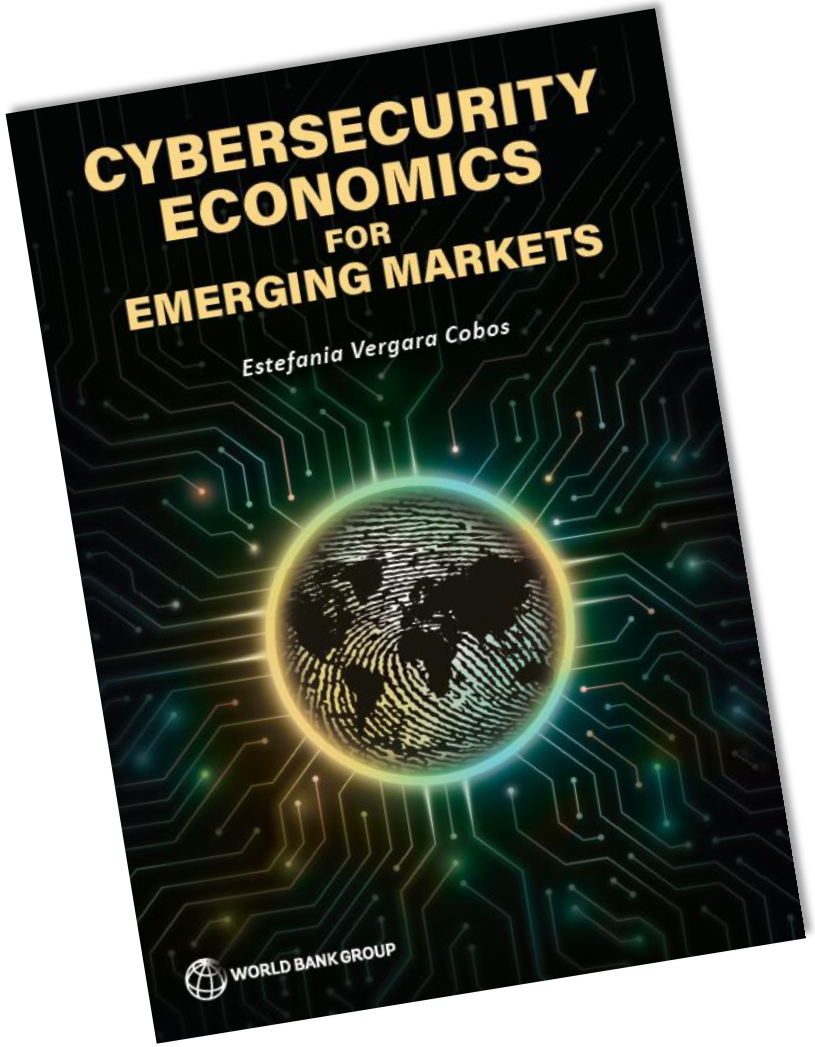
CYBERSECURITY ECONOMICS FOR EMERGING MARKETS

Estefania Vergara Cobos
Economist
Chief Economist's Office Infrastructure, World Bank

WORLD BANK GROUP



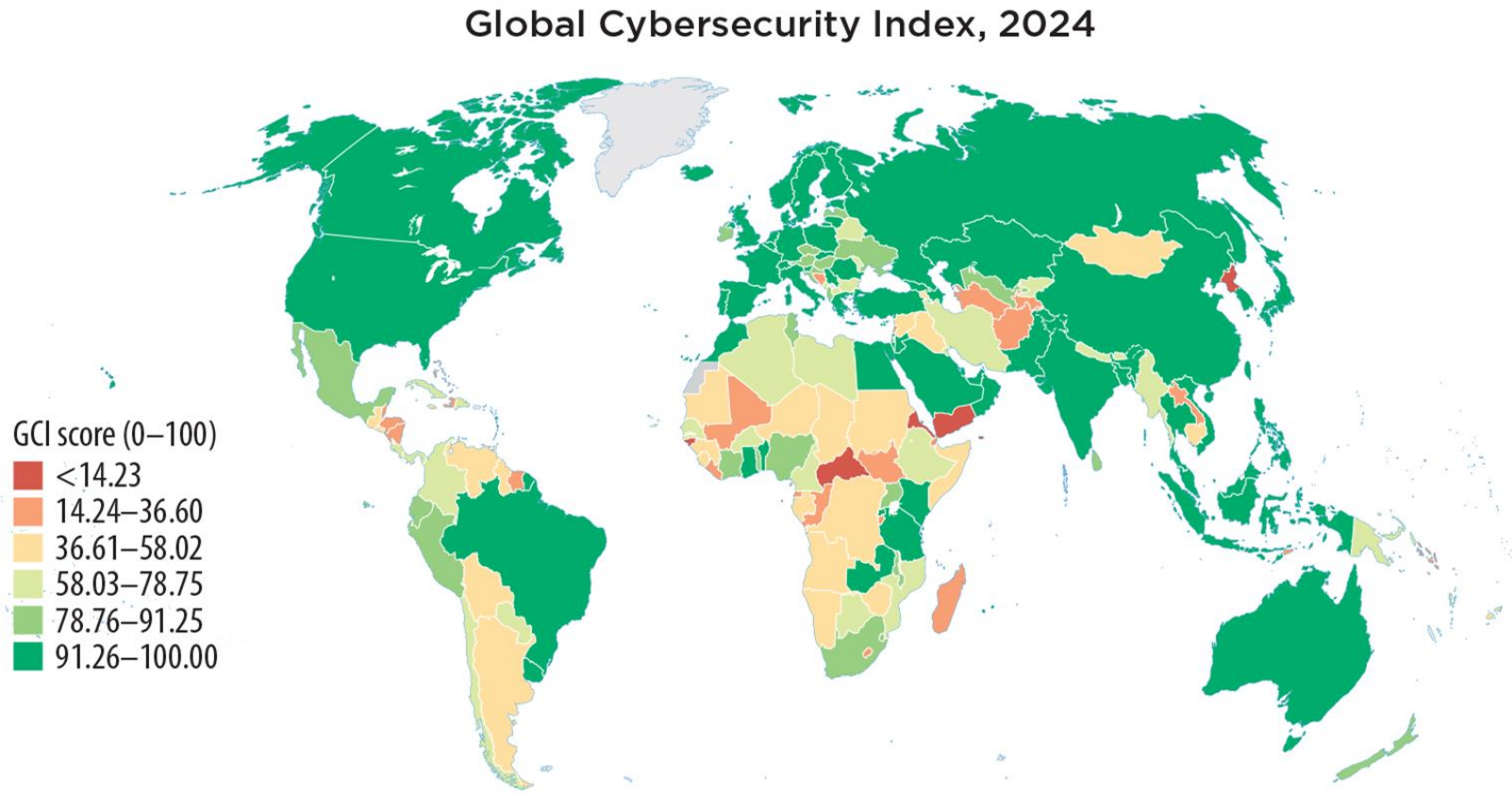
Cybersecurity is not just about protection.

It is a game-changer for economic growth in developing nations.

