its effectiveness. Addressing concerns will be crucial to bridging the gap and achieving confidence in AI's role in enhancing network security.

AI offers the potential to enhance mobile network security through several capabilities:

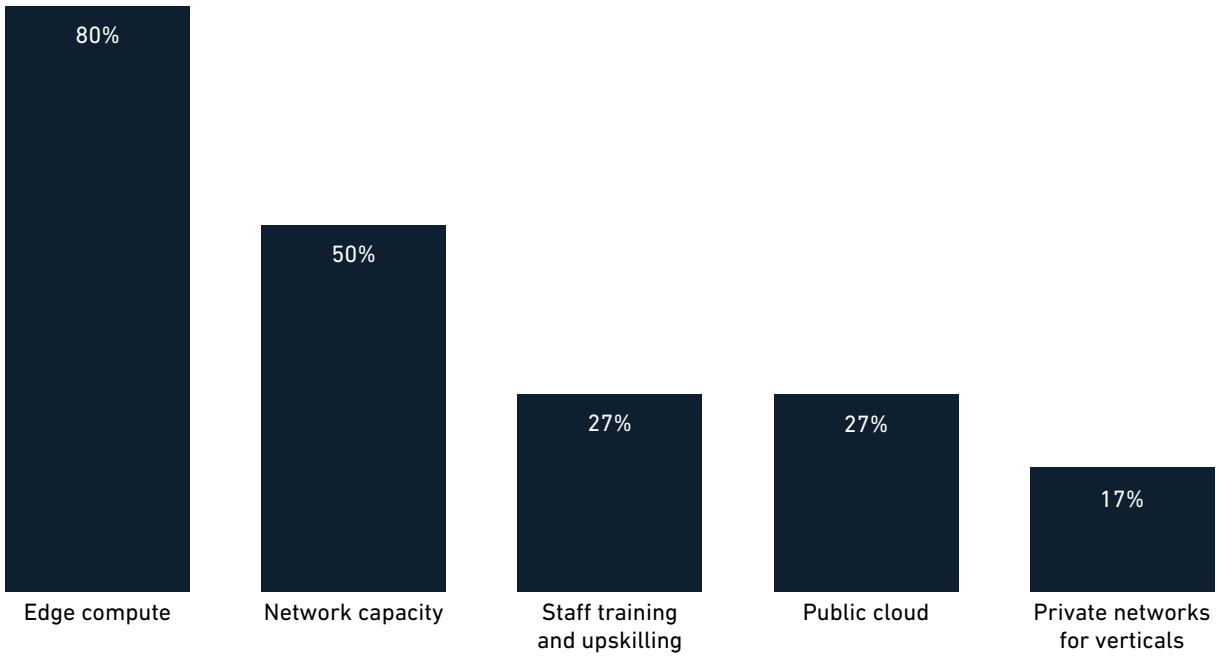
- **Automated threat detection and mitigation –** AI can significantly enhance the speed and accuracy of threat detection. By leveraging machine learning (ML), AI can analyse vast amounts of data in real-time, identifying patterns and anomalies that may indicate a security breach. When anomalies are identified, AI provides a mitigation response.
- **Adaptation to threat landscape –** AI can be trained to proactively spot new cyberthreats, through continuous learning. This adaptability ensures that mobile networks remain protected against the rapidly evolving threat landscape, which often outpaces legislative efforts.
- **Enhanced user authentication and data protection –** Techniques such as biometric authentication and AI-powered anomaly detection can provide multi-layer security.

Although AI offers some promising solutions, most operators surveyed in Europe remain in the testing or planning stages of AI adoption.[7] Among the major challenges of deploying AI at scale are technology maturity, uncertain returns and potential security vulnerabilities. To spur genAI deployment, increased investment in edge computing is a requirement for 80% of European operators (see Figure 10). This investment is essential to provide the low latency and security required for data processing.

Figure 10

Some 80% of European operators rate edge compute as an essential investment requirement for genAI

Which areas of investment will you need to make to support increasing use of genAI services across your customer base?



Source: GSMA Intelligence

7 Source: GSMA Intelligence Network Transformation Survey 2024

3.7 Operator perceptions of network security innovations

Figure 11 shows the various interventions operators can deploy to enhance network security. Over the past three years, adopting a secure-by-design approach and threat intelligence sharing have been key. Looking ahead to the next three years, the areas that require the most innovation are improving the security culture, implementing new security controls and proactive security testing. To innovate and inform in these areas, operators can leverage industry-wide tools such as the GSMA Mobile Cybersecurity Knowledge Base. They can also engage with stakeholders in industry communities such as GSMA T-ISAC and GSMA Fraud & Security Working Groups.

As shown in Figure 12, 65% of European operators claim they need most support to improve their vulnerability management processes to promptly address network security flaws.

