



CYBERSECURITY
Digital Development

Digital Safeguards Business Line

Progress Update




February 8, 2024

Agenda



CYBERSECURITY
Digital Development

- 
- **FY24 Highlights**
 - **Portfolio Stocktake**
 - **FY24/25 Priorities**
 - **Challenges**
 - **Discussion and Guidance**



CYBERSECURITY
Digital Development

Raising the Bar on Cybersecurity

The World Bank Journey

Capacity Development and Consultation Workshop on a Samoa National Data Governance Framework

May 8-9, 2024

Hagai Mei-Zahav
Senior Cybersecurity Specialist



WORLD BANK GROUP

Agenda

**Cybersecurity and Data
Governance**

**The Global Cybersecurity
Landscape**

**World Bank
Cybersecurity Activities**

**Building Knowledge and
Tools**

**להקליל
לספק נתונים על אסיה
לסיים**





Cybersecurity and Data Governance



Data Security and Data Protection as a Core Element of Data Governance

Cybersecurity: measures and controls to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of computers, and communications systems, **including information contained therein.**

[NIST Glossary]

The six elements of data governance

1 Data Standards and Standardization

2 Data Sharing Exchange and Interoperability

3 Data Security and Protection

4 Data Privacy and Ethics

5 Data Infrastructure

6 Digital Identity

The planning, development, and execution of **security policies and procedures** to provide proper authentication, authorization, access, and auditing of data and information assets.

Procuring, storing, managing, interpreting, analysing, and disposing of data with **careful attention to the protection of individual and business entities's data privacy** and in line with ethical principles.



Data Security and Data Protection as a Core Element of Data Governance

Why does **Cybersecurity** matter in the context of **Data Governance**, and why does **Data Governance** matter in the context of **Cybersecurity**?

Cybersecurity

Safeguarding the country's IT infrastructures, systems, networks, dBs, etc.

Ensuring the availability, integrity, and confidentiality of Protecting data in rest and in transit.

Data Governance

Applying standards, policies, and regulations on data security and the security of the applicable IT assets increases awareness, streamlines implementation, and fosters a high level of compliance.

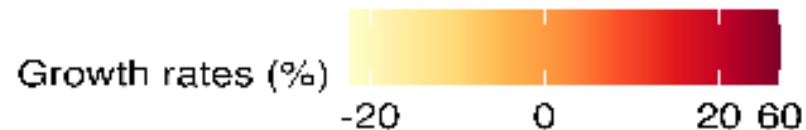
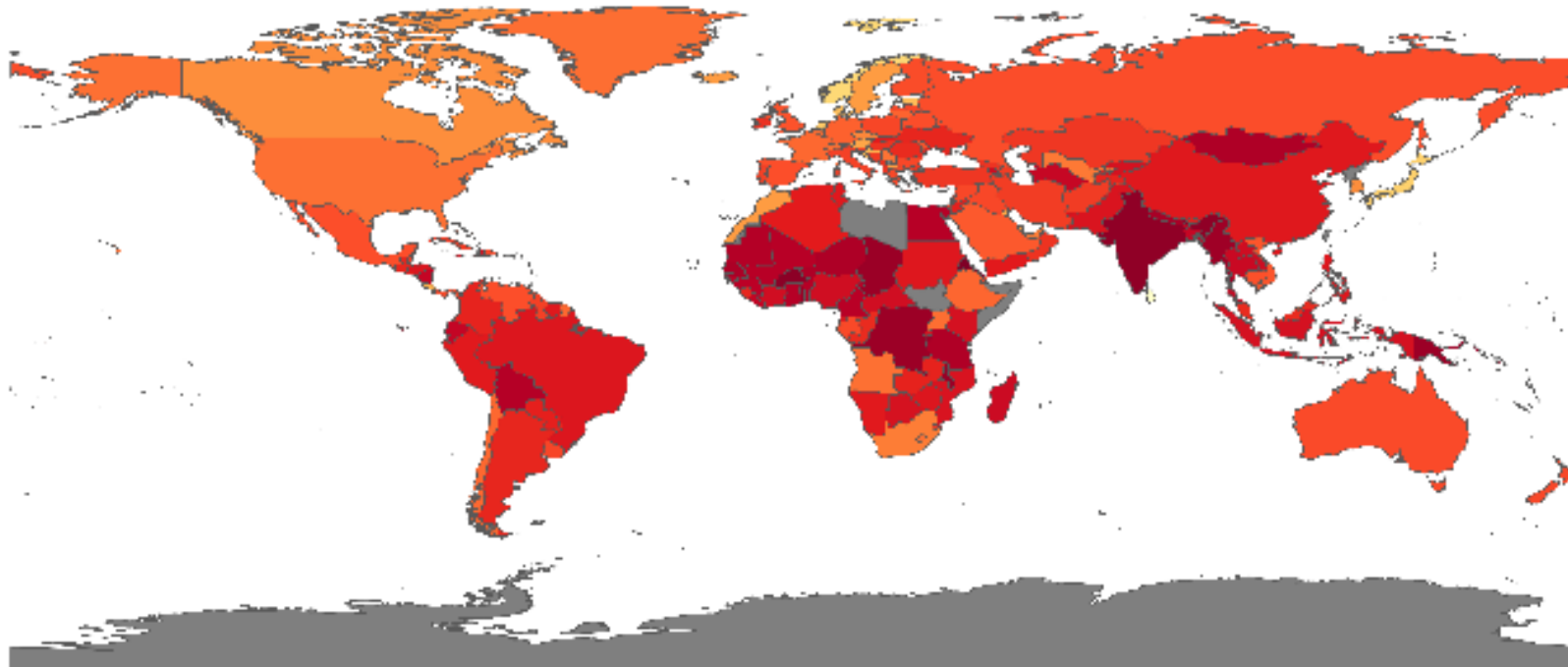


