GSMA

# The Impact of Cybersecurity Regulation on Mobile Operators

**November 2025**

GSMA

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**

frontier economics

Frontier Economics is a leading international specialist economics consultancy. Frontier uses economic principles to provide clear advice and analysis on complex matters to many of the world's largest companies, leading sector regulators, government departments and international organisations. With over 350+ staff in Dublin, Amsterdam, Berlin, Brussels, Cologne, London, Madrid, Paris and Prague, Frontier Economics Limited (www.frontier-economics.com) is one of the largest and most influential economic consulting firms in Europe. Our practitioners are renowned experts across a full range of industries, including digital markets, telecommunications, energy, transport, post, water and health, having advised both public and private sector stakeholders on the design and implementation of best practice regulatory policies, taking into account the likely impact of these policies on the behaviour of stakeholders and hence on markets more generally. Frontier works closely with its sister and legally separate company, Frontier Economics Australia.

# Contents

# 01.
# Executive summary

## Mobile connectivity and cybersecurity in a digital world

Mobile connectivity is central to modern economies and societies. It enables communication, access to information and public services, and economic participation. As digital dependency increases, so does exposure to cyber threats, posing serious risks not only for individuals, businesses, and governments, but for society as a whole. Ensuring safe and secure mobile networks is therefore not merely a technical concern but a requirement for trust and safety in a digitally connected world.

The fast-changing nature of cyber threats is driving up the costs and complexity for mobile operators to implement effective cybersecurity monitoring and protection, making the role of regulation increasingly important. Well-designed regulation supports them in managing risks proportionately and effectively, strengthening network security and resilience. In contrast, poorly designed or misaligned frameworks can impose disproportionate costs, complicate operations, and even increase vulnerabilities.

Fragmented or poorly designed regulatory frameworks may divert resources away from real security improvements, delay incident response, and stifle innovation in protective technologies. This ultimately threatens not just mobile networks, but the safety and reliability of essential digital services.

This report, commissioned by the GSMA, explores how cybersecurity regulation shapes the ability of mobile operators to defend against evolving threats. It highlights the costs, challenges, and opportunities that regulation creates and sets out how well-designed policies can strengthen resilience while poor ones increase risk.

## The rising cost of cybersecurity for mobile operators

Cybersecurity is now a foundational pillar of mobile network operations, requiring significant and growing resources. This report estimates that mobile operators globally spend between $15bn and $19bn annually on their “core” cybersecurity activities, including technical security functions and threat-monitoring teams.[1] This figure likely underestimates total spend in cybersecurity, as it excludes broader activities that contribute to cybersecurity, such as governance, training, and ensuring network resilience. As threats evolve, costs are projected to rise to between $40bn and $42bn by 2030. The burden of these investments falls especially heavily on mobile operators in low- and middle-income countries (LMICs), where high fixed costs of cybersecurity must be recovered from a customer base with much lower average revenue per user (ARPU).

## Good practice in cybersecurity regulation

Mobile operators worldwide face common challenges in complying with cybersecurity regulation, including fragmented policies and regulatory frameworks, limited institutional capacity to support mobile operators, rigid or prescriptive rules, and a lack of effective platforms for threat intelligence sharing. As a result, operators often incur disproportionate or unnecessary costs in addressing cybersecurity concerns, and, in some cases, poorly designed policies can even increase cyber risk. Many of these challenges can be mitigated through better regulatory practices, such as more coordinated, risk-based, and outcomes-focused approaches to cybersecurity regulation.

In many countries, operators face a patchwork of overlapping laws, sector-specific policies, and mandates from multiple regulators. This often results in higher compliance costs, duplicate reporting requirements and a lack of harmonised definitions or compliance processes, while not lowering cyber threats. In some cases, operators are subject to conflicting obligations or must report the same incident through multiple channels.

Poorly designed regulation creates operational inefficiencies, and shifts resources from genuine risk mitigation to compliance, and can squeeze out investments in innovation whether in advanced services or new security solutions.

Policymakers should ensure that compliance and incident reporting frameworks are aligned across sectors and policy areas. Well-designed horizontal frameworks can preserve sector-specific flexibility while supporting coherent national cybersecurity strategies.

1 Frontier Economics analysis.

## International standards can support consistency across borders

Cyber threats are international, but cybersecurity policy is implemented nationally, leading to divergence between countries. Misalignment between national frameworks creates challenges for operators working across jurisdictions. Even within the European Union (EU), where policy is designed to be harmonised across the member states, operators still face inconsistencies in national implementation. Differing standards add inefficiencies and hinder effective responses to emerging threats.

Divergent national cybersecurity policies add costs to operators that are present across multiple markets. National cybersecurity policies can be mapped to globally recognised industry and international standards (e.g., ISO[2], NIST[3] and GSMA[4]) to foster cross-border consistency which enables operators to cost effectively implement protections across their international operations. Using global standards as a baseline allows adaptation to national contexts while maintaining alignment with internationally recognised principles, but deviation should be by exception, with clear justification.

## Risk-based, outcome-focused regulation is more effective than formalistic rules

Effective cybersecurity measures should address actual risks rather than impose one-size-fits-all mandates that may be disproportionate to the threat level or operational context. Formalistic approaches, built on compliance checklists or mandated tools often create inefficiencies, foster a 'box-ticking' culture, and divert resources from genuine risk mitigation. For end users, formalistic rules can leave networks less resilient to new threats and slow the introduction of new security solutions, reducing both reliability and choice in digital services.

By contrast, risk-based, outcome-oriented regulation ensures proportionate obligations, directs resources where they are most needed, and gives operators the flexibility to innovate and deploy the most effective technologies and practices to strengthen resilience.

## Regulatory culture should encourage trust, collaboration and threat intelligence sharing

The way regulators enforce cybersecurity rules strongly shapes their effectiveness. A punitive or blame-oriented culture erodes trust, discourages information sharing, and positions compliance as a bureaucratic process focused on liability avoidance, rather than risk reduction. Unclear guidance and disproportionate penalties further limit collaboration.

At the same time, effective threat intelligence sharing remains critical to anticipate attacks and coordinate responses. Threat intelligence platforms often rely on the principle of reciprocity, where operators are more likely to actively engage and provide information where they derive value. However, in many jurisdictions, threat intelligence platforms are either absent or provide limited value to mobile operators, undermining their usefulness.

A more productive approach fosters collaboration, engagement, and mutual trust. By consulting operators through working groups or public consultations, regulators create conditions for shared responsibility and continuous improvement. An enforcement culture that favours learning and capacity-building over punishment, enhances transparency, reduces resistance, and supports more effective implementation. Secure and trusted platforms for threat intelligence can amplify these benefits by allowing faster identification and dissemination of threats, improving incident response, and creating the conditions for innovation in security solutions that strengthen the resilience of the entire digital ecosystem.

2 ISO is the International Organisation for Standardisation
3 NIST is the National Institute of Standards and Technology
4 GSMA Cybersecurity Knowledge Base

### Cybersecurity policy should encourage a proactive, security-by-design approach to mitigating risk

Cybersecurity regulations that are reactive, triggered by incidents or media attention rather than long-term planning, are costly to comply with. A proactive approach to mitigating risk, which emphasises prevention and resilience, and allows for long-term planning, is both more effective and more cost-efficient. While a reactive response is essential when incidents occur, best practice complements this with a proactive, security-by-design approach, grounded in clear, outcome-based rules that allow flexibility in implementation. This requires early risk mitigation and supports systemic investment in resilience.

### Strong institutional capacity is important for effective security

Even the best designed cybersecurity frameworks cannot succeed without strong institutions to implement and oversee them. Weak regulatory and governmental capacity, whether due to limited budgets, lack of technical expertise, or unclear mandates, undermines enforcement, reduces credibility, weakens cybercrime deterrence and creates uncertainty.

Operators need clear mandates and well-resourced agencies with skilled personnel, modern tools, and the ability to engage effectively with stakeholders. Strong and independent institutions ensure more consistent application of policy, build trust with operators, and create a stable environment that delivers more reliable protection for end users.

## Six principles for best practice cybersecurity policy

This report sets out six core principles that legislators and regulators should always consider when shaping cybersecurity policy. Applied consistently, they minimise unnecessary costs for operators, enabling them to focus effort and attention on genuine risks and mitigation. These principles apply to all countries. For countries with less mature digital frameworks they guide the development of digital policy, ensuring that as policy evolves, it supports mobile operators.

For countries with more advanced digital frameworks they will help policymakers consolidate and refine existing rules so operator efforts are focused on tackling threats and protecting end users.

### The six principles for best practice cybersecurity policy are:

- **Harmonisation:** Align cybersecurity policy with international standards wherever possible, to reduce regulatory fragmentation and inconsistency.
- **Consistency:** Ensure new policies and frameworks are consistent with existing policy to avoid duplication or conflict.
- **Risk- and outcome-based:** Adopt risk-based and outcome-based approaches in the design and implementation of cybersecurity regulation, giving operators flexibility to innovate and deploy effective solutions.
- **Collaboration:** Promote a collaborative regulatory culture with industry, supported by secure threat intelligence sharing to strengthen resilience, increase awareness of cyber threats, enable constructive enforcement, and foster a joint approach to combating cybercrime.
- **Security-by-design:** Encourage a proactive, security-by-design approach to mitigating cyber risks.
- **Capacity-building:** Strengthen the institutional capacity of cybersecurity authorities to ensure a whole-of-government approach and effective application of policy and regulation.

# 02. Introduction

Mobile services are a fundamental component of modern life, supporting communication, economic activity, and access to information and essential services. As the digital world continues to expand, mobile connectivity will play an increasingly important role in driving economic growth, fostering innovation, and promoting social inclusion. With growing reliance comes an increased exposure to cyber threats, which can have serious financial, operational, and societal consequences for individuals, businesses, and governments. Cybersecurity of mobile networks is therefore not just a technical issue, but an essential element for ensuring safety and trust in a connected world.

As cybersecurity challenges continue to evolve and grow in scale and complexity, the cost and effort required by mobile operators to implement effective protections are also likely to rise. This makes it particularly important for policymakers and regulators to design rules that support mobile operators in addressing cyber risks in a proportionate way, without imposing unnecessary burdens, with clearly defined boundaries, consistent and effective implementation, and minimal duplication with other policies and regulations.

Proportionate, well-targeted regulation enables mobile operators to innovate and safeguard their networks in the most effective way, protecting users. By contrast, when regulation is poorly designed or implemented without consideration of operational realities and risks, it can limit operators' ability to innovate, create unnecessary costs and inefficiencies. In some cases, these burdens can even increase risk, ultimately exposing end users to a higher likelihood of incidents.

The effectiveness of regulation determines whether society is better protected against cyber threats. Weak or fragmented rules may drain resources away from real security improvements, slow incident response, and discourage investment in innovative protections. This not only undermines the resilience of mobile networks but can also reduce the quality, reliability, and safety of the digital services that people and businesses depend on.