Cyberspace is a porous environment

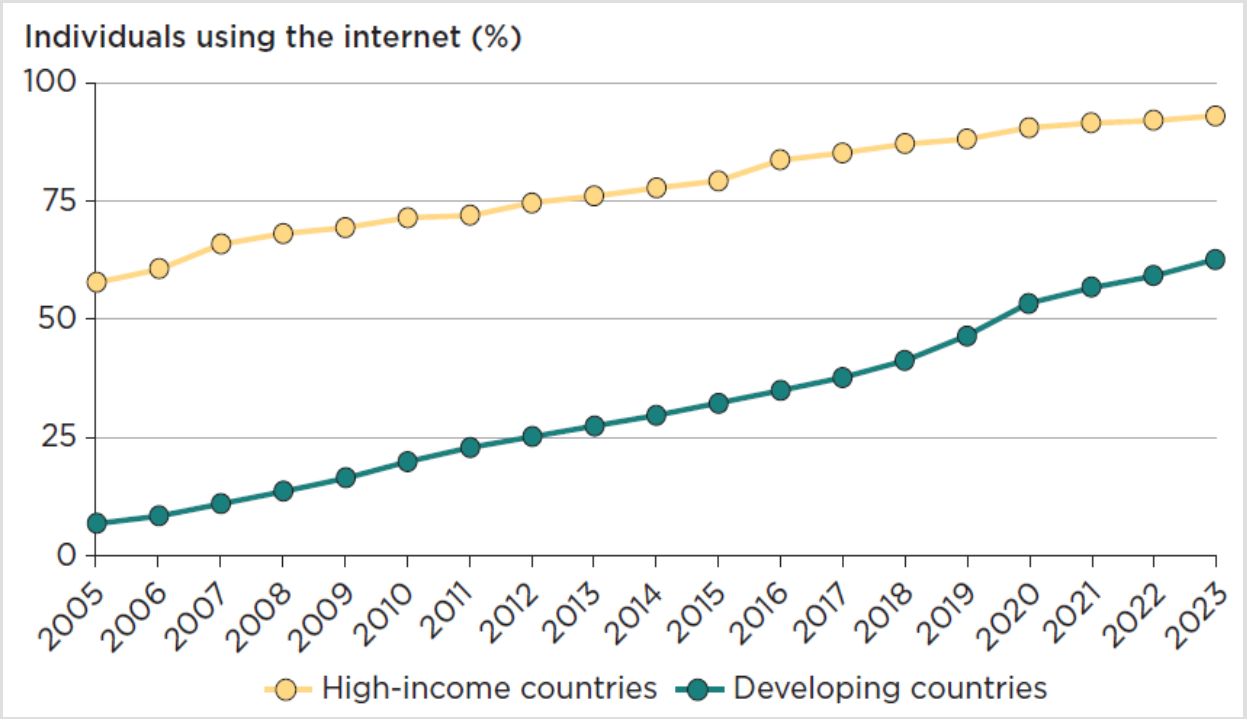
A fundamental aspect of digitization lies in the
ever-expanding cyberattack surface

A more challenging reality for developing countries



A more challenging reality for developing countries

Developing nations have yet to encounter the full extent of cyber threats



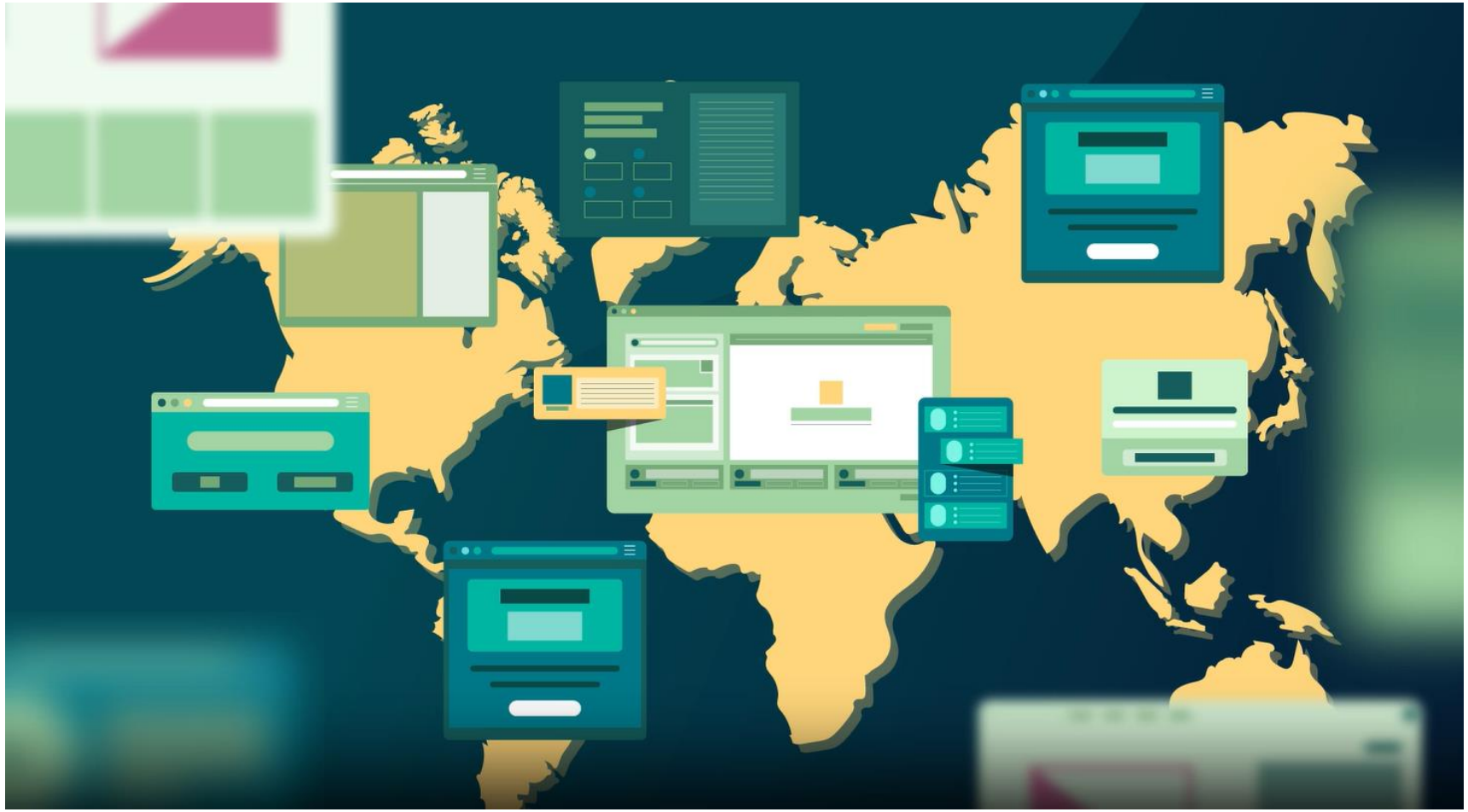
Why is this important?

This work demonstrates for the first time that reducing cyber incidents & investing in cybersecurity can

- Drive economic growth in developing nations
- Safeguard services critical to the protection of human rights

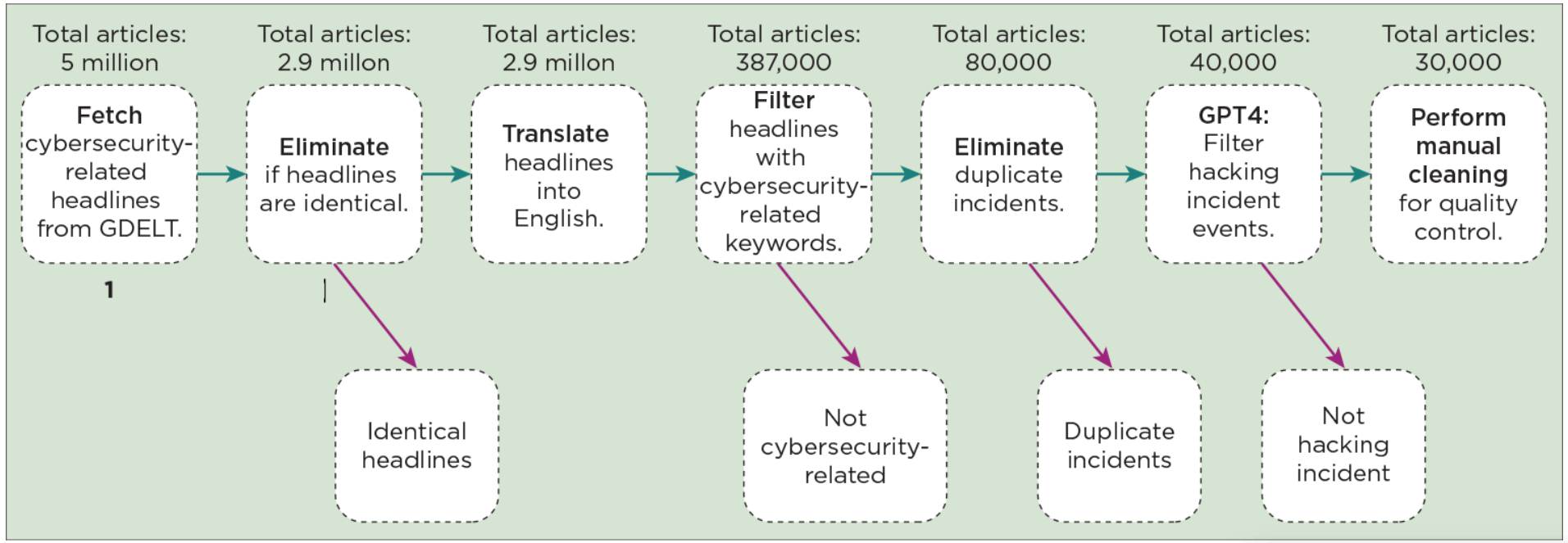
Overcoming the challenge of the lack of data