The Global Cybersecurity Landscape

Cybersecurity Landscape Overview

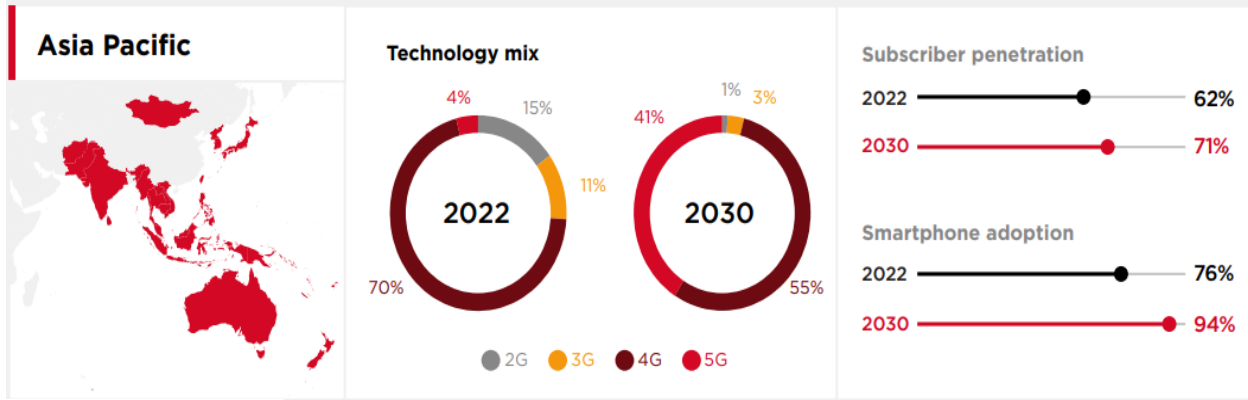
With the **rapid digitalization of developing countries**, the growing penetration of digital technologies, and the digitization of services, **the use of cyberspace grows, and the attack surface expands**, creating new vulnerabilities and reshaping the global threat landscape

Growth rates of internet users by country (2019-2021)