This report, commissioned by the GSMA, examines how cybersecurity regulation affects mobile networks across financial, operational, and strategic dimensions. It considers the wider implications for innovation, long-term investment, and risk exposure. This recognises that cybersecurity is not just a discrete technical issue, but a strategic consideration embedded across nearly all aspects of decision-making within mobile operators' business model, from network design and vendor selection to product development, customer engagement, recruitment and training, and regulatory compliance. The analysis highlights examples of poor practices that create unnecessary burdens, as well as good practices that support effective and proportionate security outcomes.

This study focuses specifically on cybersecurity regulation as it applies to mobile networks. In this context, cybersecurity is understood to encompass the protection of mobile network infrastructure (i.e., physical and virtual components) as well as the broader set of systems, processes and people that support secure network operations. This includes hardware and software management (e.g., firewalls, patching and encryption), operational procedures, and workforce-related measures such as training and usage policies. The study does not assess consumer-targeted fraud or scams (e.g., phishing or SMS fraud), and therefore does not cover customer-facing elements such as service and billing platforms or end-user devices.

While cybersecurity applied to mobile networks exists within a broader digital ecosystem, alongside other providers of digital products and services, technologies, and regulatory domains, this study considers broader digital regulations (e.g., data privacy, competition, industrial) or other ecosystem players (e.g., network equipment vendors) only insofar as they directly interact with mobile operators' network-level regulatory obligations. This targeted scope reflects the areas where operators currently hold direct responsibility and where cybersecurity regulation has the most immediate and operationally significant impact for them and their users.

The findings presented in this report draw on a mixed-methods approach, including in-depth interviews with 14 mobile operators across all global regions (Africa, Asia Pacific, Europe, Latin America, Middle East and North America), as well as a review of existing evidence, secondary data sources, and a targeted literature search.

# 03.
# Mobile operators invest significant amounts to protect their networks

## 3.1 The volume and cost of cyber threats is large and rising

Cyber threats are rising rapidly across the global digital landscape. The number of cyberattacks has increased by approximately 75% over the past five years, and the cost of cybercrime is expected to escalate sharply.[5] A recent study found that global cybercrime costs will grow by 15% per year, reaching $10.5 trillion in 2025, up from $3 trillion in 2015.[6]

Threats are coming from different sources: state actors, hacktivists that use cyberattacks to pursue objectives, organised crime and smaller-scale criminal activity. This upward trend is likely to continue as digital development accelerates, new criminal models develop (such as the emergence of ransomware-as-a-service), the number of connected devices increases, and technical barriers to launching a cyber-attack diminish.[7] The entire digital ecosystem therefore, faces growing threats that it must protect against.

## 3.2 Mobile networks have a crucial role with respect to cybersecurity

The responsibility for cybersecurity spans the entire digital ecosystem, involving operators, vendors, governments, and end users. However, mobile operators play a particularly important role in maintaining security across the broader digital environment. They are not only responsible for securing their own infrastructure and services but also act as the frontline defenders of the broader digital environment. This includes protecting millions of users who rely on mobile connectivity for critical services such as financial transactions, healthcare access, and digital identity.

Strong cybersecurity is essential to protect the integrity, availability, and trustworthiness of digital systems. This is especially relevant for mobile networks, which provide billions of people around the world with their primary access to digital communication, information, and social interaction. As of 2023, over 90% of the global population was covered by either 4G or 5G networks.[8] Moreover, mobile technologies and services generate about 5.8% of global GDP, approximately $6.5 trillion.[9]

## 3.3 Mobile operators face growing threats on an ongoing basis

Mobile networks are an increasingly attractive target for cyberattacks given the sector's wide reach and economic importance within the digital ecosystem. The sector is especially valuable to espionage-motivated threat actors due to its access to intelligence-rich data and telemetry, which can enable surveillance and tracking activities.[10] Moreover mobile networks are the backbone of the digital ecosystem meaning that disruption can have wider economic and social impacts.

> "It has become very easy to launch an attack and create disruption as the entry barriers have become very low"
>
> African MNO[11]

5 Centre for International & Security Studies at Maryland. Cyber Events Database
6 Cybersecurity Ventures. 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics
7 Frontier Economics (2024) Assessing the economic impact of EU initiatives on cybersecurity
8 International Telecommunications Union (ITU). Global mobile network coverage
9 This includes direct impacts (mobile operators 0.6% of GDP), (suppliers to mobile operators and downstream services 1.5% of GDP), and wider impacts (improvements in efficiency and productivity enabled by mobile services 3.7% of GDP). GSMA (2025) The Mobile Economy 2025
10 PwC (2025) Cyber Threats 2024: A Year in Retrospect
11 This and other quotes in the report are from mobile network operator (MNO) interviews conducted by the author.

> "Any threats that come in through cyber attacks have the ability to wipe a company out financially and reputationally"
>
> African MNO

Attacks affect operators in different ways. Denial of service (DoS) generates sudden spikes in traffic that disrupt the ability of operators to provide services, leading to outages, and degrading network performance (or can be used to disguise other attacks). Malware delivery enables hackers to load malicious software onto the operator's network which can be used to degrade or damage the network. Hackers exploit vulnerabilities to gain unauthorised access to parts of the network to extract data for gain.

The scale of cyberattacks on mobile networks is substantial and growing every day. UK operator BT reported detecting 2,000 potential attack signals per second across its network, equating to 200 million per day[12]. Globally, the frequency of DoS attacks has grown has grown from one or two a day to well over 100 per day between 2023 and 2024.[13] One operator noted that there were "70 million attacks per day on our honeypot systems in 2024 – these are traps deliberately set for attackers"[14]; and another operator noted that it faced 3.5 billion attempts to infect its systems with malware (2x increase since 2020), and 29 trillion scans probing our network for vulnerabilities (2x increase since 2020).[15]

The costs to operators of attacks are significant. Operators face direct costs in responding to the incident and restoring services (repairing, replacing and upgrading equipment), but attacks can also create reputational damage, and impose further costs on affected users. Publicly available information on customer compensation and provisional spending related to cyberattacks in the last five years shows costs ranging between $100 million[16] and $350 million.[17]

12 BT (2024) Cyber Agile Organisation UK Market Report
13 Nokia (2024) Threat Intelligence Report
14 https://report.telekom.com/cr-report/2024/governance/cybersecurity-and-data-protection.html
15 https://www.telus.com/en/business/medium-large/security/cyber-security/professional-services/incident-response
16 News article: "Optus allocates $140 million to cover data breach costs"
17 News article: "T-Mobile agrees to pay customers $350 million in settlement over massive data breach"

## 3.4 Operators' cybersecurity measures are context-specific

Although all mobile operators take responsibility for securing their networks, it is important to recognise that cyber threats are not necessarily uniform across geographies or economies. Therefore, cybersecurity measures must consider the specific conditions of each country or region. These differences reflect at least three elements: (1) varying patterns of mobile network use, (2) differences in the types of services accessed via mobile devices, and (3) differing economic conditions that shape both the threat landscape and operators' capacity to respond to and recover from cyber threats.

**Patterns of digital network usage differ significantly across regions.** In many low- and middle-income countries[18] (LMICs), mobile networks serve as the primary (and often only) channel for internet access. For instance, fixed broadband penetration in Sub-Saharan Africa remains below 0.5%, while mobile broadband penetration is 48% of the population.[19] This high reliance on mobile connectivity means that cyber threats that target mobile systems (such as network disruption or DoS attacks) can have a more severe impact in LMICs.

**The types of mobile services most widely used also vary by region, which has implications for cyber risk and the protective measures required.** In LMICs, mobile networks are a critical delivery platform for essential services such as digital financial inclusion, mobile health (mHealth), education, and government services. For example, mobile money services are central to financial access in much of Sub-Saharan Africa with over 400 million registered mobile money accounts.[20] In the Philippines, GCash has similarly become a key platform for digital financial inclusion, with almost 100 million registered users relying on it for everyday transactions such as payments, transfers, and savings.[21] These services often operate outside traditional banking regulations, exposing them to targeted cyber threats. The dependence on mobile financial services increases the stakes of any security failure for both operators and users.

**Economic conditions vary widely across countries, affecting both the scale of cyber risk and the capacity to invest in cybersecurity.** Operators' average revenue per user (ARPU) in many lower-income countries remains significantly lower than in high-income markets. For instance, in 2024, the ARPU in high-income countries was significantly higher than in LMICs.[22] This disparity inevitably affects operators' investment strategies including how they allocate capital to network resilience projects.

These structural differences can disproportionately increase the vulnerability to cyber threats of operators in LMICs. The consequences of such threats (from service disruption to financial loss and erosion of trust) may also be more severe, particularly where mobile networks serve as the main digital access point. This highlights the importance of cybersecurity frameworks and regulatory approaches that are context-aware, proportionate, and supportive of capacity-building. A one-size-fits-all regulatory model risks imposing unnecessary burdens that are misaligned with operational and economic realities, especially in settings where mobile connectivity is not just one option among many, but the only connection to digital services.

18 World Bank defines low- and middle-income countries by their Gross National Income (GNI) per capita. As of the 2024, low-income countries have a GNI per capita of $1,135 or less. Lower-middle-income countries fall between $1,136 and $4,495, and upper-middle-income countries are between $4,496 and $13,935. High-income countries are those with a GNI per capita of more than $13,935. See: World Bank income groups.