Vodafone provides an example of an operator's efforts to improve the vulnerability management process. It has separated cybersecurity risks into three main areas of risk:

- **External –** Includes a variety of attackers that seek to gain unauthorised access to steal or manipulate data or disrupt services.
- **Insider –** Includes Vodafone employees who may accidentally or maliciously pose a security threat.
- **Supply chain –** Includes attacks that come from third-party service providers.

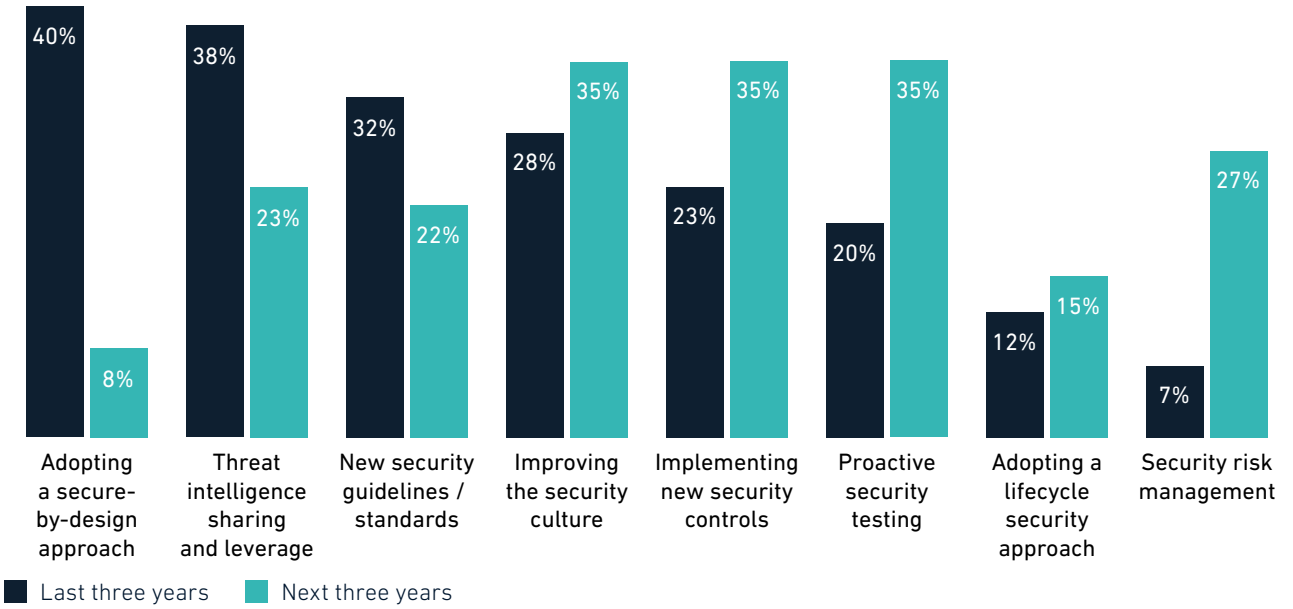
To help manage evolving risks, Vodafone continuously evaluates its business strategy, new technologies, government policies and regulations, and cyber threats. Vodafone produces regular reviews of the most significant security risks affecting its business and develops strategies and policies to detect, prevent and respond to them. When incidents do occur, Vodafone identifies the root causes and uses them to improve their controls and procedures.[8]

The GSMA's Coordinated Vulnerability Disclosure (CVD)[9] programme is one of the methods used in the mobile industry.

Figure 11

Embracing a secure-by-design methodology and threat intelligence sharing are crucial to maintaining security among operators in Europe

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?