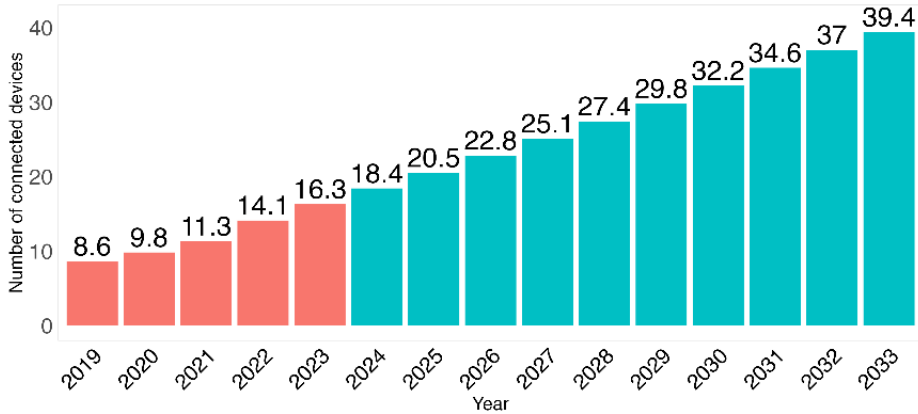


Cybersecurity Landscape Overview

The expansion of the attack surface: more people are using the internet more time.