19 International Telecommunications Union (ITU). Global mobile network coverage

20 GSMA (2024) GSMA Mobile Money Report 2023.

21 FinTech Magazine (2025) "GCash: The Rise of a Financial Super App"

22 Telegeography. Data extracted in June 2025.

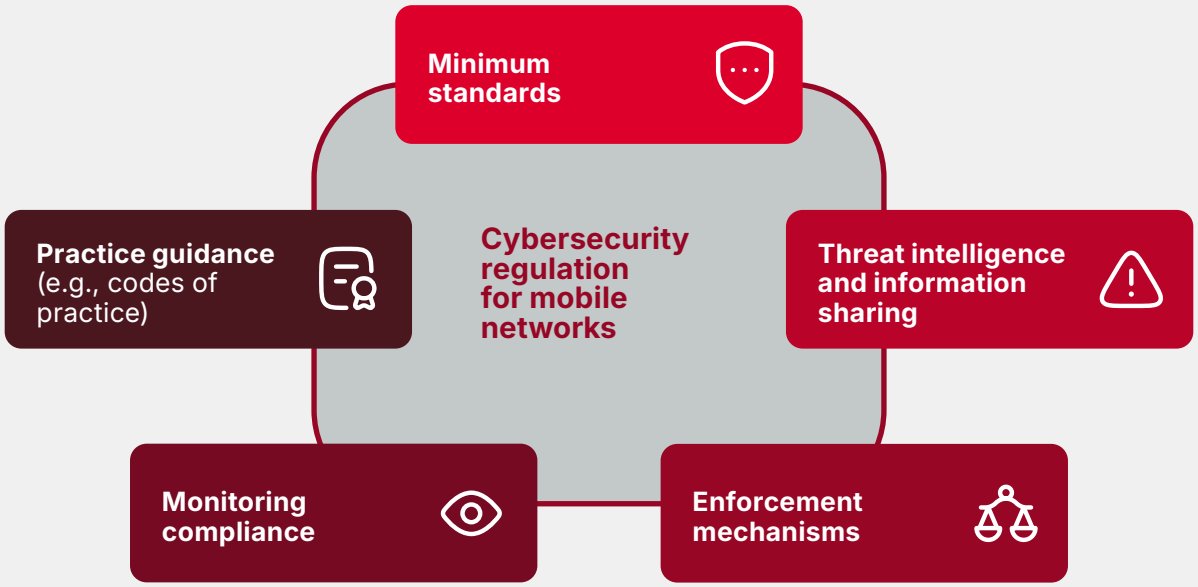
# 04.
# How cybersecurity regulation can support the mobile sector

## 4.1 Cybersecurity policy involves a number of distinct activities

Given the potential costly consequences of cyberattacks, governments and regulators have implemented a broad and mutually supporting suite of cybersecurity policies aimed at protecting customers, businesses, and public institutions from emerging cyber threats. The designation of mobile infrastructure as critical national infrastructure in many jurisdictions (alongside growing national security concerns) has further intensified the policy focus on the cybersecurity of mobile networks.

Government cybersecurity policy and regulation consists of a wide range of complementary activities that collectively shape how organisations manage cyber risks and meet regulatory obligations. These activities, presented in Figure 1, include setting minimum standards, facilitating threat intelligence and information sharing, providing practical implementation guidance, monitoring compliance, and applying enforcement mechanisms.

**Figure 1**
**Cybersecurity policy and regulation encompasses distinct activities**




Source: Frontier Economics.

Each of these activities forms part of a broader regulatory toolkit.

- Minimum standards (whether legally binding or recommended as best practice) set expectations for baseline activity to ensure cybersecurity.
- Threat intelligence and incident reporting frameworks enable timely awareness and response across the ecosystem.
- Practical guidance, such as codes of practice and technical documents (directed at mobile operators and supply-chain partners), assists organisations and helps them interpret and operationalise policy requirements.
- Compliance monitoring mechanisms to assess effective implementation of policy and regulation, and whether organisations meet best practice and regulatory expectations.
- Enforcement tools (such as notices, directives, or fines) to deter cybercrime, maximise compliance and ensure accountability across the ecosystem.

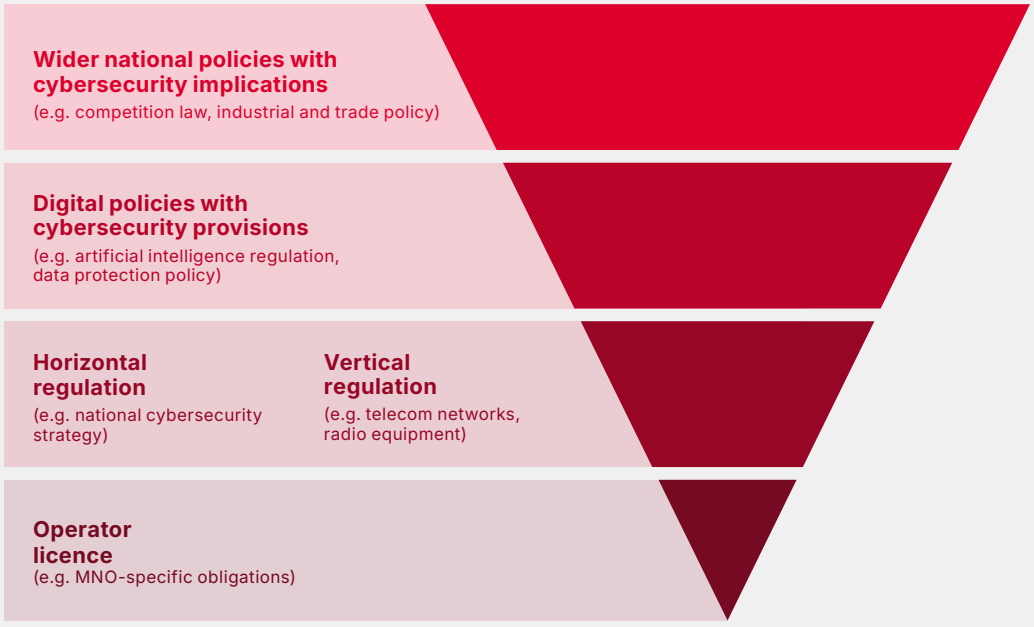
While each of these activities plays a distinct role, they do not operate in isolation. The design and implementation of one component can influence the effectiveness of others (positively or negatively), creating important relationships and trade-offs that must be understood and managed. For example, strong enforcement powers may help ensure adherence to standards, but if not paired with adequate guidance or threat intelligence, they may result in compliance-focused responses that prioritise box-ticking over improving cybersecurity outcomes. The balance among these elements influence how effectively cybersecurity regulation operates in practice, particularly in a context as fast-moving and critical as mobile networks.

## 4.2 Enacting policy through a complex web of regulation, licences and standards

For mobile networks, cybersecurity regulation does not exist in isolation but within an increasingly complex digital regulatory landscape. As shown in Figure 2, cybersecurity policy, particularly in more digitally developed countries, is not governed by a single regulation but instead emerges from a web of interlinked regulations spanning multiple sectors and domains. These include:

- Licences granted by regulators or governments, which may include cybersecurity requirements that create binding obligations on mobile operators.
- Cybersecurity policy (e.g., rules on vendor choice, telecoms-specific cybersecurity regulation).
- Policy that is not specific to cybersecurity, but contains related requirements (e.g., codes of practice).
- Horizontal regulations that apply across multiple sectors, including telecoms (e.g., national cybersecurity frameworks that apply to critical infrastructure sectors or essential service providers)
- Vertical regulations in non-telecoms sectors that affect telecoms (e.g., radio equipment devices, connected devices, financial services).
- Policy in adjacent digital areas that include cybersecurity requirements (e.g., artificial intelligence (AI) or data protection and privacy)
- Broader policy that shapes operators' approaches to cybersecurity indirectly, including industrial policy, competition policy, or trade policy.

**Figure 2**
**Mobile operators face many overlapping layers of reguation that affect cybersecurity**




Source: Frontier Economics.

These frameworks evolve at different times, shaped by diverse policy objectives and sectoral priorities. The frameworks are often developed in response to specific concerns or the state of technology at the time, which creates overlapping cybersecurity obligations for mobile operators. As a result, operators face requirements from multiple regulations that intersect and influence how cybersecurity rules are interpreted and applied.

The complex web of regulation means that operators in some jurisdictions face oversight in relation to their cybersecurity from a range of different monitoring authorities including telecoms regulators, cybersecurity authorities, financial regulators, AI authorities, and data protection authorities.

**The cybersecurity regulatory landscape in Europe**

In Europe, mobile operators face cybersecurity obligations from multiple overlapping frameworks. The Network and Information Systems (NIS2) Directive expanded the scope of "essential and important entities", including electronic communications providers, and introduced stricter security and incident reporting obligations that directly affect mobile operators. Until recently, the European Electronic Communications Code (EECC) imposed requirements on network security, integrity and incident reporting. These requirements were repealed with the adoption of NIS2 in 2024. However, during the ongoing transposition process, operators may still experience overlap and uncertainty, as responsibilities to different authorities are clarified at Member State level.

Other European Union (EU) regulations also shape operators' cybersecurity responsibilities. The Cyber Resilience Act (CRA) introduces horizontal requirements for the cybersecurity of digital products in the EU, including connected devices that operate over mobile networks, which may indirectly affect operators through compliance burdens on suppliers and partners. The Digital Operational Resilience Act (DORA), although targeted at the financial sector, has implications for mobile operators that provide critical connectivity to financial institutions, potentially exposing them to heightened scrutiny through contractual obligations. In addition, adjacent digital regulations such as the AI Act contain cybersecurity provisions that extend operators' compliance requirements.[23]

Beyond cybersecurity-specific rules, EU and national policies on network procurement and service design also influence mobile operators' approaches. These include restrictions on the use of certain vendors (e.g., 5G toolkit), rules governing the use of cloud services in networks, and broader policy domains such as competition law, industrial policy and strategic autonomy, and international trade.

Given this complexity, it is vital that policymakers and regulators adopt consistent and mutually reinforcing approaches across the disparate regulations, licences, policies and laws. However, as the threat landscape evolves, newer regulations are not always aligned with existing frameworks, while legacy legislation may remain outdated despite shifts in technology and risk profiles. Moreover, policymakers may have many different objectives in mind when designing policy, which can result in divergent terminology, definitions, or risk thresholds. These inconsistencies create uncertainty, interpretative challenges, and in some cases direct contradictions between rules.

23 AI Act Article 15.

## 4.3 Implementing cybersecurity is costly

**Global core cybersecurity spending by mobile operators is estimated by this report at between $15bn and $19bn per year.**[24] This figure covers activities specifically allocated to cybersecurity within IT budgets and excludes wider costs such as network equipment, network resilience or wider governance and training costs.

Spending levels vary significantly by business size. Smaller operators typically face proportionally higher costs relative to revenue compared to larger firms. A similar pattern is observed in LMICs where operators face structural differences that can significantly affect both the scale and nature of required investments.

> "IT budget allocated to cybersecurity is only a fraction of the cost base for an MNO"
>
> European MNO

These estimates likely understate the true cost for mobile operators, given that cybersecurity is embedded across nearly all aspects of mobile operations and decision-making. Moreover, these costs are expected to continue rising. Industry evidence shows that cybersecurity spending in the telecoms (including all markets), media and tech sector has grown by 125% in the past five years, indicating an annual growth rate of 23% per year.[25] **At this pace, cybersecurity expenditures by mobile operators could reach between $40bn and $42bn by 2030**.

## 4.4 Network security involves many types of investment

Implementing cybersecurity across mobile networks is inherently costly, in terms of direct financial costs and in terms of wider strategic and operational dimensions. As cyber threats increase in frequency and sophistication, mobile operators need to integrate robust security practices into nearly every aspect of decision-making. Cybersecurity is no longer a discrete IT or technical function but a cross-cutting strategic concern spanning network operations, governance, commercial functions and strategic planning.