The World Bank Media-Disclosed Cyber Events (MDCE) database



Overcoming the challenge of the lack of data

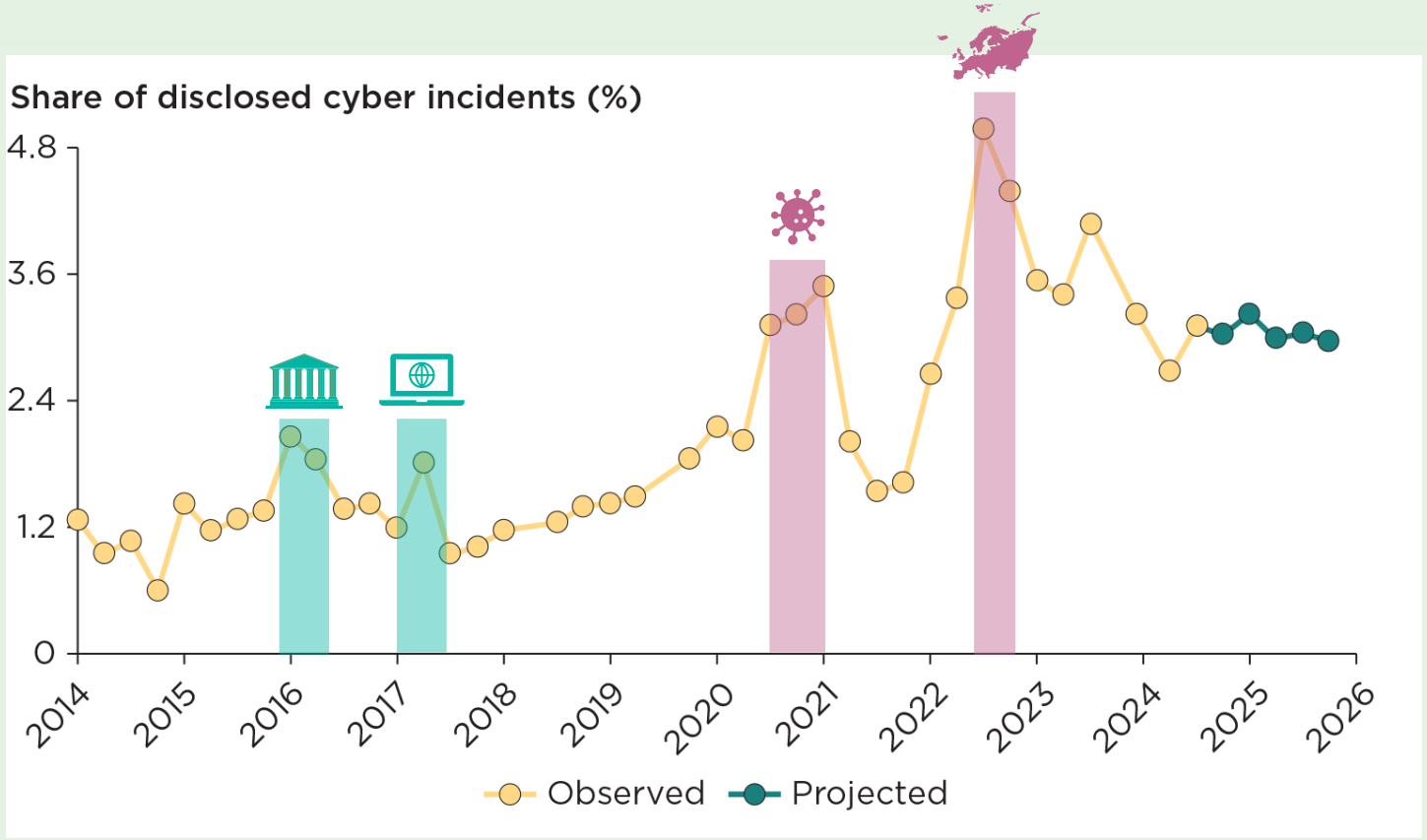
The World Bank Media-Disclosed Cyber Events (MDCE) database



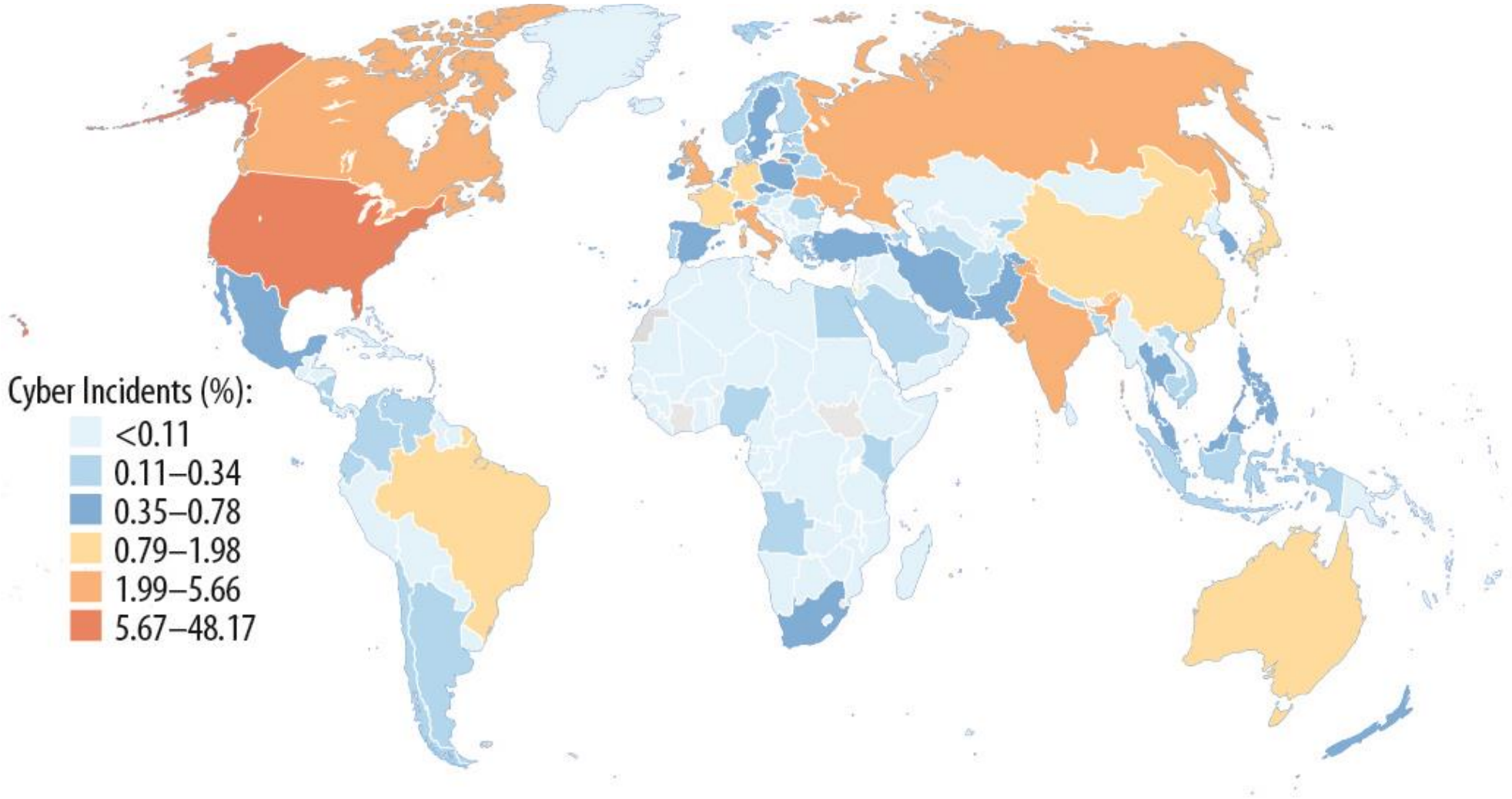
Classifying Cyber Events: A Proposed Taxonomy