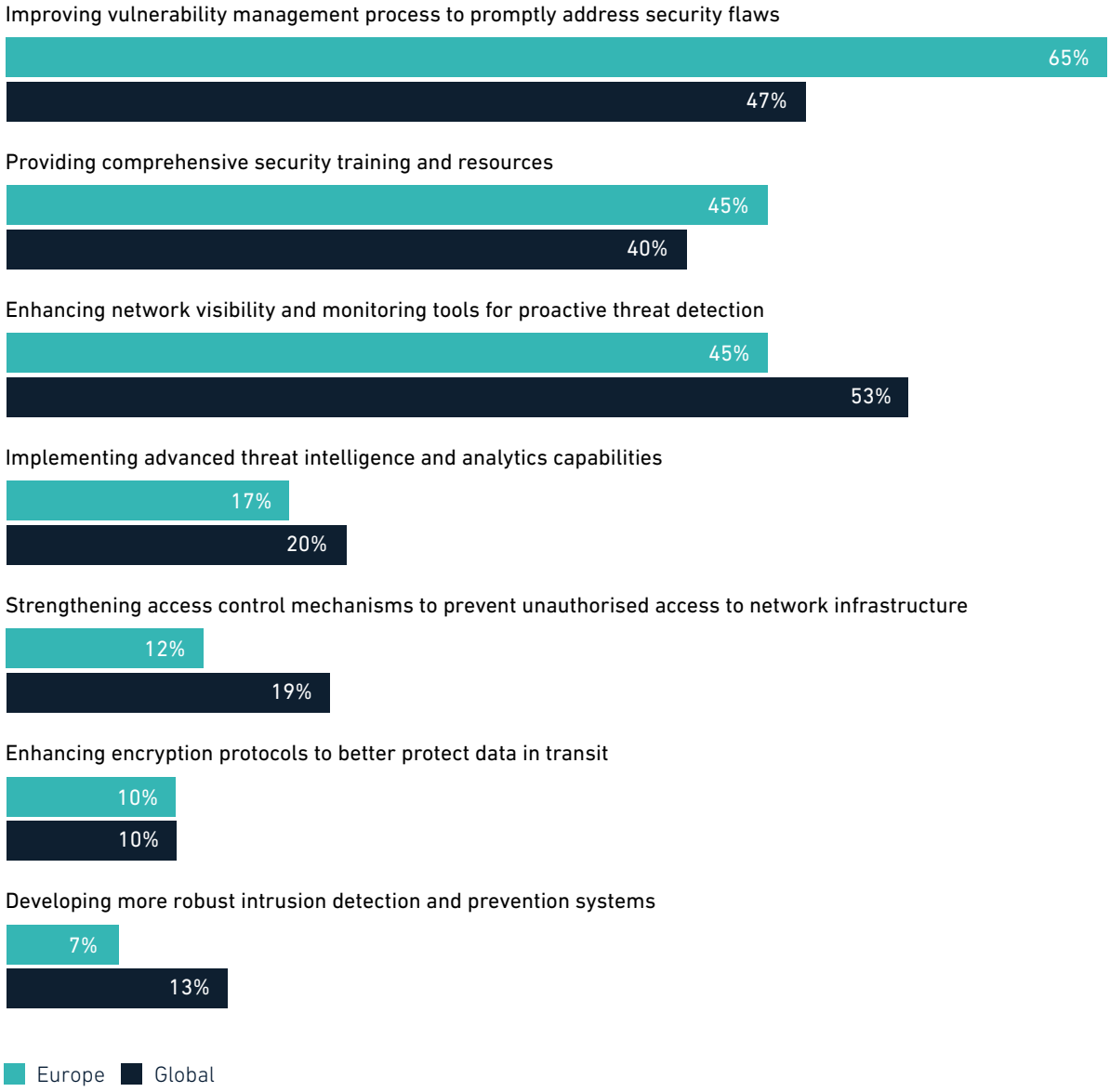
Source: GSMA Intelligence

8 Vodafone Cyber Security Factsheet 2024
9 See CVD programme

Figure 12

Improving vulnerability management and enhancing network visibility for proactive threat detection 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?



Score calculated as Rank 1st*1+Rank 2nd *0.66 + Rank 3rd *0.33
Source: GSMA Intelligence

4 Ensuring security readiness

4.1 Measures to counter the threat

Europe faces a dynamic and evolving cybersecurity landscape, with a range of threats targeting various sectors and critical infrastructure. Most cybercrime attacks in Europe are carried out by structured criminal organisations, suggesting threats not limited to a specific region or country.

AI offers both opportunities and challenges for cybersecurity. While AI can enhance threat detection and mitigation capabilities, it can also be exploited by cybercriminals to conduct more sophisticated attacks. The proliferation of smartphones, IoT and 5G networks brings enhanced connectivity but also introduces new security concerns.

While legal frameworks, cybersecurity awareness and education, and investments play a crucial role in mitigating these challenges, operators can implement several 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.

5 Innovation from telecoms operators

Operators face an ongoing requirement to improve network security controls to keep pace with security challenges. The appropriate levels of security investment in new areas and in maintaining existing controls depend on many factors, but the trend towards greater investment in network security is clear across Europe.

5.1 Leveraging industry-level tools and resources

Securing the supply chain

Selecting and testing vendors and products is key to network security. As an example, Vodafone assesses the cybersecurity of its suppliers and third parties. Controls and procedures are embedded in the supplier lifecycle to set requirements, assess the risk and monitor each supplier's security performance.