> "Cybersecurity costs are hard to isolate, they are integrated across all our operations, as part of a broader mindset"
>
> European MNO

Security considerations now influence a wide array of business functions, from vendor and supply-chain selection and contract design to network architecture, product development, and user data policies. Staff require regular training to address evolving threats and compliance obligations, while security-by-design principles affect development timelines. Customer engagement is shaped by breach notification protocols and transparency obligations. At the strategic level, cybersecurity has become integral to risk management, regulatory compliance, and organisational priorities.

> "Costs cannot be easily estimated... they are integrated into all our operations, even operations that may not explicitly fall under the heading 'cybersecurity' "
>
> European MNO

24 Frontier Economics analysis. This takes a conservative approach assuming 5% of mobile revenue is allocated to IT budget, and between 8% (lower bound) and 10% (upper bound) is directed to cybersecurity. Research shows that mobile operators typically allocate between 8% and 10% of their IT budgets to cybersecurity. Gartner (2025) IT Key metrics data 2025: IT security measures, Alvarez & Marsal (2024) Cybersecurity budgets: Spend more or spend better Moody's 2023 Cyber Survey

25 Moody's 2023 Cyber Survey

As a result, cybersecurity costs are multifaceted and extend well beyond traditional IT budgets. The estimates presented earlier likely capture only core activities such as operational processes and network security. In practice, operators also invest heavily in network resilience (technology and infrastructure) and wider organisational functions such as governance, compliance, supply-chain management, and training. As illustrated in Figure 3, these three layers together represent the full scope of cybersecurity costs, much of which is difficult to quantify but critical for maintaining secure and reliable services.

Since cybersecurity is embedded across the entirety of mobile operations, these costs are difficult to isolate. For example, when mobile operators upgrade systems or deploy new technologies, they are expected to incorporate the latest security standards and architectures. This means the incremental cost of cybersecurity cannot easily be separated from overall network investment and operational expenditures.

**Figure 3**
**Types of cybersecurity costs for mobile operators**


Source: Frontier Economics.

## 4.5 Operators increasingly invest in resilience and prevention

Cybersecurity spending patterns have also evolved in the last five years. Across industries, IT security budgets were once dominated by reactive operational functions but have gradually shifted toward proactive, security-by-design approaches.[26] This reflects a maturing sector, where protection is built into architecture and service development from the outset, with greater emphasis on resilience, prevention, and long-term risk management rather than short-term incident response or compliance.

By asset class, personnel continue to account for the largest share of costs, highlighting the central role of human expertise in cybersecurity implementation. Software investment has increased steadily, while hardware spending has declined, and reliance on external services (including managed security, audits, and consultancy) has also become more prominent.[27] Together, these trends illustrate a broader shift away from hardware-centric security models toward more flexible, software-based and cloud-enabled solutions.

Mobile operators stated that new cybersecurity investments often compete with other discretionary budgets for capital and operating expenditure. When new funding is required, the relevant security head (e.g., Chief Security Officer or Chief Technology Officer) needs to present the case for board approval. In practice, this means rising cybersecurity costs can crowd out investment in service improvements, network quality, or new products. Mobile operators cited cases where unexpected cybersecurity expenses during budget cycles led to other projects being cancelled, delayed, or deprioritised.

> "Uncertainty affects investment decisions we need to invest to keep up with developments in the world... but regulation is not clear and there is no guidance at all"
>
> MENA MNO

These pressures may ultimately affect end users. While mobile operators did not suggest that higher compliance costs are directly passed on to customers, diverting resources away from innovation and resilience can lead to longer or more frequent service disruptions, slower recovery from cyber incidents, weaker protection against emerging threats, and fewer choices in secure connectivity.

## 4.6 Regulation should be designed to enhance security benefits while avoiding unnecessary costs

Mobile operators dedicate substantial resources to cybersecurity, both to comply with regulation and to maintain efficiency, competitiveness, and user trust. This trend will continue as threats become more sophisticated, network architectures grow in complexity, and supply chains are increasingly global and interconnected. This sustained investment is driven not only by the frequency and severity of attacks but also by structural shifts, such as the transition to cloud-native and virtualised infrastructures, which expand the attack surface.[28,29] Well-designed regulatory frameworks are therefore essential to ensure rising costs do not include unnecessary or duplicative burdens.

Mobile operators emphasised that regulation generally has a limited impact on the overall level of cybersecurity defences they implement in their networks. Strong commercial and reputational incentives already drive operators to maintain robust protection for their end users, meaning necessary investments in security are undertaken regardless of regulatory requirements. However, a significant proportion of cybersecurity expenditure can be consumed by activities or investments that add costs without directly improving security or resilience.

26 Gartner (2025) IT Key metrics data 2025: IT security measures
27 Idem.
28 Cybersecurity Dive (2024) Telecom, media and tech companies are cyber defence standouts: Moody's
29 GSMA (2025) Mobile Telecommunications Security Landscape 2025

The costs of cybersecurity regulations tend to fall into three categories:

1. **Obligations that align with, or increase, the cybersecurity measures operators already implement in a way that is consistent with their existing approach.** These obligations ensure minimum standards but tend not to add significant costs to operators who meet the requirements. Regulatory obligations should be designed so that as far as possible they fall into this category. The minimum standards should reflect the ongoing activities of the mobile operators.
2. **Regulations that require mobile operators to do things that are different but not better.** These requirements can have the same objectives or outcomes as the operators' cybersecurity activities, but mean that mobile operators have to undertake incremental activities, or incur incremental investment in a way that does not lead to an increased level of cybersecurity defences. These burdens can be technical (e.g., mandating specific technologies and approaches or requiring premature equipment replacement). In many cases, operators are required to act in ways that diverge from their preferred approach without meaningfully improving security (e.g., being restricted in their choice of vendors). Policy should be designed to avoid imposing obligations that do not improve cybersecurity standards.
3. **Regulatory obligations that impose costs that do not directly improve cybersecurity but arise from interpreting and demonstrating compliance.** These include the technical and legal costs of reviewing and interpreting new laws and mapping requirements to existing standards (e.g., ISO 27001 or NIST). A significant volume of resources is dedicated to reporting compliance (either directly to regulators or via requests from customers). Some mobile operators report that as much as half of their cybersecurity operations teams are occupied with compliance tasks rather than actively identifying threats or managing risks. Policymakers should seek to design policy in a way that minimises these costs.

# 05. Effective policy strengthens cybersecurity, poorly designed policy creates avoidable costs

## 5.1 Good and poor practice in the application of cybersecurity policy

The design, governance, and implementation of cybersecurity regulation for mobile networks has an important impact on the costs that mobile operators face in applying the regulation. The impact of regulation on mobile operators and their ability to support cyber security is shaped by a set of interrelated "dimensions", which for this study are grouped into three broad categories as presented in Table 2 below: (1) design and structure of regulation; (2) regulatory culture and institutional context; and (3) enablers of security readiness and innovation. Using this framework and based on in-depth interviews with mobile operators, examples of good and poor practices in the application of cybersecurity were identified for each dimension.

**Table 2**
**Dimensions that affect the application of regulation**

| Category | Design and structure of regulation | | | Regulatory culture | | Enablers of security readiness and innovation | |
|---|---|---|---|---|---|---|---|
| **Dimension** | Framework coherence and fragmentation | Harmonisation with international standards | Focus on outcomes and risks | Coordinated approach | Enforcement and supervision approach based on trust | Proactive vs reactive approach to mitigating risk | Regulatory and governmental capacity |
| **Good practice** | Coherent frameworks both across and within sectors and wider digital regulation, frameworks are transparent and accessible | Cross-border regulatory coordination and mutual recognition, standards are well-defined and accessible | Outcome-oriented, risk-based and proportionate in adaptation | Bottom-up, industry-led as "first resort", based on evidence<br><br>Trusted and structured information sharing platforms | Proportionate liability for enforcement loss, culture of learning and engagement with stakeholders to promote collaboration and transparency | Promotion of security- and privacy-by-design across product/service life cycle | Well-resourced with sufficient technical and human capacity, clear mandates |
| **Poor practice** | Regulatory fragmentation, overlapping, national gold-plating | Divergence from global or industry standards | Focus on formalistic compliance, rigid rules over real outcomes | Top-down, rigid without stakeholder input or risk assessment<br><br>Limited or absent threat intelligence sharing platforms | Unpredictable or disproportionate liability for loss, culture of blame, penalises disclosure | Reactive approach to security threats | Under-resourced with limited expertise, no clear mandates |

Source: Frontier Economics.

Overall, insights from mobile operators reveal recurring challenges in the implementation of cybersecurity policy. Operators were asked which aspects create disproportionate avoidable costs, or policies that can increase rather than decrease risks. The most frequently cited issue was a lack of harmonisation within and across countries.

Other concerns included limited regulatory and governmental capacity, unclear mandates from authorities, the absence of effective threat intelligence platforms, and overly formalistic and rigid rules. Some mobile operators also noted that the penalisation of disclosure deters transparency and weakens collective cyber resilience.

# 5.2 Frameworks should be internally coherent and consistent

National cybersecurity frameworks must be coherent, aligned, and internally consistent to ensure they are easy to interpret and implement. Clear and well-structured policies enable mobile operators to meet their obligations effectively, avoid duplication, and focus resources on strengthening security, which in turn delivers more resilient and reliable services for end users.

## Overlapping mandates and conflicting obligations create regulatory incoherence

Given the diversity of regulation and authorities involved in cybersecurity regulation, a degree of complexity in cybersecurity policy is unavoidable. However, this often results in inconsistencies across sectors and with broader digital frameworks. Operators frequently cited the lack of regulatory coherence as a key driver of avoidable cost and implementation challenges.

> "When faced with different requirements we need to follow the strictest mandate to design our cyber systems"
>
> Asia-Pacific MNO

**Different compliance requirements.** Mobile operators noted challenges created by overlapping and conflicting compliance requirements from different regulators. For example, some face separate reporting and compliance obligations from cybersecurity and telecoms authorities, and in some cases also from financial regulators (when an incident affects financial services). In practice, this forced many operators to adopt the strictest standard across all requirements (i.e. "gold-plating"), leading to unnecessary costs without improving network security. Several operators described this as having to "design for the strictest one" even when the requirement was disproportionate to the actual level of risk.

**Misaligned or even inconsistent definitions within different regulations.** The absence of shared definitions (such as what qualifies as a critical system, a breach or an incident) leaves mobile operators uncertain about which rules to prioritise and how to implement them. As a result, they often need to reconcile conflicting requirements or duplicate processes simply to remain compliant. Differing interpretations can also create uncertainty over whether one regulation should take precedence over another. In India, for example, the Department of Telecommunications (DoT) uses a very broad "security incident" definition for operators[30], while the Computer Emergency Response Team India (CERT-In) uses "cyber incident" within an explicit list of incident types.[31] Both set six-hour deadlines, but the definitions and recipients differ (DoT vs CERT-In), which can mean dual reporting and uncertainty over scope (for example, whether every "security incident" (DoT) automatically counts as a "cyber incident" requiring CERT-In reporting, and vice versa).