By Charles Harry, PhD, and Nancy Gallagher, PhD

Disclosed cyber incidents worldwide grew at an average annual rate of 21% in the last decade



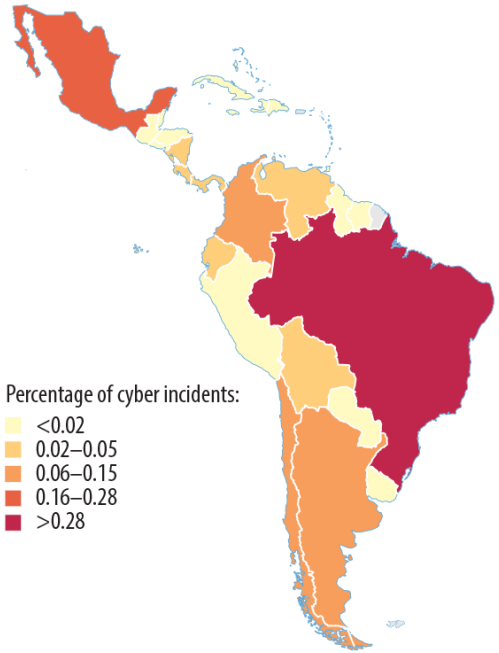
Developing countries present approximately 30% of disclosed cyber incidents



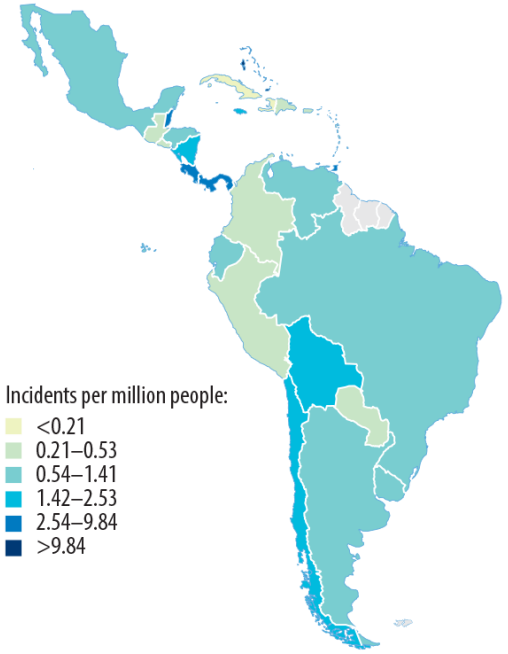
LAC: the world's region with the fastest growth of disclosed cyber incidents

LAC presents the fastest growth of disclosed cyber incidents, at an average annual growth rate of 25%

Share of the region's disclosed cyber incidents



Number of disclosed cyber incidents per million people



The ever-expanding cyberattack surface

145% increase in internet of things devices

280% rise in e-commerce volume

Greater adoption of e-government tools

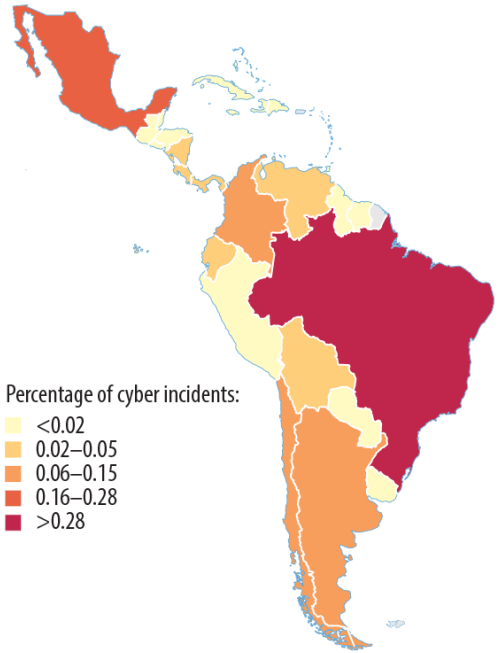
6m developers writing code at every moment, almost none from scratch

WORLD BANK GROUP

LAC: the world's region with lowest scores in cybersecurity commitments

LAC presents the fastest growth of disclosed cyber incidents, at an average annual growth rate of 25%

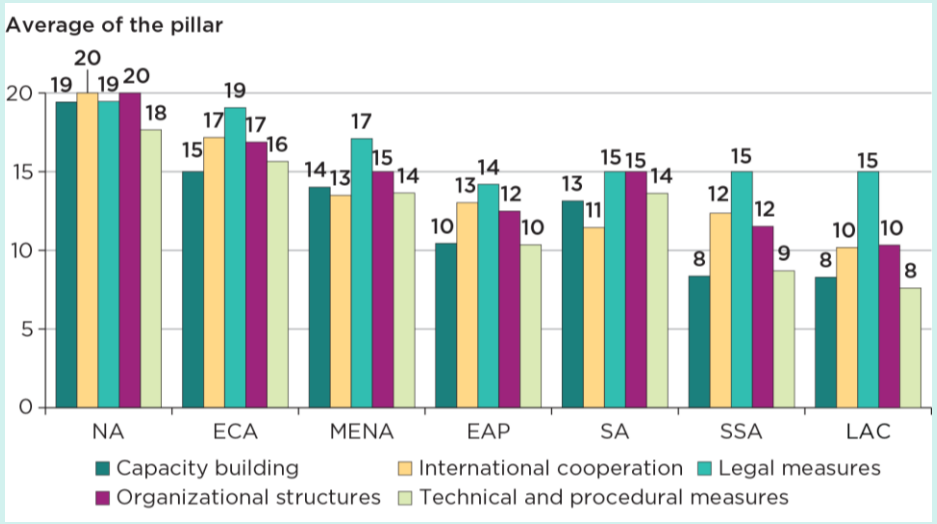
Share of the region's disclosed cyber incidents