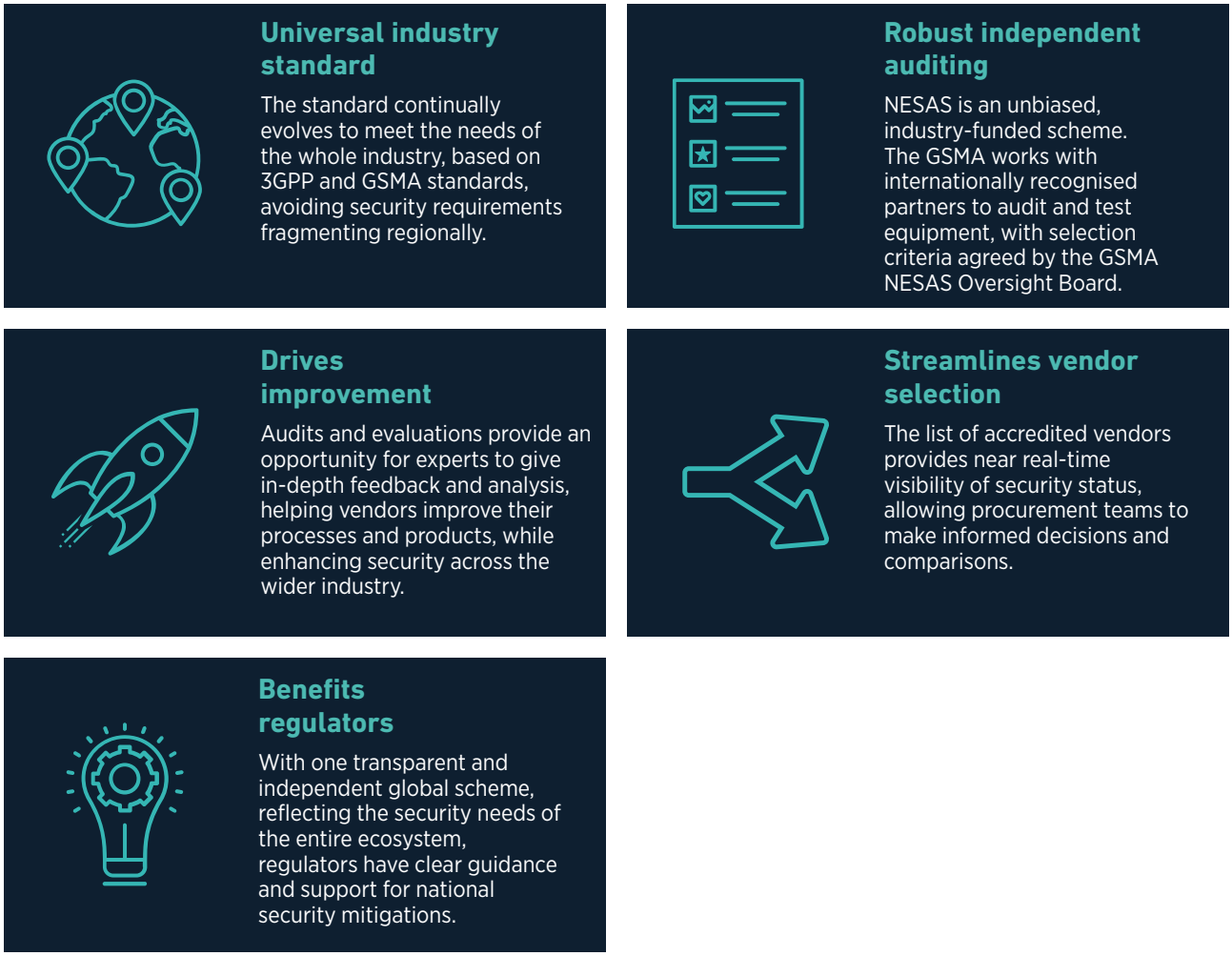
At supplier onboarding, minimum requirements are written into contracts. Vodafone determines the inherent risk of the supplier based on the service provided. Supplier and third-party controls and procedures are then assessed using a questionnaire to understand any residual risk, which informs the

frequency of review, from annual to every three years. Vodafone then follows up on open actions and ensures any security incidents are tracked and managed.

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 13.

Figure 13

The NESAS framework provides a universal industry standard for network security



Source: GSMA[10]

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. This is crucial as operators evaluate introducing new network suppliers as part of their 5G rollout plans.

10 See NESAS

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:

- **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.[11]

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 standalone (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.

11 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.