**Lack of consistency with wider digital frameworks.** In many jurisdictions, cybersecurity is regulated in isolation from other digital frameworks, often with unclear scope, inconsistent terminology, or overlapping enforcement responsibilities. For example, in Europe, one operator noted the increasing regulatory overlap between cybersecurity, data privacy and AI frameworks, which had created legal uncertainties. These relate not only to whether cloud-based or AI-enabled security solutions used in mobile networks can be deployed while still meeting data protection requirements, but also to how cybersecurity incidents involving personal data should be reported. In practice, if too little detail is disclosed, operators risk non-compliance with cybersecurity rules, if too much is disclosed, they risk breaching data protection regulations. Mobile operators described scenarios whereby they must report the same incident involving personal data multiple times to different agencies (and in response to customer requests), each using different platforms, formats, and timelines.

30 DoT's Telecom Cyber Security Rules (2024).
31 CERT-In – Directions (April, 2022).

**Poor coordination between agencies** was frequently cited as a source of confusion, particularly when multiple authorities regulate overlapping aspects of cybersecurity in mobile networks. In some cases, frameworks directly conflict, especially where cybersecurity and data privacy mandates overlap. One mobile operator noted that when laws are introduced without consultation, it is often unclear whether compliance with one framework satisfies others, creating uncertainty and unnecessary costs.

> "Sometimes it feels there is competition between regulators because they publish contradictory policies...at the end, we don't know which one to follow"
>
> MENA MNO

**Inconsistent requirements exacerbate compliance burden.** Mobile operators noted that multiple and inconsistent frameworks may create overlapping obligations across the supply chain. This means evidence must be provided to many different stakeholders, with regulatory authorities, enterprise customers, and partners all issuing requests that often cover the same requirements. As a result, compliance has become increasingly resource-intensive, multiplying the number of requests operators need to address.

## Inconsistent regulation adds to avoidable costs and inefficiency

Mobile operators stressed that the growing number of regulatory frameworks has become increasingly duplicative and difficult to reconcile. Inconsistent and poorly coordinated regulatory practices add significant and unnecessary costs, as compliance teams spend substantial time interpreting requirements rather than addressing core security risks. This often forces them to duplicate processes or reformat information simply to meet audits, reporting obligations, or overlapping demands from different agencies.

> "The main cost is the resource drain... which decreases overall security because we spend more time formatting data to suit the reporting authorities than in improving security and resilience"
>
> European MNO

Resources that could strengthen defences or support incident response are instead absorbed by procedural tasks, and fragmented reporting channels can even heighten exposure by risking disclosure of sensitive vulnerabilities. This often requires hiring additional staff or diverting skilled personnel away from frontline cybersecurity functions.

> "We have to assign people to compliance work which means they are not working on actual security...80% of the year we spend on audits, follow ups and compliance... not on threat mitigation"
>
> Asia-Pacific MNO

Beyond operational inefficiencies, unclear and inconsistent rules can limit mobile operators' capacity to innovate. They have fewer resources and weaker incentives to invest in new security technologies or advanced digital services. Moreover, as one mobile operator noted, poorly designed regulation may inadvertently act as a barrier to growth and competitiveness, particularly where telecoms operators face stricter requirements than those of competing digital platforms.

## Mitigating the risks of fragmented regulation

Given the rapid evolution of digital infrastructure and the shifting threat landscape, cybersecurity frameworks must remain flexible, prioritising adaptable tools such as codes of practice over rigid legislation that is difficult to update. This type of alignment reduces the need for regulatory interpretation, prevents duplicative audits, and helps operators assign accountability across legal, security, and operations teams.

**Horizontal regulation by design can be more coherent than a patchwork of sector-specific rules.** Mobile operators noted that good practice involves a unified cybersecurity framework that applies across critical infrastructure sectors (such as telecoms, energy, banking, and transport) and sets out a minimum baseline of security. Such alignment promotes consistency, facilitates cross-sector threat intelligence and mitigation, and is particularly valuable for operators that work across multiple regulated industries or provide diversified services. This allows operators to focus resources on improving cybersecurity rather than navigating fragmented and overlapping obligations.

> "If you don't secure the whole ecosystem, you're only as good as your nearest neighbour"
>
> Asia-Pacific MNO

At the same time, sector-specific guidance remains essential, which can be delivered through flexible instruments like codes of practice. This is especially important as some operators reported that guidance is often absent or inconsistent, leaving them to weigh regulatory risk against operational need.

> "Policies need to be horizontal, not only for the telco market...Cyber policy cannot be framed in only one part of the value chain"
>
> Latin American MNO

The Australian and Singaporean cybersecurity frameworks both illustrate how horizontal legislation can promote consistent approaches across sectors, while accounting for sector-specific risks. Horizontal regulation recognises the interdependence of critical sectors and ensures consistency. This can be applied with flexibility to certain sectors, such as telecoms operators to create a more cohesive and effective national cybersecurity posture.

The Australian Security of Critical Infrastructure (SOCI) Act established minimum unified obligations across key sectors, such as communications, energy, and healthcare, while recognising their interdependence and the need for consistent baseline protections.[32] Moreover, the Enhanced Response and Prevention Act 2024[33] amended the SOCI Act to introduce specific legal duties for telecoms operators through the Telecommunications Security and Risk Management Program Rules 2025. The SOCI Act led to the repeal and replacement of sector-specific requirements to report incidents to the Department of Homeland Affairs and the telecoms regulator, and instead requires a single unified reporting regime to the Cyber and Infrastructure Security Centre.

The Singaporean framework applies a similar approach. The Cybersecurity Act 2018[34] applies overarching requirements to 11 critical infrastructure sectors, including telecoms, while sectoral regulators such as the Infocomm Media Development Authority (IMDA) issue tailored codes of practice. For example, the Telecommunications Cybersecurity Code of Practice provides flexibility and can be updated as threats evolve, ensuring consistent protections while remaining responsive to sector-specific risks.[35]

To promote coordination across different policies operators suggested that **as new regulation is implemented, policymakers should automatically review its consistency with existing rules.** If necessary, inconsistencies can be identified and ideally eliminated as new regulation is introduced.

32 Security of Critical Infrastructure Act 2018 (SOCI)
33 Security of Critical Infrastructure Rules
34 Singaporean Cybersecurity Act
35 Telecommunications Cybersecurity Code of Practice

> "Data access provisions are important, but governments need to think of this holistically, to make sure that data privacy, and telco and cyber regulations are consistent"
>
> Latin American MNO

For example, some operators noted that consistent definitions must be used in cybersecurity regulation and related adjacent regulations such as telecoms licensing, data protection and privacy regulations or AI policy frameworks. This avoids overlapping or inconsistent obligations with sector-specific cybersecurity requirements, which can otherwise create uncertainty over how personal data is used, processed, and secured – particularly when AI-enabled or cloud-based security solutions are deployed to safeguard networks, or when incidents and breaches involving personal data must be reported. An internally consistent approach strengthens internal governance, clarifies compliance responsibilities, and ensures that privacy and cybersecurity obligations reinforce rather than conflict with each other.

## 5.3 International standards and frameworks can support global and cross-sector collaboration

Cybersecurity threats are inherently transnational, often affecting networks and infrastructure across borders. In this context, national cybersecurity policies should be mapped to globally recognised standards and foster cross-border consistency. Alignment with existing industry and international frameworks not only enhances interoperability and strengthens security solutions, but also facilitates shared responses to emerging threats. Collaboration between countries and regions is therefore crucial to treat cybersecurity as a collective issue, rather than one constrained by national borders.

## Internationally misaligned regulation adds cost

**Misalignment of regulation across countries within a region is a concern.** Many operators noted that they face differing cybersecurity regulations in neighbouring countries where they operate. In some cases, even where rules are derived from a regional framework (e.g., an EU Directive), national implementation often introduces variations. For operators active in multiple markets, these differences create uncertainty and unnecessary compliance burdens.

> "Companies operating across [European] countries require unified cybersecurity regulation, ideally through an Act rather than a Directive like NIS2 because cross-border harmonisation is needed."
>
> European MNO

Global standards are designed to provide high-level objectives that can be adapted to national contexts. However, when countries diverge too far from these standards or isolate themselves from international cooperation, they risk creating national vulnerabilities. Such fragmentation weakens collective defences and makes it harder for mobile operators to access up-to-date threat intelligence or respond effectively to emerging threats, as they must navigate unique national systems and tools.

**Diverge from global standards only where necessary.** Despite the global nature of cyber threats, some policymakers still design regulations in isolation to address local challenges. While it is important to reflect national context, infrastructure and capabilities, overly localised frameworks can create inefficiencies and new vulnerabilities. Global standards provide a strong foundation, but national frameworks may at times need to diverge to account for local risk levels or sector maturity. When this occurs, operators stressed that regulators should clearly explain how and why they are going beyond international norms. Without such clarity, requirements risk being misinterpreted, leading to inconsistent and fragmented implementation.

> "You need to align with the local context...In some cases ISO 27001 might be right, but it should not be applied in every case...it might not be appropriate for your own threats and limits"
>
> Asia-Pacific MNO

## Divergent standards add complexity and weaken resilience

The absence of harmonisation across countries forces operators to navigate multiple, often conflicting, cybersecurity standards. Instead of relying on a consistent baseline, multinational operators must maintain separate compliance frameworks for each jurisdiction, increasing unnecessary costs and complexity. This fragmentation can also delay decision-making during critical incidents, as different reporting requirements and definitions create uncertainty about which standards apply. In practice, the lack of alignment not only creates administrative inefficiency but may also reduce the speed and effectiveness of operators' cybersecurity responses.

These inconsistencies have wider consequences for resilience and innovation. Fragmented standards may make it harder for operators to adopt advanced technologies or to scale security solutions across markets, slowing the deployment of tools such as AI-driven threat detection or secure cloud-based services.

### Enhancing cybersecurity with global standards and regional cooperation

**Align national rules with international standards.** To reduce duplication and inconsistency, cybersecurity regulation should be aligned with widely accepted standards, such as the ISO 27001, which sets principles for information security, cybersecurity, and privacy protection.[36] Using industry and international standards as a baseline allows regulators to reflect domestic priorities while maintaining coherence and avoiding unnecessary divergence. It also makes the compliance process more efficient, since alignment with international standards will typically be sufficient to demonstrate compliance with specific requirements for both regulators and customers.

> "Good practice will be to go to global industry standards, for example taking ISO27000 series as global baseline"
>
> Latin American MNO

**Map national regulations to existing international standards.** In Europe, for example, operators noted that the European Union Agency for Cybersecurity (ENISA) mapped NIS2 requirements to existing European and international standards or frameworks, including ISO 27001.[37] This approach enabled operators to extend existing internal processes rather than build duplicative processes or complex mapping to national regulations. This supports predictability in audits, facilitating implementation by compliance teams, and ensuring regulation complements rather than complicates cybersecurity operations.

