



ARTICLE

Cybersecurity Strategy for Developing Countries

[Rory Macmillan](#) and [Christina Heliotis](#)

Jun 15, 2026

7 min read

<u>Africa</u>	<u>Agriculture & Food</u>	<u>Asia & Pacific</u>	<u>Data Privacy</u>	<u>Data Privacy Laws &</u>
<u>Regulations</u>	<u>Data Privacy Litigation & Enforcement</u>	<u>Financial Services</u>	<u>Healthcare</u>	<u>Latin</u>
	<u>America & Caribbean</u>	<u>Transportation</u>		

Narumon Bowonkitwanchai via Getty Images

An effective and sustainable cybersecurity strategy is a baseline requirement for effective governance for economies at every income level. Without it, public services, private organizations and individuals are vulnerable to cyber-attacks of increasing sophistication which can disrupt a country's critical infrastructure, supply-chains and digital economy services.

For all countries the question is how to design a cybersecurity strategy that is realistic, sustainable, and aligned with available resources and actual risks. For developing countries, the lack of human and technical resources makes risk-based prioritization all the more important.

A shared exposure to cyber attacks

No country is immune to cyberthreats. Ransomware, phishing, business-email compromise, and supply-chain attacks have affected governments and operators in economies at every income level. Public administration, finance, health, digital infrastructure, and transport remain among the most heavily targeted sectors worldwide, and many jurisdictions now face serious incidents on a near-daily basis. ¹ Such attacks often target payment and health systems and have compromised millions of personal records and temporarily halted critical services. ² The use of AI-assisted tools is increasingly changing the way cyberattacks against public-sector systems are carried out, by enabling attackers to automate parts of an intrusion, accelerate vulnerability exploitation, generate custom attack scripts, and support large-scale data extraction. This risk was illustrated in late 2025 and early 2026, when Mexican government systems were reportedly compromised in a multi-agency cyberattack affecting the federal tax authority, civil registry, health department, electoral authority, local governments, and a public water utility, resulting in the reported exfiltration of more than 150 GB of sensitive public-sector data. ³

Constraints specific to developing countries

Developing economies must confront this threat landscape with a much thinner technical, legal, institutional and fiscal toolkit. Typical constraints include a shortage of trained cybersecurity professionals, limited or nascent national CSIRTs, fragmented sector oversight, and legal frameworks that are incomplete, inconsistent, or poorly implemented. Financing is often episodic and heavily donor-driven. This can skew

national agendas toward external priorities rather than a coherent sequence of domestic reforms. Telecom regulators, central banks, digital-government units, and security agencies may each hold partial cyber mandates, but without clear hierarchy or coordination, resulting in gaps and overlaps.

Prioritization under tight constraints

In practice, developing countries can execute only a small number of major reforms in any given cycle. Over-ambitious strategies are therefore prone to stalling, leaving implementation gaps, eroding confidence in the institutions responsible for delivery, and crowding out more urgent, high-impact measures. International organizations and specialist bodies 4

underline the same point: ambition must match capacity, be properly sequenced, and rest on sustainable financing if it is to produce real resilience.

Asking the right questions before legislating

Against that backdrop, cybersecurity strategy for any given developing country needs to be developed strategically and systematically, aligned with national development priorities and constraints. The following questions are framed for developing countries and draw on the authors' practical experience and the updated World Bank and ITU Guide to Developing a Cybersecurity Strategy. 5

1. Who is in charge?

- Which institution will be the lead national cybersecurity authority, and on what statutory basis will it coordinate across government and with independent regulators? A clearly mandated lead authority is essential for accountability and for donor coordination. Very often, this will build on and integrate the early efforts of the Central Bank and the telecom regulator to promote cybersecurity across the financial and electronic communications systems, respectively.
- How will its mandate intersect with those of defence and interior ministries and security agencies, telecom and financial regulators, the data protection authority, and digital-government units? A formal mapping of "who does what," in law and in

practice, is necessary to avoid duplication and gaps. Some variable geometry is inevitable and not necessarily harmful – the jostling among different institutions can, while inefficient, even lead to better outcomes. But caution is needed to avoid cybersecurity powers being used for evidence collection for cybercrime investigation (which may include content that is frowned upon by powerful interests).

2. What are the key sectors and main risks?

- Based on the country's current levels of connectivity, degree of digitalization, and its economic structure, which sectors are most critical to protect: government platforms and ID systems, payments and mobile money, health, energy, transport, or communications? These can be very different depending on the country. For instance, many developing countries do not have extensive centrally controlled infrastructure, operating on the basis of distributed systems (e.g., electricity generators, informal bus networks, water delivery trucks). Payment systems may need to include mobile money systems operated by telecom operators.
- How does this affect the first wave of regulation, supervision, and capacity-building? Priorities in developing economies often differ from advanced economies, which may focus more on industrial control systems or complex financial instruments. Design needs to weigh the overall objectives of establishing a coherent system alongside the benefits of building incrementally on existing initiatives and institutions. In several low-income countries, rapid growth in mobile money and limited supervisory capacity have justified prioritizing security of digital financial services and telecom infrastructure ahead of more advanced industrial cyber risks in the initial reform cycle.