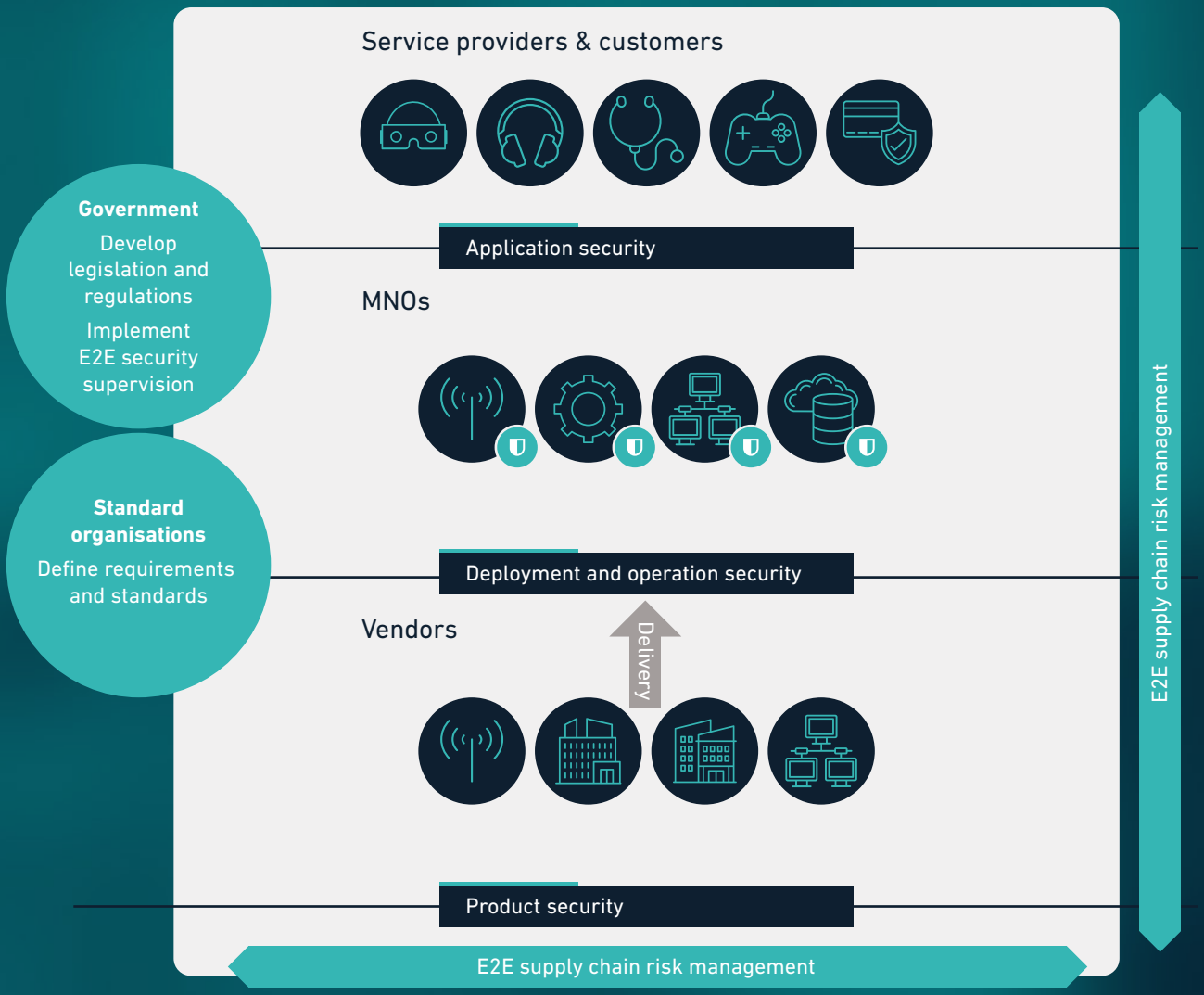
The Knowledge Base facilitates and encourages collaboration to protect networks and services against disruption and unauthorised access, as well as the prevention and mitigation of risks. It will help enhance mobile security competencies and capabilities, and will strengthen the work of operators, enterprises, 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 that 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, 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 11

Cybersecurity is a shared responsibility



Source: GSMA[12]

12 See Network Equipment Security Assurance Scheme (NESAS)

Establishing business controls

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.[13] These controls are not always technical and might pertain to reporting or communication practices critical for operators to improve their security posture. Table 4 highlights some of the key measures along with relevant examples from European operators.

Table 4

Examples of baseline security controls in Europe

Baseline security controls		Operator example
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 senior standing. Their role must be able to influence and direct enterprise-level investment and change.	BT has brought together cyber, physical and personnel security teams into one function under a new expanded Executive Committee role of Chief Security and Networks Officer.
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.	All KPN employees must abide by the company's Code of Conduct, which provides clear privacy guidance, including how to deal with customer information. Employees must also perform KPN's privacy awareness e-learning training every two years.
Developing business continuity management (BCM) plans.	BCM improves the resilience of an organisation by developing its 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 recover and return to business as usual.	Telefónica applies privacy and security by design, meaning that privacy and security are incorporated into the initial concept of its products/services and subsequently throughout the development process.
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).	Telia's security governance is constantly developed and improved in alignment with standards and best practices such as ISO/IEC 27001, NIST Cybersecurity Framework (CSF) and CIS Critical Security Controls (CSC).