> "ENISA mapped ISO standards to NIS2, if new regulation could always be easily mapped to existing standard, it would reduce the cost and burden for operators"
>
> European MNO

**Promote regional cooperation.** Beyond global standards, regional engagement and cooperation by policymakers reduces fragmentation and strengthens coordinated defence and responses to cyber threats. Joint regulatory design, cross-border threat-sharing platforms, and capacity-building initiatives help create unified cybersecurity policies that operators can implement consistently across markets.

For example, the EU has institutionalised regional cooperation through the NIS Cooperation Group[38] and the CSIRTs Network[39]. In the African Union (AU), the Malabo Convention provides a continent-wide cybersecurity framework,[40] but its slow ratification (adopted in 2014, in force only since 2023 after 15 of 55 states ratified) has limited its credibility and effectiveness.[41] Region-wide conventions of this nature can offer Africa a vehicle to harmonise cybersecurity frameworks and coordinate regional cyber defence.

## 5.4 Obligations should be outcome-oriented and risk-based

Cybersecurity regulation is most effective when centred on achieving meaningful security outcomes while allowing flexibility in how these are reached. This ensures that regulation is impactful across both the telecoms sector and all critical infrastructure sectors while minimising market distortions. Proportionate regulation should also be risk-based, reflecting the varying and potential impacts across networks, rather than applying rigid one-size-fits-all standards.

### Cybersecurity regulation is often too prescriptive and input-focused

**Over-prescriptive regulation can drive a box-ticking culture.** Operators highlighted that overly prescriptive cybersecurity regulation tends to foster a compliance culture centred on meeting rules, rather than addressing real cyber risks or delivering genuine security benefits. Instead of enabling proportionate, threat-informed responses, some regulatory frameworks encourage 'box-ticking' exercises, particularly in jurisdictions with less mature institutions. For example, some operators reported

36 ISO/IEC 27001
37 ENISA (2025) NIS2 Technical Implementation Guidance
38 NIS Cooperation Group
39 CSIRTs Network
40 African Union Convention Cybersecurity
41 Africa: AU's Malabo Convention set to enter force after nine years

inspections focused on whether specific security technologies were adopted, even when they were ill-suited to their actual risk profile or threat landscape, or had already been superseded by more effective alternatives.

> "Regulation can affect culture. Overly prescriptive compliance drives security culture from threat-risk mitigation towards box-ticking culture"
>
> Asia-Pacific MNO

**Compliance regimes are less effective when they focus on inputs, not outputs.** Operators noted that compliance regimes are often designed around inputs (i.e., specific controls, tools, documentation or technologies) rather than real outputs (i.e., improve resilience, reduced risk, stronger detection and response). Several operators reported that current approaches evaluate whether particular requirements have been met, not whether they have actually improved network security.

> "The issue is regulators think compliance equals being secure...This is not the case."
>
> Latin American MNO

**In some jurisdictions ad hoc compliance requirements create regulatory ambiguity and are disconnected to risk.** In addition to regular audits and formal inspection cycles, some operators reported being subject to a growing volume of ad hoc compliance requests from regulators or other agencies. These demands are costly as they are resource-intensive and unplanned. However, operators noted that they are often not directly linked to specific cyber threats, risk events, or changes in the network, but appeared to reflect reactions to social media comments. For example, operators reported that in some jurisdictions, incidents may be escalated to regulatory attention not because of technical severity, but because they attracted media coverage or public scrutiny.

> "Ad hoc requests can create huge distractions that are not necessarily mapped to risk"
>
> North American MNO

**Prescriptive mandates can also limit flexibility for operators** to develop new solutions, restricting innovation and investment in innovation in the telecoms market. Operators stated that overly prescriptive requirements of inputs were sometimes difficult or impractical to implement because they referred to older systems or legacy technologies that the operator had already phased out.

## Rigid and inconsistent compliance regimes divert focus from real threats

Compliance regimes that prioritise rigid inputs over outcomes lead to operational inefficiencies and diverts capacity from core cyber functions such as threat analysis, incident detection, and vulnerability management. Operators noted that unstructured or reactive requests from regulators increasingly drive day-to-day compliance work, over and above planned obligations. These ad hoc requests are rarely risk-based and seldom lead to meaningful remediation, instead adding a parallel layer of informal oversight that adds to reporting fatigue and reduces predictability. The resulting uncertainty undermines planning, complicates internal governance, and weakens trust between operators and public authorities.

> "Compliance doesn't always drive real cybersecurity, sometimes operators buy a new firewall or prepare for the audit because they need to comply rather than operationalising anything. This diverts investment from operations to build security"
>
> Asia-Pacific MNO

## Outcomes are improved by targeting actions on where risks are higher

**Formalistic standards do not reflect different levels of risk.** When standards fail to account for risks and trade-offs, regulation often becomes rigid, overly cautious, and misaligned with real cyber threats. Operators noted that obligations are sometimes imposed without clear purpose or proportionality, which undermines regulatory credibility and weakens compliance.

> "Risk-based frameworks help organisations target resources more effectively"
>
> MENA MNO

Regulation that does not follow a risk-based approach may also fail to safeguard networks. By focusing on threats that are not relevant to national conditions, policymakers risk diverting attention and resources away from genuine vulnerabilities, leaving gaps in network protection. For example, one operator described how strict nationality requirements on cybersecurity staff were applied even to low-risk activities, despite a shortage of qualified staff in the country. This forced the operator to hire less suitable or insufficiently trained personnel, potentially increasing risks rather than reducing them. Another operator observed that policymakers and regulators sometimes prioritise visible or politically salient issues that carry relatively low risk, further diverting resources from more pressing vulnerabilities.

## Effective regulation focuses on outcomes and recognises that resources should be directed to the higher risks

**Outcome-focused compliance offers a more effective way to manage cyber risk across mobile networks.** Rather than enforcing prescriptive, box-ticking rules, regulation should focus on achieving clearly defined security outcomes, such as improved resilience, detection, and response. This allows operators to tailor their approach based on their specific risk profile, operational context, and technical capabilities. By allowing flexibility, outcome-based regulation supports more efficient use of resources, faster adoption of new technologies, and greater adaptability to emerging threats. In a constantly evolving threat landscape, regulatory frameworks should be designed to support solutions that are both effective and adaptable to ensure sustained protection.

Existing frameworks demonstrate how this can work in practice. Australia's SOCI Act requires operators to meet specific security outcomes, without prescribing the exact technologies or processes they must use. Under the Telecommunications Security and Risk Management Program Rules 2024, mobile operators are required to identify and manage cyber risks, but are given discretion in how to do so based on their operations and risk environment. This outcome-driven model ensures alignment between regulatory expectations and each operator's security priorities, without stifling operational flexibility.

The UK Cyber Assessment Framework (CAF) also takes an outcome-based approach, guiding organisations to demonstrate compliance through the achievement of a specific security objective.[42] It provides guidance to organisations on assessing cyber risk. For example, the system security principle requires secure configuration but does not dictate how that outcome must be achieved. This approach helps organisations focus on actual risk mitigation while supporting different implementation strategies across diverse technical environments.

**Compliance should be context specific.** Operators note that compliance should sometimes be context specific, accounting for differences in scale, maturity, and risk exposure. This is an increasingly important element of an effective regulatory framework due to the fast-paced nature of cyber threat evolution, where overly prescriptive mandates may quickly become outdated. In a rapidly changing threat landscape, regulation should remain flexible to support the timely adoption of new technologies and threat-informed practices.

**Avoid costly ad hoc compliance where possible.** Operators highlighted that informal or ad hoc compliance demands (particularly those not clearly grounded in legal frameworks) create uncertainty and weaken trust in regulatory oversight. Regulators should provide clear, stable expectations supported by structured engagement, including regular dialogue, threat intelligence sharing, and performance-based reviews.

**Risk-based policy design is essential.** Effective regulation should calibrate obligations to the actual risk being addressed, not simply enforce blanket rules. Several operators pointed to examples

42 UK Cyber Assessment Framework

where they had to invest in security measures with unclear benefits. A risk-based model mitigates this issue by aligning requirements with real threats, and reducing unnecessary costs. For example, in the UK, the Telecommunications Security Code of Practice differentiates standards based on operator size (measured by annual revenue), helping to protect competition while maintaining high security standards.[43]

## 5.5 The regulatory culture should promote collaboration and trust

Regulatory supervision should foster a collaborative relationship between operators and regulators, positioning compliance as a shared effort to strengthen cyber resilience rather than a bureaucratic process. A constructive regulatory culture is essential for timely intelligence sharing and coordinated threat responses, and for ensuring a collaborative approach to the fight against cybercrime. Regulators can support this by establishing trusted and secure intelligence sharing platforms that protect networks and society, and by promoting public awareness of cyber threats.

### One-sided regulation undermines collaboration and erodes trust

**Lack of engagement with industry leads to a formalistic approach to regulation.** In jurisdictions where regulator-led platforms are weak, absent, or not trusted, operators often rely on private or industry-led alternatives. While initiatives like the GSMA's Telecommunication Information Sharing and Analysis Centre (T-ISAC)[44] and Mobile Threat Intelligence Framework (MoTIF)[45] provide more effective forums for intelligence exchange, the reliance on industry initiatives highlights the gaps in many public systems, which often vary in quality, legal protections, and technical reliability.

**Lack of trust between operators and authorities increases cyber risks and limits participation in formal systems.** Regulatory environments characterised by mistrust or overly punitive oversight discourage transparency and reduce the effectiveness of threat intelligence sharing. When supervision is perceived as penalty-focused, operators may become more cautious in their engagement with authorities, limiting openness in reporting and collaboration. In some jurisdictions, fear of non-compliance or unclear legal rules (especially under regimes with high or even criminal penalties) may reduce incentives to share potentially sensitive cyber threat data.

**Some operators perceived a lack of reciprocity in threat intelligence sharing.** Threat-intelligence sharing is a pillar of cybersecurity. However, some operators reported that, despite investing heavily in intelligence sharing mechanisms, they rarely receive meaningful information in return.

> "You share intelligence where you trust"
>
> Latin American MNO

In some cases, authorities fail to explain how data is used or how it supports broader cybersecurity outcomes. In other cases the information shared with operators was low-quality and lacked review or filtering. The lack of reciprocity reduced the perceived value of reporting and undermines operators' willingness to engage with national threat-sharing systems.

**Structural and institutional barriers to coordinate limited threat intelligence sharing.** In some countries, access to secure and trusted platforms is limited by unclear mandates, overlapping agency responsibilities, or the absence of central coordination. In these cases, threat reporting becomes an burdensome obligation rather than a tool for collective defence against cybercrime.