Number of disclosed cyber incidents per million people

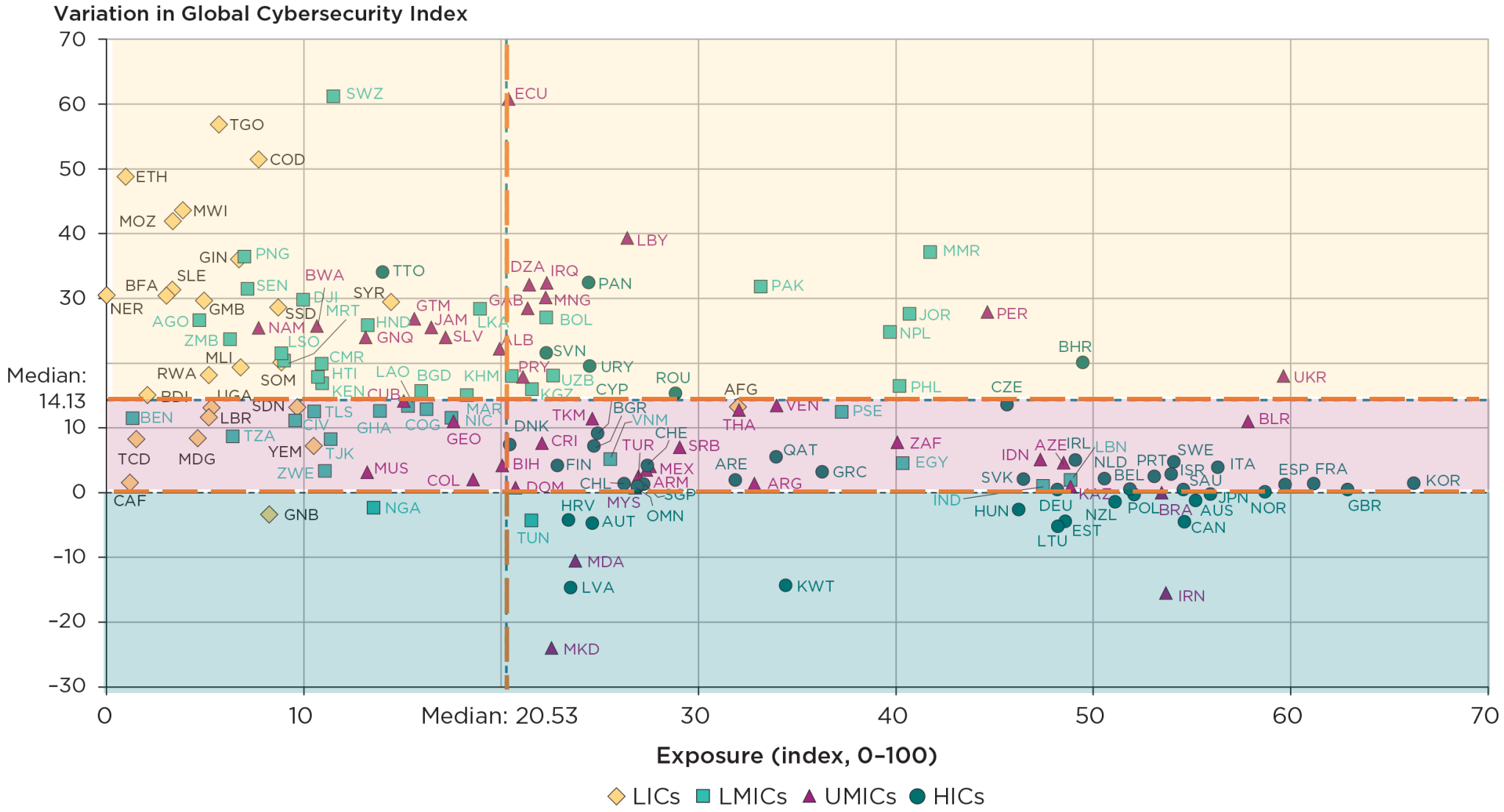
The ever-expanding cyberattack surface

Commitments Gaps

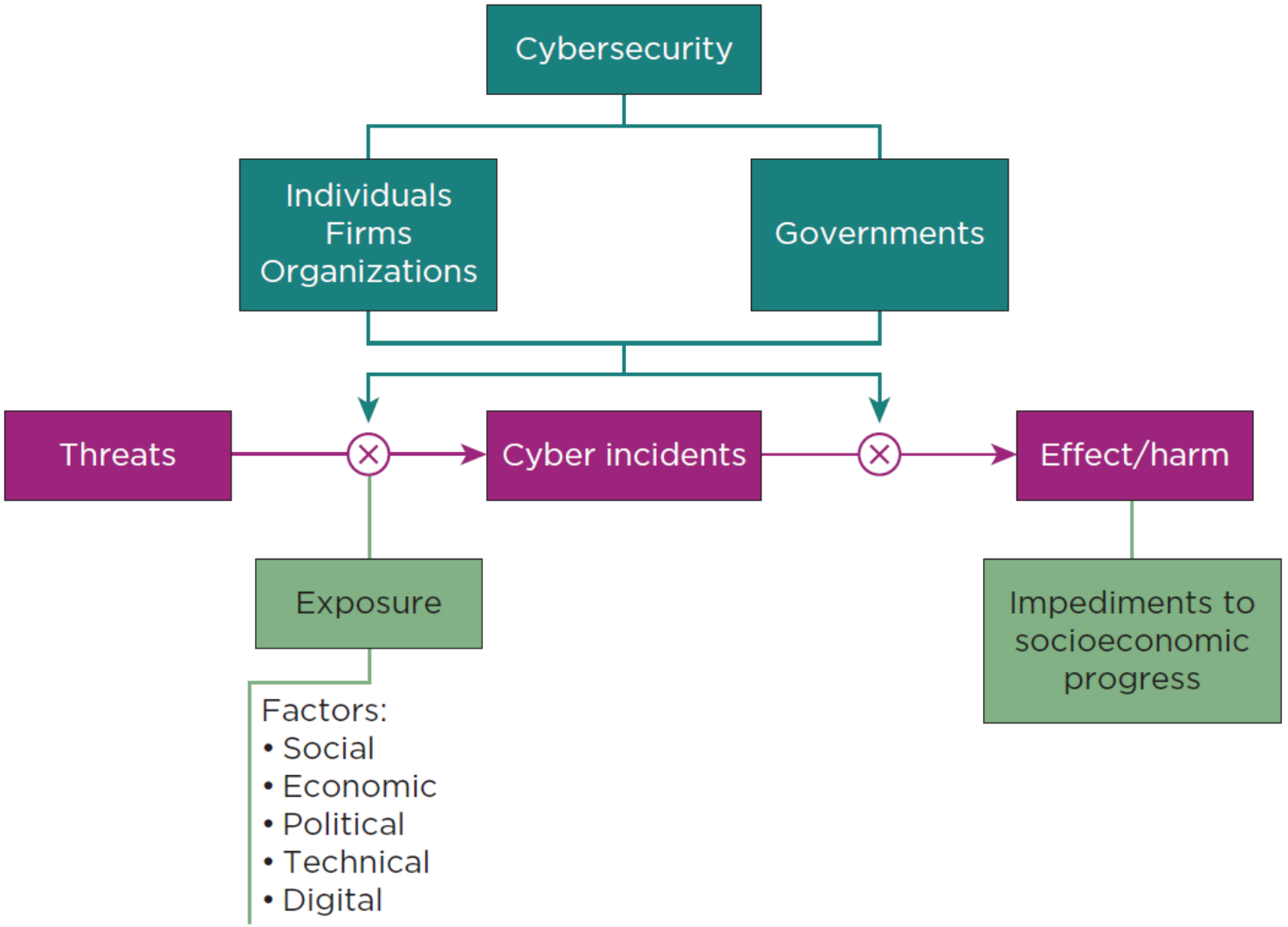


WORLD BANK GROUP

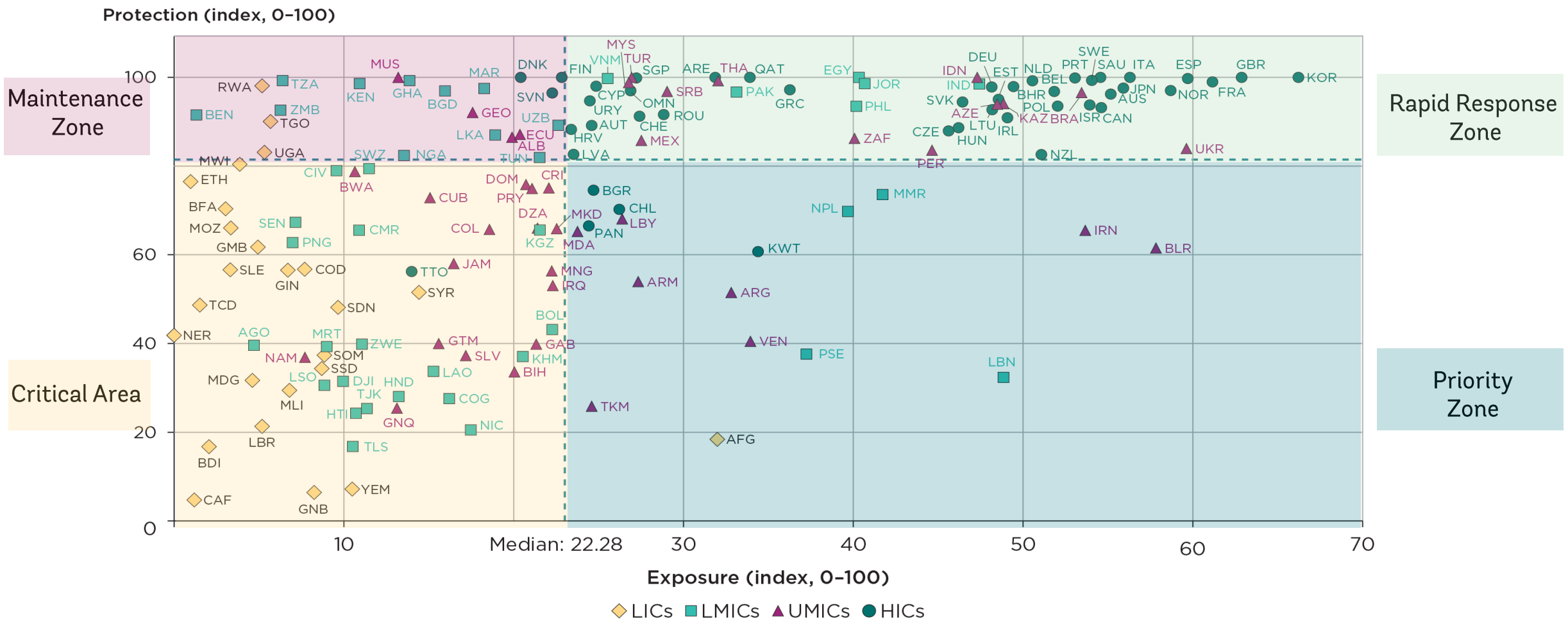
LICs are making remarkable advances in the limitless cybersecurity path (2020-24)