Source: GSMA Intelligence, operator annual reports and websites

13 For more information on business controls, see the GSMA's FS.31 GSMA Baseline Security Controls

Improving intelligence sharing

Contributing to relevant sharing communities is another way operators can defend against security threats. The sharing of information between mobile operators is most commonly achieved 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 near real-time. T-ISAC also allows its members to share best practice with each other in a trusted environment, bolstering the security of operators and their partners.[14]

Furthermore, the GSMA's Fraud and Security Group (FASG) 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 on the effectiveness of deployed security and fraud controls. Many European operators highlight the FASG's importance in mitigating a range of threats.[15] The GSMA also facilitates regional FASGs focusing on local fraud campaigns through threat intelligence sharing.

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.

Operators also engage in non-industry-specific intelligence sharing communities. Telenor, for instance, is an active member of the Information Security Forum, contributing strategically as a council member and collaborating with vendors and partners to share intelligence. Additionally, operators participate in national initiatives such as Deutsche Telekom's membership of the Alliance for Cyber Security, a platform created by Germany's Federal Office for Information Security and Federal Association for Information Technology (Bitkom) to share knowledge on cybersecurity risks.

14 GSMA members can join T-ISAC
15 See for example www.telenor.com/about/corporate-governance/cyber-security/

5.2 Navigating 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 compulsory security training, staff vetting, additional administrator controls and operating a 'least privilege regime'. Additionally, operators have introduced a number of initiatives to bolster the number of cybersecurity professionals in their field amid the global shortage in cybersecurity talent.

For example, BT supports the UK National Cyber Security Centre's CyberFirst programme, which aims to encourage school pupils to pursue cyber and tech careers, hosting events for more than 2,000 pupils in the UK. Furthermore, the operator continues to offer its reskilling programme CAPSLOCK, helping existing employees transition into security roles. Everyone who has graduated from the programme now has a BT Group security job. The initiative won the award for Recruitment and Workforce Planning Strategy at the HR Excellence Awards 2022.[16]

CASE STUDY FROM FINLAND

Elisa enhances employees' understanding of cybersecurity threats

Challenge: Phishing scams are designed to trick employees into disclosing confidential information, which can result in security violations, financial damage and data breaches. These threats are especially relevant to telecoms operators due to the sensitive information they handle. It is therefore essential for operators to provide comprehensive security training to employees to safeguard their operations and customers.

Solution: Elisa enhanced its security posture by hiring a third-party firm that specialises in security awareness and phishing training.[17] The firm trained Elisa's staff using personalised phishing simulations, adjusting for employees' skills and backgrounds to keep the training relevant and challenging for everyone.

Impact: Over the past six years, Elisa has maintained a phishing simulation failure rate below 2% and an engagement rate over 70%. This gives Elisa a resilience score above 33, which surpasses most companies globally.[18] Elisa's real threat reporting rates are also high, helping combat threats such as ransomware.

16 BT Group plc Annual Report 2024
17 "How Elisa built awareness into the security stack to boost detection and response while preventing breaches", hoxhunt.com
18 Resilience score is engagement divided by failure rate

5.3 Tackling fraud and malware attacks

Minimising SMS and voice fraud

SMS and voice fraud has emerged as a major concern for operators and their customers due to increasing attempts by criminals to use deceptive text messages to steal personal information, money or install malware. These text messages are often disguised as legitimate communications, making it difficult for individuals to spot potential scams. To help combat rising levels of fraud, Orange recently launched its Cybersecure portal, enabling both Orange and non-Orange subscribers to check the legitimacy of suspicious sites, links, emails and SMS.[19]

SMS firewalls are also a key part of an operator's defence against fraudulent SMS traffic.[20] For instance, Vodafone implemented a new SMS firewall in September 2021. During its first full month of operation, it blocked a total of 18 million fraudulent SMS messages – all in real-time.[21]

Operators are also investing in solutions to prevent voice fraud, including voice firewalls to evaluate voice traffic and block calls to minimise the impact of vishing on the end user. Voice firewalls can be employed alongside complementary solutions such as branded caller display, which allows organisations to display their brandname or logo on the recipient's phone.

The example of BT's Enhanced Call Protect highlights how 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 phone call in real-time, enabling a swift response to emerging threats. BT's solution, deployed in partnership with Hiya, has stopped more than 20 million scam and spam attempts in the first four months since it was introduced in May 2024.[22]

CASE STUDY FROM FRANCE

Operators step up efforts to combat spoof calling

Challenge: Fraudsters can manipulate the calling line identifier (CLI) to make their calls or SMS appear as though they are coming from a trusted number. In reality, the communications often originate from a different number, undermining trust and increasing the risk of fraud.