Source: GSMA 2023

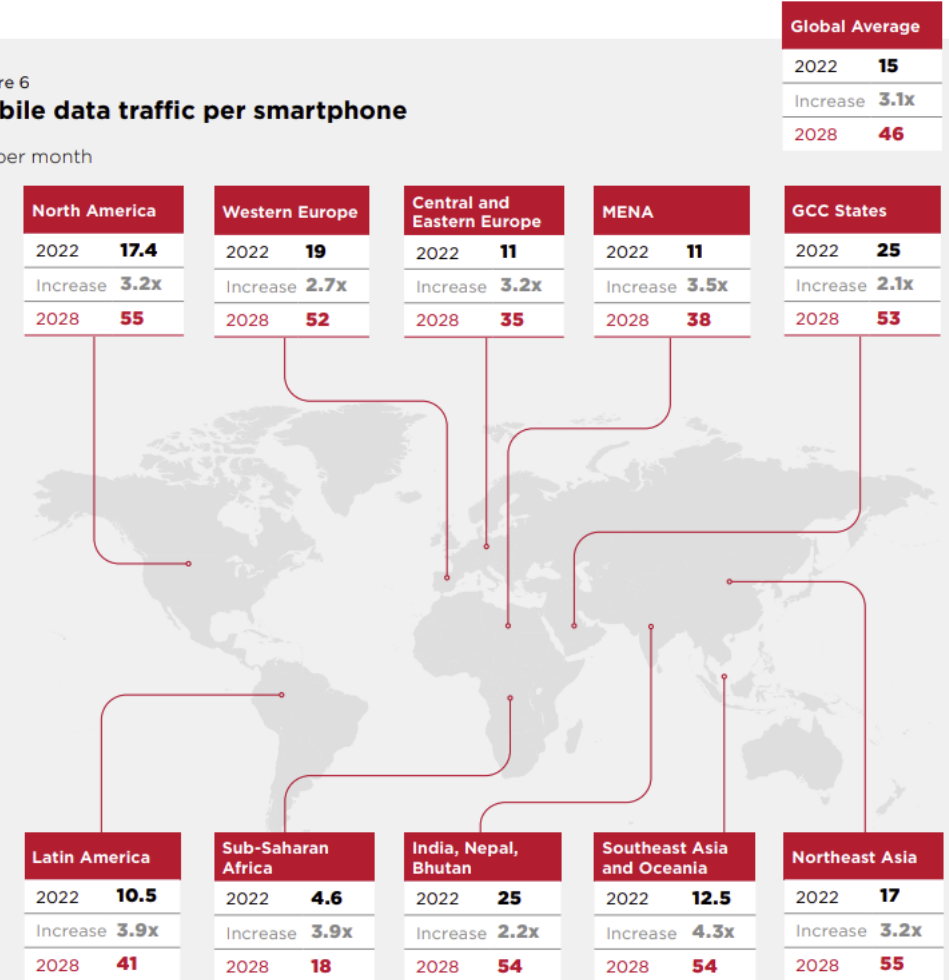


Source: WB

Observed Projected

Figure 6
Mobile data traffic per smartphone

GB per month



Source: GSMA 2023



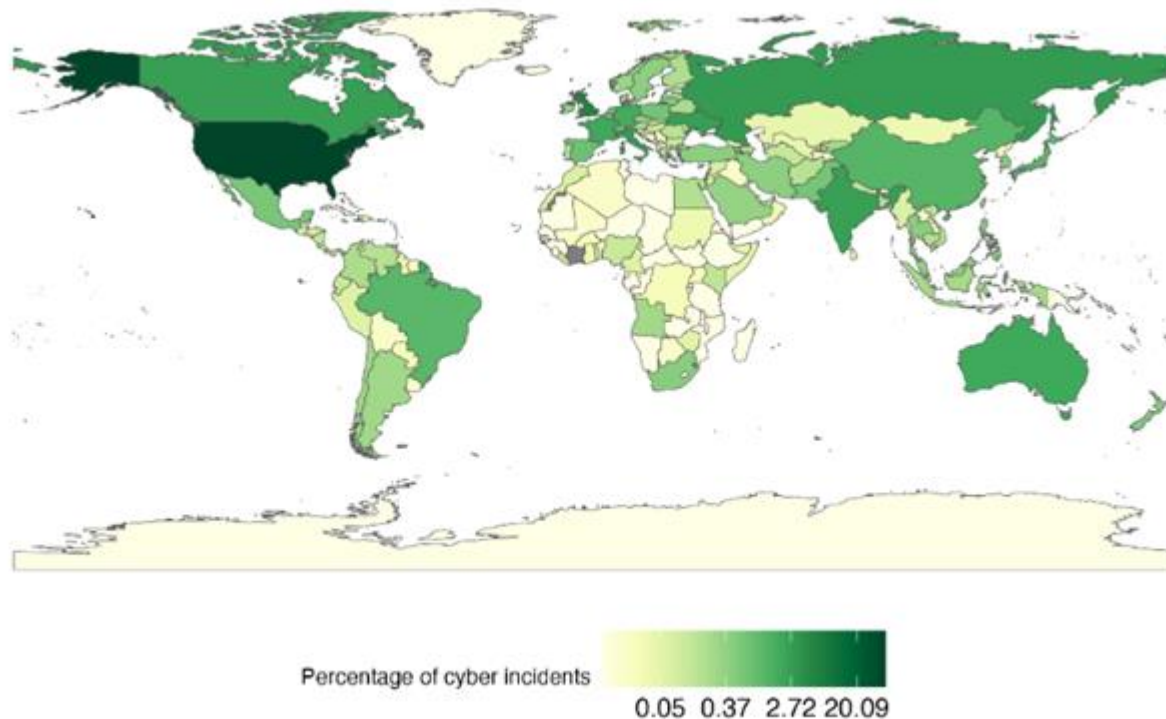


Developing countries are increasingly exposed to cybersecurity risks

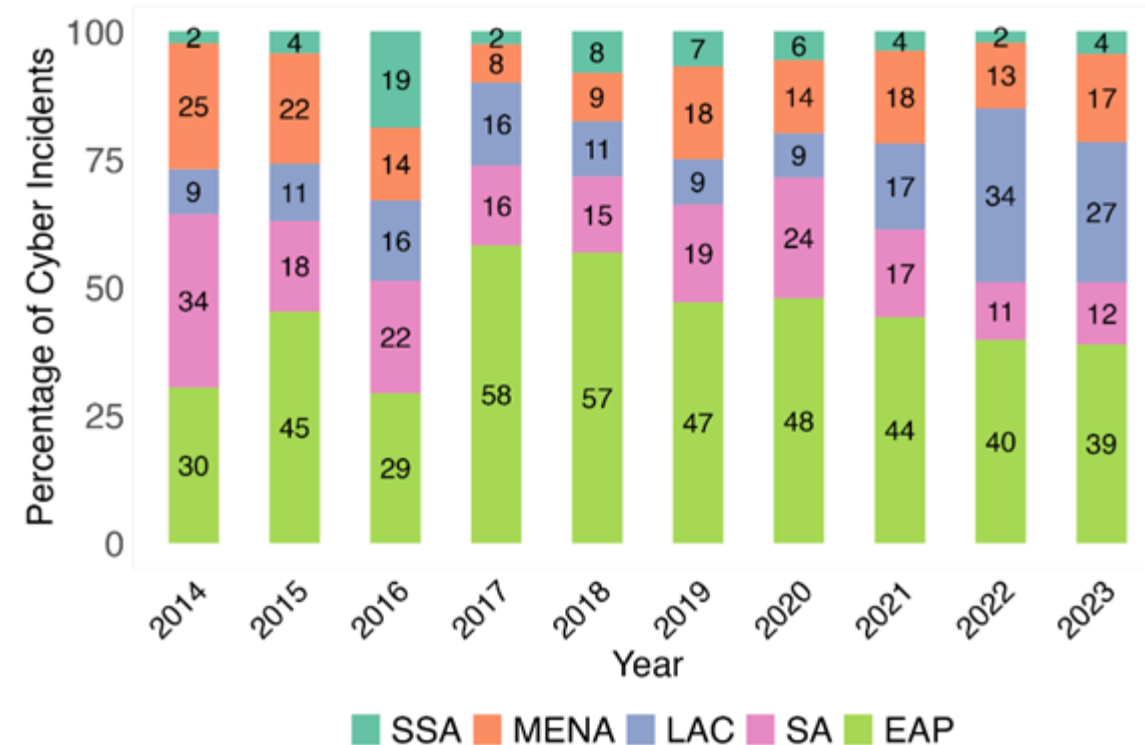
As a result, the number and intensity of cyber incidents increase worldwide, countries with rapid digital infrastructure growth rate are more vulnerable. **The distribution of cyber incidents is complex, being influenced by a variety of interconnected factors**, such as economic performance, political stability, cyber capacity, and geopolitical tensions.

Asia-Pacific is the most targeted region amongst developing regions

Map of cyber incidents distribution in the last decade



Distribution of cyber incidents by developing regions



Source: The cyber incidents estimates presented above are based on two databases built scraping data from publicly available information on disclosed cyber incidents: 1) the cyber incidents database collected by the Center of International and Security Studies (CISS) at the University of Maryland, and 2) the Media-Disclosed Cyber Incidents database built internally by scraping data from news articles in over 98 languages.



The Economic Impact of Cybersecurity; Preliminary Findings - Report to be published in July 2024

Studying the economic effects of cyber incidents revealed that cyber incidents are statistically significantly associated with losses in GDP per capita in non-HICs – with an average disclosed incident in non-HICs being correlated with a decrease between USD 2.4 and USD 2.7 in GDP per capita

Countries with higher cyber-protection levels (based on cyber commitment, measured by ITU's GCI score):

- Seeing lower and more stable growth rate of cyber incidents
- Grow faster in cyber-vulnerable industries