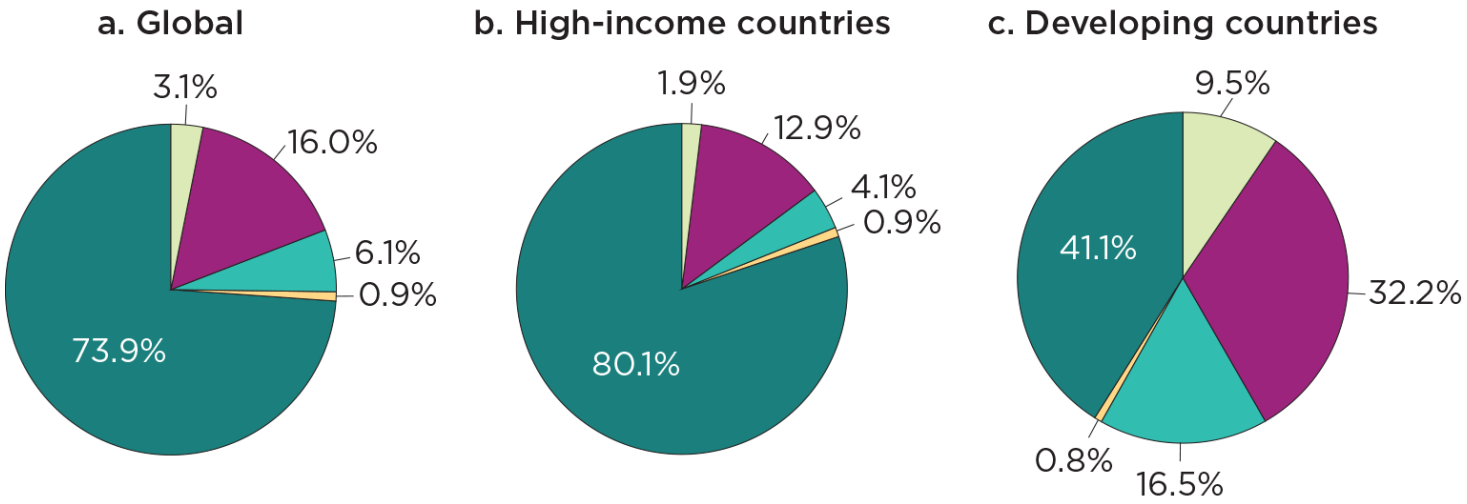
The Cybersecurity Economics Framework

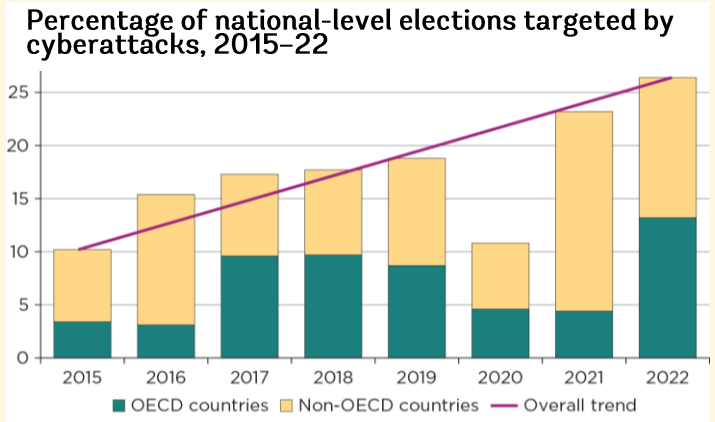


The risk assessment scenario in 2024

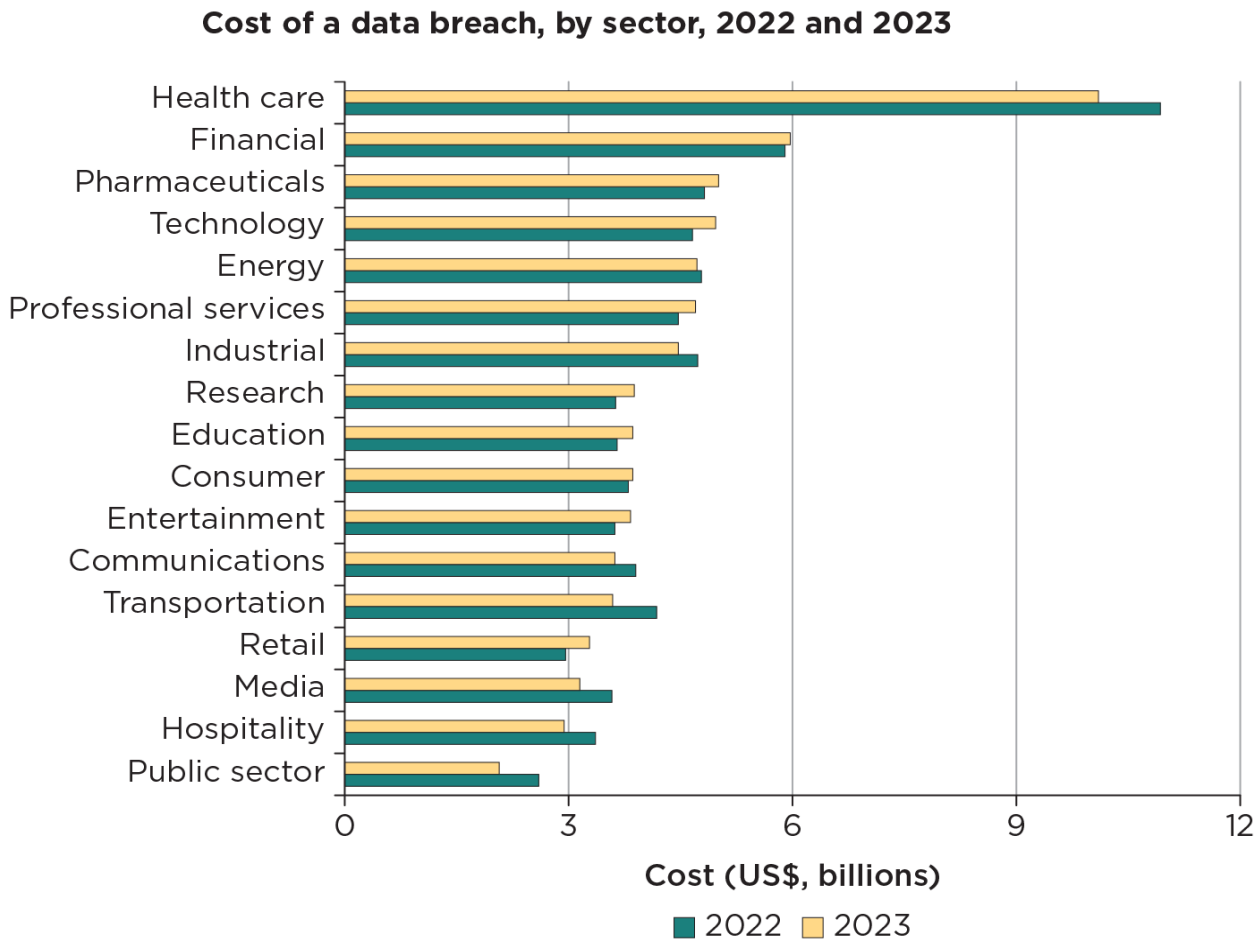


Diverse threat landscapes demand diverse approaches



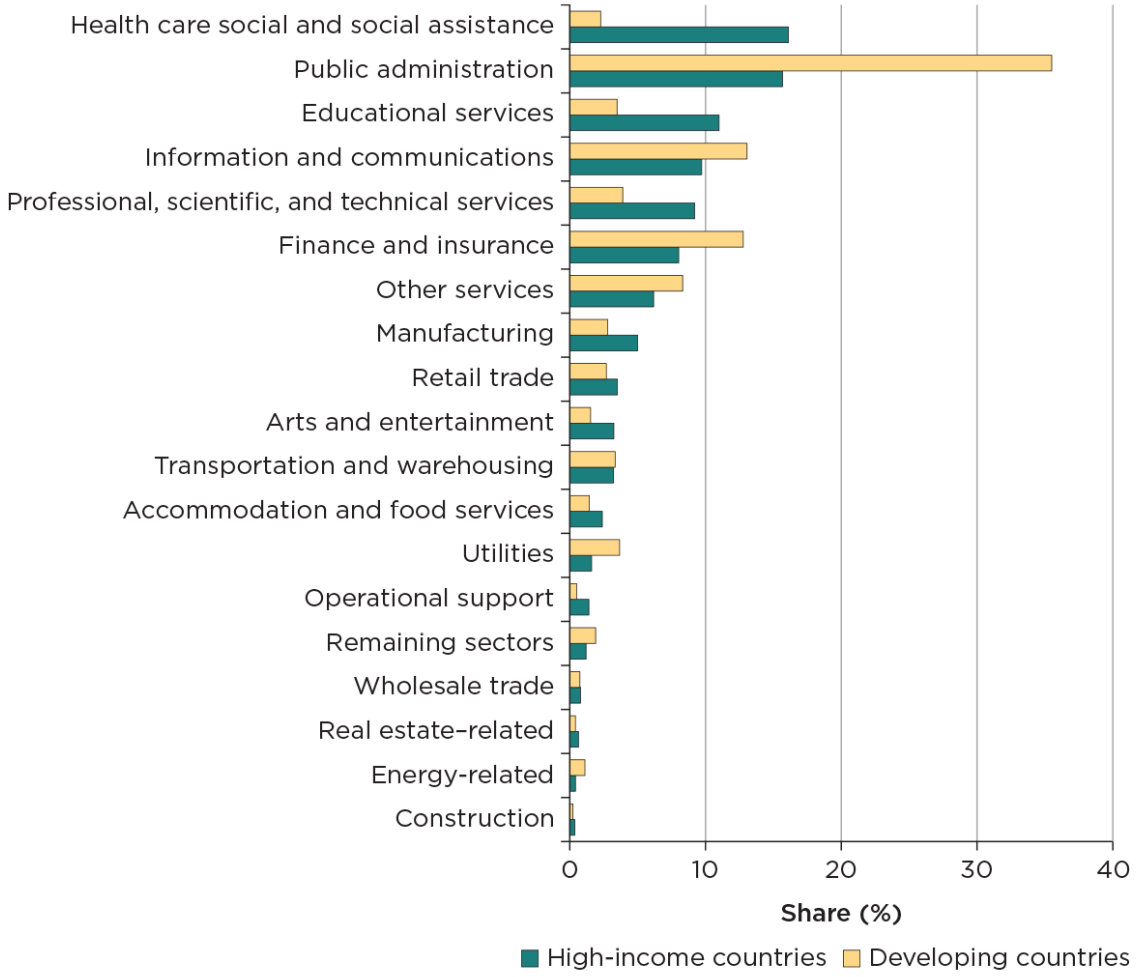


The sectoral landscape of disclose cyber incidents



The sectoral landscape of disclosed cyber incidents

Distribution of cyber incidents by income group



Different reporting rules and/or cybersecurity challenges?

Finance: Focus on the two best practices working well in HICs.

- A market approach: that fosters a competitive national cybersecurity market for cybersecurity products and services tailored to the needs of local institutions.
  - Support startups.
- A regulatory approach: that establishes robust regulatory bodies that continuously monitor safety and stability.
  - Remain vigilant against potential "cyber runs."

Health care: The landscape in HICs serves as a warning for the digitalizing health sector in developing countries.

- Recognize this sector as highly attractive to malicious actors.
- Establish strong regulatory agencies with the authority to oversee and monitor activities.
- Ensure that data protection laws of highly-confidential data are current and effective.

Public Administration: A continuous priority for all countries.