43 UK Telecommunications Security Code of Practice
44 T-ISAC
45 GSMA MoTIF

## Effective regulation is built on trust, collaboration and proportionality

**Industry engagement to better align with industry realities and real risks.** Operators consistently stressed the value of frameworks that involve early engagement and consultation with the industry. Designing cybersecurity policy in partnership with industry leads to better alignment with real-world risk and enhances compliance outcomes. When regulators invest in regular dialogue, working groups, or joint assessments, they gain deeper insight into operational challenges and promote alignment with national objectives. Public-private partnerships also strengthen capabilities on both sides.

> "There is no central intelligence in developing countries. There is a gap between the higher bar set by more developed countries and what we can achieve at the moment"
>
> Asia-Pacific MNO

Operators called out jurisdictions that actively engage with mobile operators and integrate industry experience into cybersecurity policy. In Finland, nearly 100 public- and private-sector stakeholders contributed to the Cybersecurity Strategy[46], ensuring that regulation reflects real-world threats and operational realities. In Singapore, the IMDA regularly seeks mobile operator feedback on draft standards[47], facilitating trust and cooperation between the public and private sectors. In the US, the NIST Cybersecurity Framework is co-developed with industry input[48], while the Communications Security, Reliability and Interoperability Council (CSRIC)[49] brings regulators and telecoms experts together to shape cybersecurity guidance collaboratively. Finally, the UK's National Cyber Security Centre (NCSC) Industry 100 programme embeds private-sector professionals into the agency to shape guidance and facilitate shared learning.[50]

**Secure, centralised threat intelligence platforms improve national and global resilience.** Operators strongly support secure platforms for reporting and sharing threat intelligence. These platforms reduce duplication, ensure consistency, and provide a trusted single point of contact for regulatory communication. But effective design matters: platforms must offer legal protections for information shared in good faith, technical safeguards to ensure confidentiality, and reciprocal feedback loops that deliver timely, actionable insights. When operators see clear value in participating (through tangible improvements in visibility of cyber threat) they are more likely to contribute actively. Conversely, fragmented systems without feedback or reciprocity discourage engagement and weaken resilience at both national and international levels.

Several jurisdictions provide strong examples of best practice. Saudi Arabia's Haseen platform consolidates incident reporting, threat intelligence, and evidence of compliance into a single interface, supporting national coordination. Australia's SOCI Act also mandates timely reporting to the Australian Cyber Security Centre (ACSC)[51], while allowing flexibility in how operators meet their obligations. In the US, The US Comm-ISAC[52] demonstrate the value of coordinated responses, while industry-led platforms help extend this collaboration into the private sector.

**Cross-border coordination is essential in a transnational threat environment.** Cyber threats do not stop at national borders, and operators stressed the need for international coordination to monitor and response to cybercrime. Regulatory frameworks should reflect this reality by supporting secure global data flows and interoperable threat intelligence platforms. In the EU, the CSIRTs Network links incident response teams across Member States, enabling rapid information exchange and coordinated cross-border responses.

> "Cross-country coordination in cyber intelligence is important...the problem is usually transnational"
>
> Asia-Pacific MNO

**Trust-based supervision builds better compliance.** Operators consistently highlighted that cybersecurity regulation is most effective when built on trust and collaboration. A constructive regulatory culture (characterised by early consultation, structured engagement, and predictable enforcement) fosters openness and improves compliance.

46 Finnish Revised Cybersecurity Strategy
47 IMDA Feedback on Regulatory Standards
48 NIST Cybersecurity Framework Industry Input
49 CSRIC
50 Industry 100
51 Australian SOCI Act Reporting Guidelines
52 US Comm-ISAC

Operators in LMICs noted that sometimes authorities had different levels of trust in mobile operators' abilities to meet cybersecurity standards, and to constructively engage with authorities. As a result, they adopted "low trust" behaviours in their interactions with mobile operators. This imposed unnecessary costs on operators and some noted that it could increase the level of network vulnerability where mobile operators were compelled to grant authorities routine access to parts of their network (so authorities could directly collect data and monitor compliance). Mobile operators argued that it would be more efficient and effective for them to be able to earn the trust of cybersecurity operators, and for high trust mobile operators to face a less intrusive and more flexible different approach to compliance.

**Proportionate enforcement encourages engagement and builds confidence.** Effective cybersecurity oversight requires not just collaborative engagement, but also fair and proportionate enforcement. Operators highlighted that penalties and compliance expectations must be scaled to their capacity, role, and risk exposure. When enforcement is transparent, predictable, and tailored, it reinforces trust and encourages operators to engage openly with regulators. In contrast, one-size-fits-all or punitive approaches can drive caution, reduce cooperation, and ultimately weaken cyber resilience. Proportionate enforcement allows regulation to serve as a shared mechanism for managing risk, rather than as a compliance burden or adversarial threat.

## 5.6 Regulation should take a proactive approach to managing cyber threats

In some jurisdictions, cybersecurity approach to mitigating risk can be excessively reactive, triggered by incidents or media attention rather than long-term planning. This can lead to short-term compliance activity at the expense of sustained investment in resilience. While a reactive response is essential when incidents occur, best practice complements this with a proactive, security-by-design approach, grounded in clear, outcome-based rules that allow flexibility in implementation. When regulation is stable and forward-looking, operators can plan strategically, innovate, and build stronger defences, delivering better protection and reliability for end users.

### Incident-led approach undermines strategic security planning

**Regulatory oversight is triggered by specific events or media attention, rather than grounded in a structured, forward-looking strategy.** Operators described scenarios where regimes incentivise short-term responses to external pressure, rather than long-term investment in security resilience. In this context, operators may be forced to shift resources to respond to one-off regulatory demands, rather than pursuing more strategic or risk-prioritised improvements.

> "Europe takes a proactive approach, while Asia currently tends to be more reactive. Reactive regulation typically increases costs compared to proactive, input-oriented regulation"
>
> European MNO

### Excessively reactive oversight diverts resources from long-term cyber resilience

When regulation is unpredictable, or authorities respond inconsistently to emerging threats, operators find it challenging to justify investments in long-term cybersecurity initiatives. Instead, resources may be funnelled into short-term, surface-level compliance activities that offer limited improvement to actual cyber defences. Over time, this weakens the sector's ability to stay ahead of threat actors.

Best practice promotes forward-looking and security-by-design approaches to mitigating risks.

**Security-by-design should be the foundation of regulation.** Best practice embeds security-by-design principles into regulatory expectations, encouraging operators to integrate security considerations at every stage of product and network development. Security-by-design does not exclude the need for agile responses to threats or incidents, but it ensures that operators are structurally equipped to do so. Policymakers should explicitly promote this approach through guidance, incentives, and outcome-based mandates.

> "Security-by-design regulation like NIS2 is more cost-effective in the long-run"
>
> European MNO

For example, the EU framework for protection of critical national infrastructure (NIS2) explicitly required telecoms operators to implement "security-by-design and default".[53] The Australian Signals Directorate Manual on Information Security provides principles by which organisations can protect their infrastructure. These include that "systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned using Secure-by-Design and Secure-by-Default principles and practices."[54]

**Forward-looking frameworks reduce disruption and strengthen resilience.** When rules are forward-looking and built around resilience and adaptability, operators are more likely to invest in robust defences rather than diverting resources into reactive compliance. Regulation that provides stability and allows operators to choose how to meet defined objectives also reduces the need for ad hoc interventions, which can disrupt innovation and weaken trust. Ultimately, these frameworks enable more secure networks and deliver better protection for end users.

## 5.7 Regulatory capacity should be strengthened to ensure effective implementation

Cybersecurity regulation is only effective if regulators have the capacity to put frameworks into practice, promote the application of best practice, and monitor compliance in a proportionate way. In many countries, this capacity is constrained by shortages of skilled personnel, inadequate technical infrastructure, weak institutional support, underinvestment, unclear mandates, or fragmented governance. Effective cybersecurity regulation therefore depends on well-resourced, credible institutions with the expertise to enforce rules proportionately, engage constructively with operators, and adapt to evolving threats.

### Limited regulatory capacity undermines effective implementation

**Some countries have frameworks without the means to ensure effective implementation.** Operators sometimes noted a degree of disconnection between policy and implementation. In some countries, cybersecurity rules are introduced without any dedicated institutions to monitor or guide implementation. Even where regulators exist, they may lack resources to carry out audits, offer clarification, promote best practices or engage with industry on technical issues. A weak institutional base undermines the credibility of regulation and erodes trust between regulators and operators. It also opens the door to regulatory inconsistency, especially where agencies lack the technical expertise to adapt rules to evolving threats.

**Consider risks of "copy and pasting" cybersecurity frameworks from more advanced jurisdictions.** Operators reported that simply copying cybersecurity frameworks from more advanced cyber security jurisdictions, without the capacity to interpret, adapt, and implement them effectively, can lead to unintended burdens and inefficiencies.

> "It is not helpful to import regulation from the EU or US, and implement it straight away without necessary institutions"
>
> African MNO

53 Directive (EU) 2022/2555 measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) recital 104.

54 Australian Signals Directorate Manual on Information Security

In contexts where institutional capacity is limited, even well-intentioned global standards may overwhelm regulators and result in frameworks that are poorly aligned with operational realities. As one operator noted, what is needed is regulators who are equipped with the skills, tools, and expertise to evaluate international best practices and tailor them intelligently to national threat environments and regulatory objectives.

**Regulatory capacity varies significantly across jurisdictions.** While some countries have established dedicated cybersecurity agencies, trained staff, and established audit mechanisms, others face challenges in resourcing and sustaining regulatory functions. Operators described scenarios where mandates were introduced before the supervisory authority was fully functional. Others raised concerns that enforcement practices were influenced by political or commercial pressures, undermining the credibility of the regime. This uneven landscape can lead to uncertainty for mobile operators, particularly those operating across multiple jurisdictions with uneven regulatory maturity.