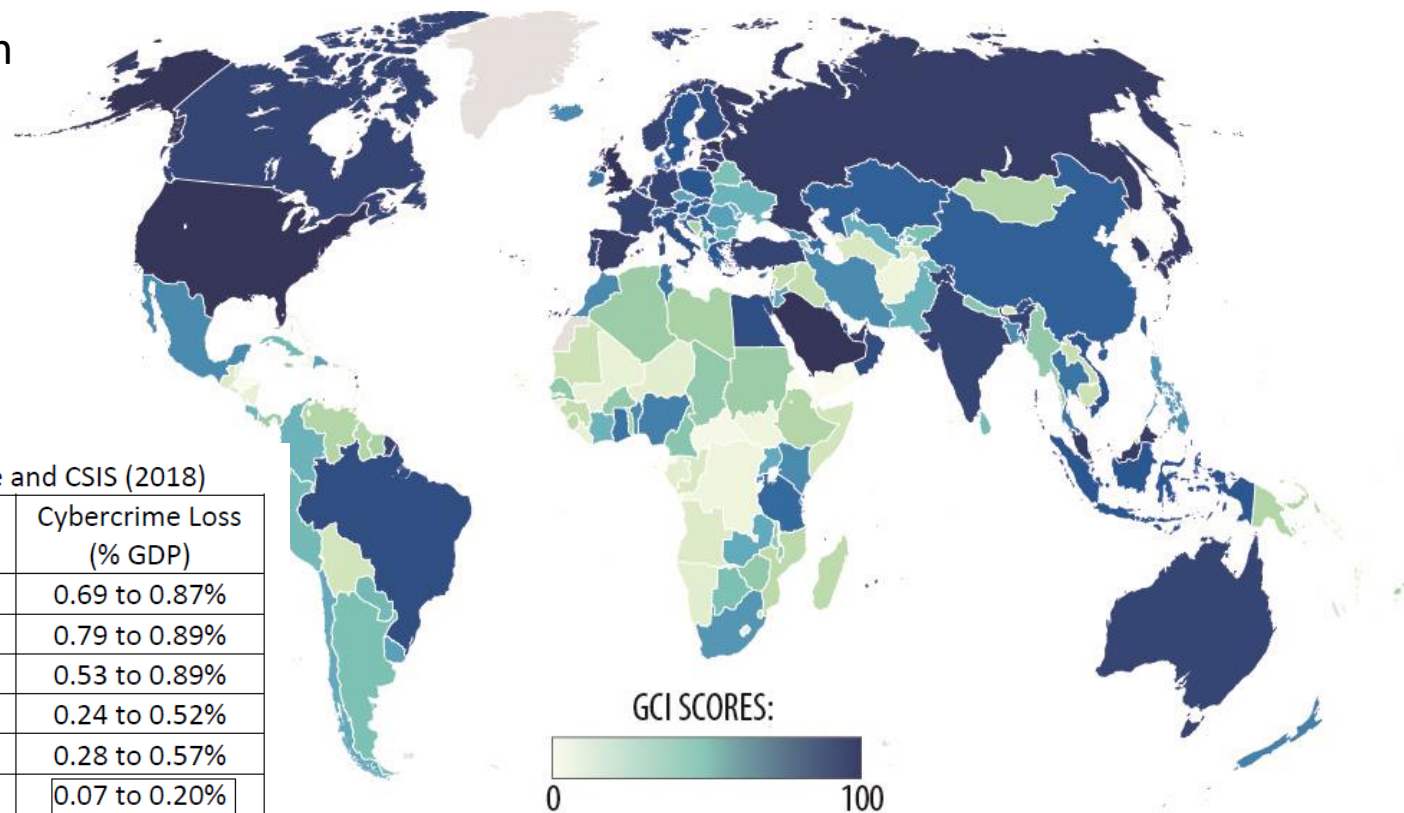
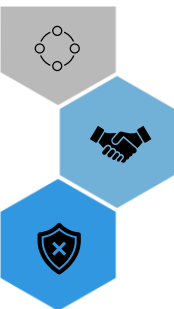


Table 5: Regional Distribution of Cybercrime Costs in 2017 according to McAfee and CSIS (2018)

Region	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
LAC	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	75.8	445 to 608	0.59 to 0.80%



Cybersecurity Impact is beyond Economic Loss



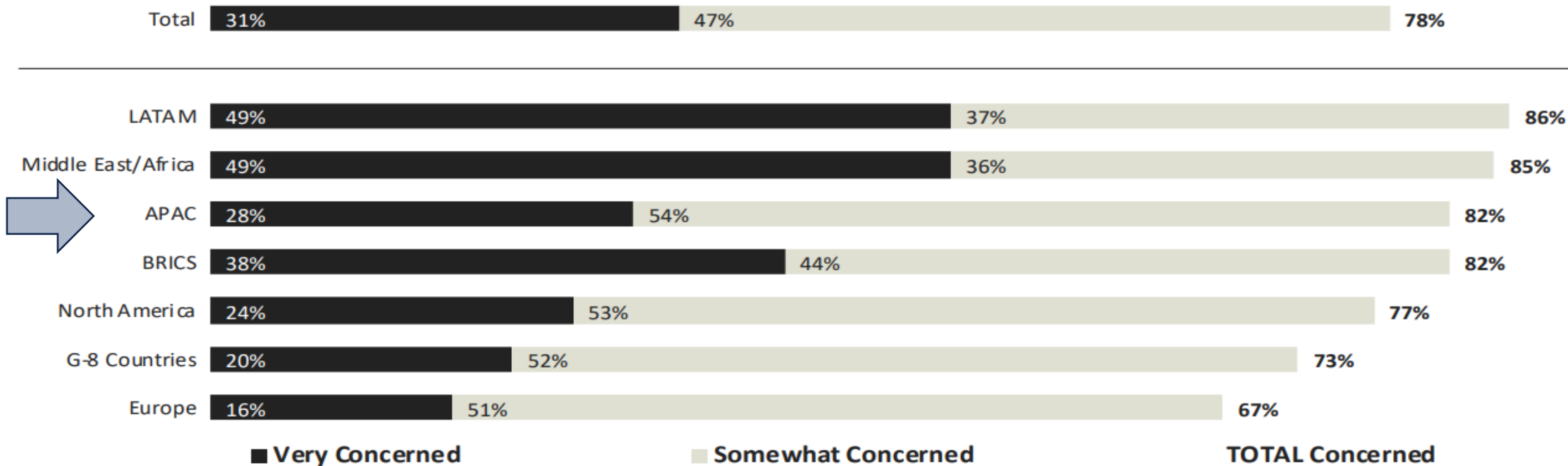
SERVICES Disruption of **critical government services**: financial systems, infrastructure, healthcare