3. How will cybersecurity be financed and sustained?

- Who will bear the cost of security measures in critical sectors: end users, regulated operators, the national budget, or development finance institutions, and in what proportions? This will depend on the structure of the sector. Telecom operators and banks are often among the largest and most profitable economic players in the economy and will be expected to self-fund. The costs of digital public infrastructure, such as a national ID system, may be borne from fees for

authentication services, the national budget, or in early years by international financial institutions.

- How will multi-year operating costs, including for staffing, incident response, supervision, training, public awareness, be integrated into regular budget cycles rather than treated as exceptional projects? Here, long term financial planning is vital. The risk of embarking on cybersecurity strategy that runs dry of funding as the years advance is high.

4. How will relevant laws and policies be aligned and harmonized?

- How much should cybersecurity be governed on a horizontal, economy-wide basis, as opposed to through vertical sector regulators? Should risk-based security obligations for operators of essential services be implemented primarily through sectoral regulation and standards, limiting cross-cutting cybersecurity law to what is strictly necessary, instead of layering overlapping regimes? What matters is the overall coherence, clarity of obligations, and realistic enforcement.
- How does the structure of sector ownership and operation affect how law and policy should be used? If the sector is government owned and operated, decisions may be made and implemented through policy. If the sector includes private sector entities, legal obligations will be required. These need to be designed so that they incentivize the desired outcomes, in particular risk-based adoption of proportionate measures, and sharing information about incidents. The use of regulation may encounter resistance. Obligations to adopt security measures may eat into the income statement. Obligations to share information may cause concern with competitors. Requirements to conduct risk assessments, audits and other processes may require hiring staff and creating governance levels on top of running the core business.
- How does the structure and complexity of the sector affect regulatory functions? Dealing with a sector that has many competing players and many-layered supply chains will differ from a highly concentrated sector with only a few major infrastructure operators. Close relationships and iterative communication and consultation may be useful between cybersecurity authorities and key large players, but a proliferation of smaller players may require more structured rules.

- How do the existing legal and regulatory frameworks relevant to cybersecurity, including criminal law, cybercrime, national security, procurement, telecoms, data protection and procurement interact? What potential conflicts, gaps, or deviations from international good practices should be identified? Are these frameworks adequate for ensuring cybersecurity practices, or do they create unrealistic or overly burdensome obligations for regulated entities?

5. What level of centralization is appropriate?

- Related to question 4, which functions should be centralized (for example, threat intelligence, national situational awareness, some incident-response capabilities), and which should sit with sector regulators or major operators that have domain expertise? The Guide to Developing a National Cybersecurity presents this as a deliberate choice between breadth and depth, centralization and subsidiarity, not something to be left to institutional drift. 6
- How can central oversight be designed to avoid paralyzing rapid local action, especially in sectors where outages have immediate human consequences, such as telecom, payments, health and energy?

6. What will incident reporting and response look like in practice?

- Whom should operators of critical information infrastructure be legally required to notify, under what thresholds, and within what timelines? How will this work when incidents span multiple sectors, such as a ransomware attack that affects both a government payment platform and mobile money providers?
- Who conveys cross-sector response, what must be communicated publicly and when, and how will a nascent or future national CSIRT fit into this framework?

7. When should the country seek external advice, and on what terms?

- Which external partners, other states, development institutions, standard-setting bodies, private service providers will the government rely on for technical, legal,

and operational support, and how will engagement be coordinated to avoid conflicting advice?

- What safeguards will ensure that external support aligns with national priorities and does not create dependence on a single vendor, model, donor, or externally drafted legal template unsuited to local conditions?

8. How will human rights, transparency, and democratic governance be protected?

- How will new cybercrime offences, expanded investigative powers, and security obligations be calibrated to protect privacy, dignity, freedom of expression and association, and due process, in line with constitutional and treaty obligations? International bodies increasingly warn that poorly designed cybersecurity laws can harm rights and trust, sometimes as much as the cybercrime they aim to address.
- What transparency, oversight, and redress mechanisms will accompany new powers, especially where national security and secrecy are invoked, so that cybersecurity is not used as a pretext for unrelated control measures?

9. What factors should be evaluated when designing a cybersecurity capacity-building program?

- Which sectors and operators are so critical to the digital economy that their security teams and operational staff must be first in line for training, tooling and on-site support, and how will this prioritization be sequenced over the next three to five years?
- What governance mechanisms will ensure that donor-funded programs, vendor trainings and domestic initiatives follow a single national plan, using concrete performance metrics like response times and implementation of basic controls?

10. How will the strategy become a living cycle, not a static document?

- What mechanisms will translate the national strategy into a set of concrete, costed initiatives with named owners, milestones, and performance indicators that can be monitored over time?
- How will evaluation, course-correction, and renewal be institutionalized so that lessons from incidents and implementation shape the next version of the strategy, creating a continuous governance cycle rather than a one-off exercise?

For legal and policy decision-makers in developing countries, discipline at this structuring stage can be critical. If these questions are answered candidly and in order, the resulting cybersecurity framework is more likely to be coherent, fundable, and rights-respecting. If they are not, initial misalignment between ambition, capacity, and context risks ineffective cybersecurity practices, vulnerability to attack, and ultimately harm to government systems, infrastructure and populations.

Endnotes 

Authors



Rory Macmillan

...

[View Bio →](#)



Christina Heliotis

[View Bio →](#)

Authors