Solution: Regulators in a growing number of countries are adopting measures to combat spoofing practices. For example, Arcep has mandated STIR/ SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted Information Using toKENs) protocols for all national SIP traffic in France. This authenticates and verifies the identity of callers by having their caller ID 'signed' as legitimate by originating operators and validated by other operators before reaching consumers.

In January 2024, SFR (part of Altice France) announced the successful production deployment of the STIR/ SHAKEN framework, following work in 2023 to test and prove end-to-end interoperability with other French operators.[23] The deployment builds on previous STIR/SHAKEN deployments in North America, which have helped reduce unwanted robocalls.[24]

Impact: The mobile industry has seen a range of different approaches seeking to improve the validity of the CLI as a response to the rapidly growing threat from CLI manipulation.[25] The deployment of STIR/SHAKEN in France will provide important learning points for identifying the best approach for improving CLI validity in different situations.

19 "Orange launches 'Orange Cybersecure', a comprehensive cybersecurity solution for all French citizens", Orange, June 2024
20 See GSMA FASG security guidance on firewalls and other topics.
21 "How Vodafone protects its customers from scam calls and texts", Vodafone, November 2021
22 "BT's new home phone scam protection service stops 20.1 million scam and spam attempts in first 4 months", BT, October 2024
23 "Second Largest French Telecommunications Company SFR and Titan.ium Platform Partner to Reduce Phone Number Spoofing", GlobeNewswire, January 2024
24 "TNS 2024 Robocall Investigation Report: STIR/ SHAKEN Implementation paying off for top US carriers", GSMA, February 2024
25 "Improving CLI Validity – Solutions and Regulatory Assessment", GSMA, October 2023

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. Operators can also provide businesses with an API to verify recent SIM swaps.

CASE STUDY FROM SPAIN

Spanish operators launch GSMA Open Gateway APIs

Challenge: Figures from Spain's Interior Minister show that reported cases of cybercrime increased by 72% in 2022 compared to 2019, with almost 90% of them related to online fraud.[26] Cybercrime now accounts for around a fifth of all offences registered in the country.[27]

Solution: GSMA Open Gateway is a common, open framework between operators to make it easier for developers and cloud providers to build safer apps and services that seamlessly communicate with each other and work for all devices and customers. This is achieved through single access points to mobile networks, known as APIs.

In December 2023, Spanish operators Orange, Telefónica and Vodafone announced the launch of two Open Gateway APIs focused on improving digital security:

- SIM Swap, which checks the last time the SIM card associated with a mobile number was changed
- Number Verify, which enables the authentication of a mobile device by the mobile network.

Impact: Second-hand fashion e-commerce retailer Vinted is among the early adopters to have integrated the GSMA Open Gateway Number Verify API into their security framework. This adds an additional layer of security to Vinted's authentication processes to reduce the risks to its customers. The tool also simplifies the identification process, making the consumer experience more convenient and straightforward. [28]

Evidence from Spain highlights the potential of GSMA Open Gateway to combat digital fraud. In total, 53 operator groups have joined the initiative, representing 245 mobile networks and accounting for 67% of mobile connections globally. Europe is the leading region with committed operators representing a quarter of the entire global addressable base despite accounting for only 10% of mobile connections.

26 "Minister: 1 in 5 crimes in Spain now committed online", AP News, February 2023
27 Ibid
28 https://opengateway.telefonica.com/en/resources/documents/case-study/vinted-security-registration

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 offering digital security solutions to subscribers. 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).

Many operators in Europe offer digital security solutions with varying features and capabilities. Telefónica Germany, for example, began offering a network-based security solution to its subscribers in September 2024.[29] The solution detects and blocks malicious activity in real time using advanced machine learning algorithms and behavioural analysis. To encourage adoption, Telefónica Germany offers all customers a one-month free trial of the service. DNA is among the operators in Europe to offer an endpoint security solution. Its DNA Digiturva service shields against security threats, safeguarding all devices, personal data, passwords and internet activity. The service operates on mobile devices through a single app and is also available for use on desktop computers.

CASE STUDY FROM ITALY

WindTre provides subscribers with a range of security tools

Challenge: A survey of adult internet users in Italy found that 53% were concerned about distinguishing between real and fake content online, while 34% worried about how companies might use their personal data.[30] Despite these concerns, fewer than 1 in 5 adults use security tools (e.g. VPNs) when accessing the internet.[31] This underscores the need for greater adoption of cybersecurity measures, especially as online threats grow more sophisticated.