- Continuously implement preventative measures.
- Promote cyber audits and initiatives to detect ongoing threats.
- Prioritize resilience efforts during periods of heightened political activity.
- Ensure citizens' data is effectively protected against emerging threats.

Utilities, Energy, Transport, ICT:

- Recognize cybersecurity in these sectors as essential for safeguarding services closely linked to human rights protection.
- Focus on designing resilient digital infrastructure, particularly in countries with high geopolitical risk.
- Collaborate closely with the private sector and the international community to ensure robust protection of shared systems.

But how do we prove it?

Cybersecurity isn't just about protection—it's a game-changer for economic growth in developing nations

A cross-country cross-industry model

$$ValueAdded_{ij} = \alpha_i + \theta_j + \beta GCI_i * Vulnerability_j + controls_{ij,2014} + v_{ij}$$

Exposure to cyber incidents in j

Compound growth rate of j in i between 2014 and 2021

Cyber commitment score in i, 2014

A Non-Negotiable Must-Have

Given countries' initial levels of cybersecurity commitments (CC):

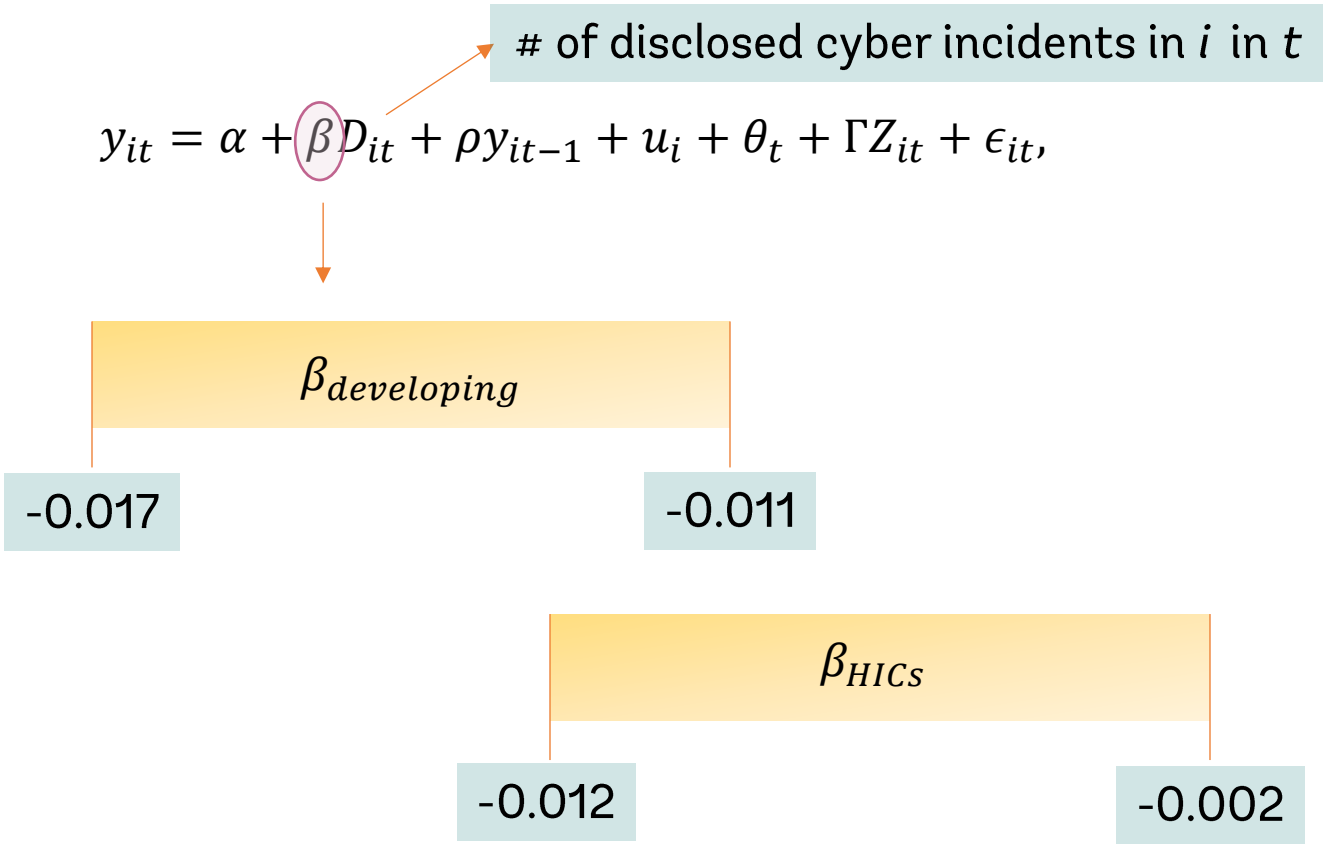
The residual growth rates of industries that are more exposed to cyber incidents is negative in countries with low CC scores, and positive in countries with high CC.