> "Institutional capacity impacts the culture around regulation"
>
> Asia-Pacific MNO

## Credible and resourced cyber security institutions build sector wide capabilities

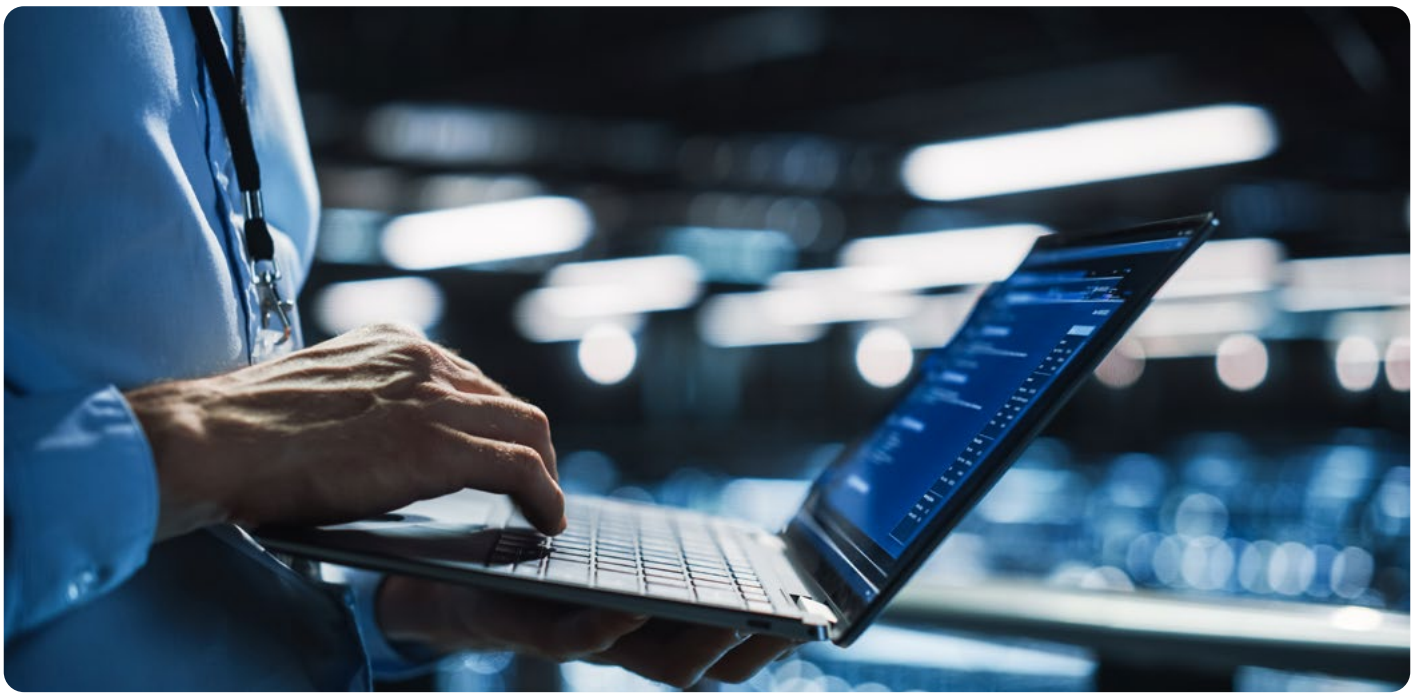
**Strong regulatory capacity is critical to making cybersecurity frameworks credible, effective, and trusted.** This means investing in well-defined institutions with the skills and expertise, tools, and infrastructure needed to enforce regulation and engage constructively with operators. Skilled regulators (those with up-to-date threat intelligence, auditing capabilities, and real-world industry insight) are far better positioned to support meaningful security improvements. They can provide clear implementation guidance, facilitate policy feedback loops, and help operators interpret evolving regulatory expectations.

**Trusted institutions promote strategic engagement and sector alignment.** When regulators are capable and well-resourced, operators are more likely to see compliance as a strategic function, not just an administrative burden. This improves alignment, enhances sector-wide resilience, and helps ensure that regulatory frameworks deliver tangible outcomes. Operators also noted the value of providing cybersecurity training to regulatory staff to strengthen understanding of operational realities and support more context-aware policy development.

Operators in Latin America highlighted Chile's Agencia Nacional de Ciberseguridad (ANCI) as a positive model for institutional credibility and regulatory professionalism: "Chile stands out in Latin America with the adoption of their law on cybersecurity and critical information infrastructure, representing a major step forward in the region". ANCI was established following the 2024 enactment of the country's Cybersecurity Framework Law.[55] It was created with a clear mandate to oversee and enforce cybersecurity obligations for essential service providers, and it operates with dedicated financial resources and a merit-based leadership structure grounded in public service law.

**Institutional capacity is necessary for cybersecurity regulation to be applied in a proportionate way that reflects risks.** Without sufficient regulatory capacity, even well-intentioned rules may be applied in rigid or formalistic ways. Operators noted that where supervisory authorities lack the expertise or legal foundations to apply frameworks effectively, compliance becomes procedural and does not reflect risks.

55 Chile: a frontrunner in cybersecurity in Latin America



# 06. Conclusions and recommendations

Cybersecurity is essential to ensuring trust, safety, and resilience in a digitally connected world. The regulatory and policy framework that governs cybersecurity for mobile operators is becoming ever more complex, with multiple requirements stemming from telecoms sectoral policy, horizontal regulation, obligations from adjacent sectors, and wider policy areas such as data privacy or AI regulation.

While regulation plays a critical role in supporting mobile operators to manage cyber security, poorly designed frameworks can impose unnecessary burdens, reduce operational efficiency, and, in some cases, increase exposure to cyber threats. These inefficiencies ultimately affect end users by weakening network resilience and delaying access to secure, reliable digital services.

Operators face different regulatory challenges depending on the maturity of national digital policy frameworks. In more mature cybersecurity regimes, regulation is often complex and fragmented, with overlapping or inconsistent requirements. A significant share of resources that operators allocate to cybersecurity is spent not on active threat mitigation but on interpreting new rules, reconciling inconsistencies, and responding to reporting demands. However, more advanced cyber security regimes tend to benefit from stronger institutions, trusted threat intelligence platforms, and more collaborative approaches to policymaking.

In less mature regulatory contexts, operators may enjoy greater flexibility in managing risks, but often face more ad hoc oversight, unclear guidance, and rigid, formalistic enforcement disconnected from real threats. In the absence of a coherent framework, the burden of designing and maintaining effective security systems often falls disproportionately on operators. Under-resourced authorities may impose rigid mandates that do not reflect actual risk or operational context, resulting in unnecessary costs and inefficiencies.

These challenges highlight the need for proportionate, coherent, and outcomes-focused regulation. Effective cybersecurity policy should reduce unnecessary complexity, align compliance expectations across sectors, follow global standards and provide flexibility in how operators implement secure networks in a way that reflects risk. Regulatory frameworks should be clear, consistent, and designed to support real-world resilience, not just procedural compliance.

This report has proposed six practical steps for policymakers to strengthen mobile network security without imposing unnecessary or significant new costs. They focus on applying policy in a way that is risk-informed, collaborative, and effective, helping the sector remain secure in an evolving threat landscape.

- **Harmonisation:** Align cybersecurity policy with international standards, such as ISO 27001 or NIST, to support coherence across policies and internationally. While some local adaptation may be inevitable, global standards provide a common framework that can reduce duplication, simplify compliance, and strengthen coordinated responses to transnational threats.
- **Consistency:** Ensure new policies and frameworks are consistent. Technology in digital markets moves at a rapid pace. This means that policies including those around cybersecurity, inevitably evolve. In this context governments should systematically ensure that as new policy is introduced it is consistent and coherent with adjacent policy areas. It may be helpful to explicitly require that as new regulation is introduced it is consistent with pre-existing regulation.
- **Risk- and outcome-based:** Where possible, ensure cybersecurity obligations are risk-based and outcomes-based. Cybersecurity frameworks should define clear objectives and reflect the level and nature of actual risk. Regulations should be tailored to the operational realities of different types and sizes of operators, ensuring that obligations are proportionate. An outcome-focused regulatory approach allows operators flexibility to meet goals in the most effective and efficient manner for their context. This reduces "box-ticking" compliance, fosters innovation, and ensures resources are directed toward genuine security improvements.
- **Collaboration:** Institutions should promote a collaborative regulatory culture. Cybersecurity regulation should be enforced through engagement, not punishment. Genuine consultation with industry stakeholders can ensure that implementation of cybersecurity policy is proportionate to regulatory objectives. At the same time, threat intelligence sharing with streamlined reporting can increase awareness of cyber threats, strengthen resilience, and foster a joint approach to combating cybercrime.
- **Security-by-design:** Encourage a proactive, security-by-design approach to investment. Cybersecurity regulation should promote proactive risk mitigation strategies, such as security-by-design principles, early threat detection, and crisis simulation. Governments should avoid relying solely on post-incident compliance or ad hoc enforcement. Instead, policies should incentivise long-term investment in prevention, helping reduce overall system vulnerability and long-term costs.
- **Capacity-building:** Ensure that cybersecurity authorities have the institutional capacity for effective application of policy and regulation. Governments and regulators need adequate human, financial, and technical resources to credibly implement and enforce cybersecurity frameworks. Strong institutions enhance regulatory credibility, ensure consistent application, and support effective engagement with the mobile industry.

These recommendations do not require major new investments but rather a shift in approach toward collaboration, trust, and shared responsibility. By adopting these, policymakers can help ensure that mobile networks remain secure, resilient, and capable of supporting the digital services that societies increasingly rely on.

# Annex
# List of best practice examples

| Dimension | Sub-category | Country or region | Example |
|---|---|---|---|
| **Harmonisation** | Map policy and regulation to international standards | EU | Network and Information Systems (NIS) 2 Technical Guidance |
| | Regional cooperation | EU | NIS Cooperation Group and Computer Security Incident Response Teams (CSIRTs) Network |
| | | African Union | Malabo Convention |
| **Consistency** | Sector-specific guidance | Australia | Security of Critical Infrastructure (SOCI) Act, Enhanced Response and Prevention (ERP) Act, Telecommunications Security and Risk Management Program (TSRMP) Rules |
| | | Singapore | Cybersecurity Act 2018, Telecommunications Cybersecurity Code of Practice |
| **Risk- and outcome-based** | Policy design | UK | Telecommunications Security Code of Practice |
| | Outcome-focused compliance | Australia | SOCI Act, TSRMP Rules |
| | | UK | Cyber Assessment Framework (CAF) |
| **Collaboration** | Industry engagement | Finland | Cybersecurity Strategy |
| | | Singapore | Infocomm Media Development Authority (IMDA) |
| | | US | National Institute of Standards and Technology (NIST)<br>Cybersecurity Framework, Communications Security, Reliability and Interoperability Council (CSRIC) |
| | | UK | National Cyber Security Centre (NCSC)'s Industry 100 |
| | Secure threat intelligence platforms | Saudi Arabia | Haseen |
| | | Australia | Australian Cyber Security Centre (ACSC) |
| | | US | US Communications Information Sharing and Analysis Centre (Comm-ISAC) |
| | Cross-border coordination | EU | CSIRTs Network |
| **Security-by-design** | Proactive approach to mitigating cyber risk | EU | Network and Information Systems (NIS) 2 |
| | | Australia | Australian Signals Directorate Manual on Information Security |
| **Capacity-building** | Trusted institutions | Chile | Agencia Nacional de Ciberseguridad (ANCI) |

Source: Frontier Economics.

**GSMA Head Office**
1 Angel Lane
London
EC4R 3AB
United Kingdom
gsma.com