Solution: WindTre, in partnership with a third-party security vendor, offers subscribers two cybersecurity plans. The entry-level plan is a network-based solution that provides safe browsing on the WindTre network for €0.99 per month. For €1.99 per month, the WindTre Security Pro+ plan offers both network-based and end-point security. It provides protection on both the WindTre network and public or private Wi-Fi, offering malware scanning for emails, apps and files. It also monitors the dark web for potential email and password breaches and includes a VPN for secure, anonymous browsing.[32]

Impact: The WindTre example demonstrates how partnerships between operators and security vendors can enhance protection for subscribers while providing operators with the opportunity to generate additional revenues and enhance customer satisfaction.

29 "O2 Telefónica Germany Launches 'o2 Onlineschutz' in Collaboration with Whalebone", Whalebone, September 2024
30 Digital 2024: Global Overview Report, DataReportal, 2024
31 Ibid
32 For more information, see "CKH Innovations Opportunities Development Partners with Bitdefender to Provide Mobile Security Services", CKH IOD, October 2022

5.4 Safeguarding against operational attacks

Reinventing the security operations centre

Security operation centres (SOCs) provide continuous prevention, protection, detection and mitigation of cyber threats. In some cases, European 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 instance, Swisscom has implemented a Security Orchestration Automation and Response (SOAR) solution which helps automate repetitive tasks by linking case management systems with security tools, asset databases and ticketing systems. This enables SOC analysts to focus more on higher-value activities, enhancing the efficiency of Swisscom's SOC.[33]

Operators are also harnessing genAI to enhance SOC automation and improve their overall security posture. For instance, BT is utilising genAI to sift through thousands of internal and external documents, enabling the visualisation of potential attacks and streamlining the work of security analysts.[34] Many extended detection and response (XDR) solutions also now integrate genAI assistants to help operators swiftly detect and neutralise threats.

CASE STUDY FROM GERMANY

Deutsche Telekom bolsters cyber defence capabilities with new SOC

Challenge: Deutsche Telekom faces 30,000 to 40,000 attack attempts every minute – a number that is rising as AI is increasingly harnessed to develop, enhance and manage more of these attacks.

Solution: In response to the increasing number of attacks generated, Deutsche Telekom has opened a new Master Security Operations Center in Bonn, Germany. More than 250 cybersecurity experts in the Master SOC monitor Deutsche Telekom's systems and those of its customers, ensuring a robust and vigilant defence against cyber threats.

The SOC automatically analyses billions of security-related data points from 250,000 sources.[35] Deutsche Telekom also assesses up to 95 million daily attempted attacks on its decoy traps live, integrating these insights into the Threat Intelligence database, which is among the most comprehensive in Europe.[36]

Impact: The building of a new SOC highlights Deutsche Telekom's commitment to safeguarding its infrastructure, protecting customer data and maintaining trust and reliability amid an increasingly challenging cybersecurity landscape.

33 Telco Security Landscape 2023, ETIS, 2023
34 "BT execs explore AI role in evolving threat landscape", Mobile World Live, September 2024
35 "Telekom expands protection center", Telekom, September 2024
36 Ibid

Protecting interconnect and signalling networks

Leading operators are deploying signalling firewalls that support multiple security protocols. In Belgium, for example, Telenet has deployed a signalling firewall covering both Signalling System 7 (SS7) and Diameter networks.[37] This helps prevent a range of attacks, including data theft, identity spoofing, location tracing and denial-of-service attacks.

There are also ongoing efforts to improve signalling threat intelligence sharing among operators and vendors. The GSMA has 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.

Additionally, the GSMA's Global Title Leasing Code of Conduct serves as a reference document for the leasing of Global Titles within SS7 networks, detailing motivations and usage while setting a code of conduct to prevent abuse and minimise risks for mobile operators and their customers.[38] Deutsche Telekom is one of the first telecoms operators to publicly commit to adopting the code of conduct.[39]

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 common 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). Several operators in Europe offer a DDoS protection 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. This can help operators grow their enterprise service revenues while enhancing overall network security.

37 "Telenet selects Infradata and BroadForward to enable converged signalling firewall solution", BroadForward, December 2019
38 See FS.52 – Global Title Leasing Code of Conduct
39 Threat Intel in Telecoms (TTIS 2024), Hardenstance, 2024

Appendix

Defining Europe

The following countries are classified as being part of Europe for the purposes of this research: Albania, Andorra, Austria, Belgium, Croatia, Czechia, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands. Norway, Poland. Portugal, Romania, San Marino, Spain, Slovakia, Slovenia, Sweden, Switzerland and UK.

This does not conform to the United Nations geo scheme; rather, it is a designation for the purposes of this research.

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.

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.[40]

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 (DDoS) attacks

DDoS attacks 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.

40 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.[41]

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.[42]

41 Global Call Threat Report, Hiya, 2023
42 Global Call Threat Report, Hiya, 2023

gsmaintelligence.com

GSMA
Intelligence

gsmaintelligence.com