Sector	Countries with below-median GCI scores (growth rate, %)	Countries with above-median GCI scores (growth rate, %)
Industries most often subject to cyberattacks		
Wholesale, retail trade, restaurants, and hotels (ISIC G–H)	−0.04059	0.03146
Mining, quarrying, and utilities (ISIC C–E)	−0.30133	0.25937
Transport, storage, and communication (ISIC I)	−0.70363	0.58349
Manufacturing (ISIC D)	−0.85575	0.71493
Industries least often subject to cyberattacks		
Construction (ISIC F)	0.45236	−0.39914
Agriculture, hunting, forestry, and fishing (ISIC A–B)	1.41115	−1.35395

Source: Vergara Cobos et al., forthcoming.

Cybersecurity isn't just about protection—it's a game-changer for economic growth in developing nations

Dynamic panel-data estimation, GMM



The economic impact of cyber incidents is likely higher in developing countries

Cybersecurity isn't just about protection—it's a game-changer for economic growth in developing nations

A developing country that reduces its major disclosed cyber incidents from the top quartile of the distribution (around 50 incidents) to the bottom quartile (around 7 disclosed cyber incidents) in a decade could see an increase in GDP per capita of approximately 1.5%

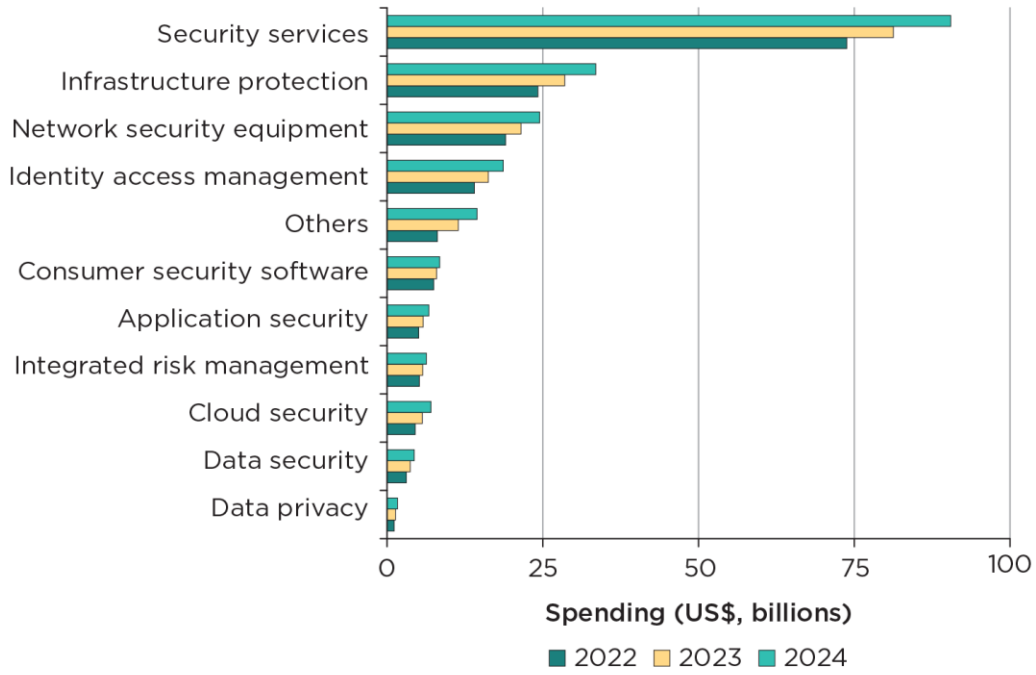
Distribution of disclosed cyber incidents in emerging economies

Finding market solutions

A market filled with challenges

- Global spending on information security and risk management accounts for 0.2% of the world's GDP.
- This market is projected to surge by over 14% in 2024
- Rapid growth is anticipated to continue in: cloud security, data privacy, and data security sectors.
- Spending on professional security services will remain dominant: 40% of the global market.
- **Despite the growth, the cybersecurity industry is constrained by:**
  - **inadequate investment in R&D**
  - **low public cybersecurity**
  - **Large gap of highly-skilled cybersecurity professionals**

Global security and risk management end user spending for all segments, 2022–24



Finding market solutions

A market largely influence by HICs on market dynamics through

- Substantial procurements,
- Customized standards and certifications, and
- Investments in R&D

Filled with sources of market failures

- Low cybersecurity awareness
- The risk of vendors: at least 90% of organizations worldwide maintain business ties with third-party vendors that have recently experienced a cyber incident.
    - The highest vendor risk: information and communications and health care sectors (+20 vendors)
    - The lowest vendor risk: finance (~6 vendors)

Almost 60% of victim firms translate losses from cyber incidents into price hikes

Lessons learned and recommendations

Strengthen national cybersecurity industries

Investing in public cybersecurity awareness:

- Drive demand for cybersecurity products and services
- Reduce sources of market failures

Encouraging startups

Supporting the development of a highly skilled cybersecurity workforce

Lessons learned and recommendations

Create incentives to invest in cybersecurity

Rethink how to assess cybersecurity ROI: cybersecurity is still driven by a cost-saving rationale.

- What is the price of our data? Our privacy? Essential services?

Recognize cybersecurity as a growth driver and continue gathering scientific evidence to move beyond anecdotal cases

- Standardized and safe collection of data
- Shared terminology

National cybersecurity R&D strategic planning

Lessons learned and recommendations

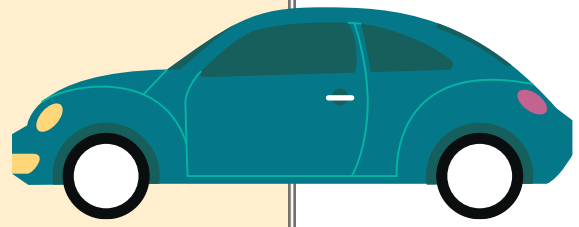
Monitor and act proactively
Track both short- and long-term indirect losses from cyber incidents
Focus on emerging technologies such as advanced artificial intelligence and cloud computing • Dynamic and up-to-date regulatory frameworks
Acknowledge that higher geopolitical risks require more resilient digital infrastructure

Lessons learned and policy recommendations

Prioritize the most vulnerable cyber-personas and critical sectors

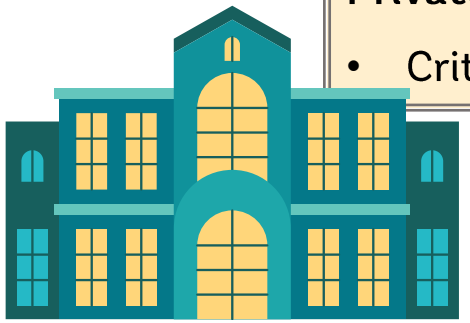
Support for SMEs

Encourage cyber audits in highly targeted & critical sectors



Private-public collaboration on risk management efforts

- Critical sectors providing essential services



Lessons learned and policy recommendations

Dynamic, adaptable, tailored, and evidence-based policy making

Advocating for and supporting tailored research on the economics of cybersecurity

Efficient cybersecurity is essential for the socioeconomic progress of nations

Thank You!

ありがとう

Download book here!