DATA Unauthorized access to **confidential information**: national security, personal data

REPUTATION Loss of **reputation**: reduction in consumer spendings

TRUST undermining citizen trust in digital economy and transformation

Globally, **78 percent** are concerned about their online privacy





Developing countries are increasingly exposed to cybersecurity risks

Cyberattacks are growing in sophistication and intensity. The rapid digitalization of developing countries increases their attack surface, making them even more vulnerable.

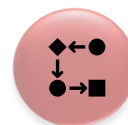
2024 Trends:



Continued Geopolitical instability including the US election, Ukraine, Paris Olympics



A transformative impact of Generative AI on attackers and defenders



Shift from cybersecurity to cyber resilience, ensuring business continuity



Growing sophistication of cyber-attacks, such as Phishing & Ransomware



Evolution of Zero-Trust from technical model to holistic approach

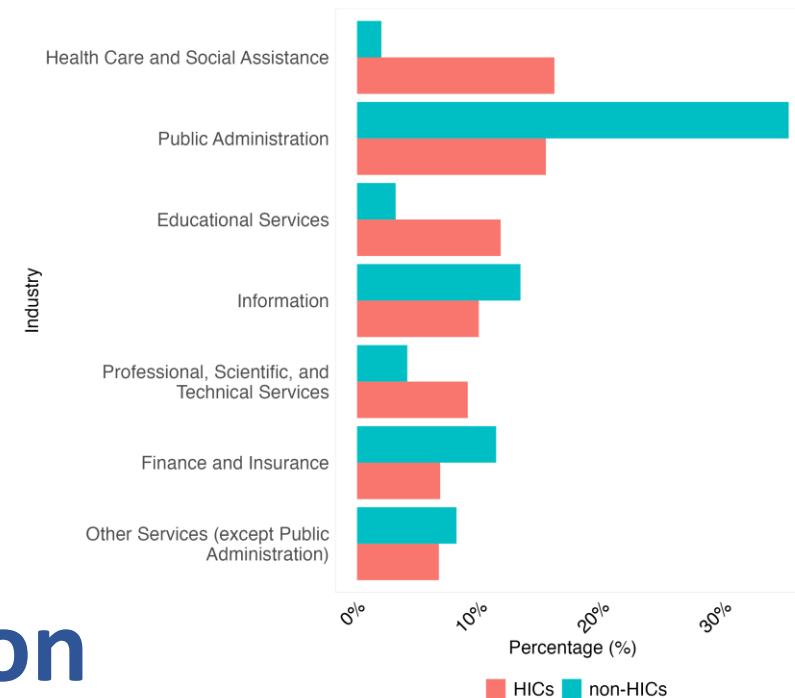


Growing attack surface with the expansion of IOT and cloud-based solutions



Skills shortage intensifies and becomes a critical hurdle for cyber resilience

LMICs are increasingly hit by cyber incidents, across critical sectors:



4 million – 2.6 million

Estimate of unfilled cybersecurity positions globally

Estimate of unfilled cybersecurity positions in Asia-Pacific Region



Cyberattacks are disrupting economic and social development

In 2022-23, many developing countries fell victim to debilitating cyberattacks across public and private sectors, with severe economic and social consequences.



Costa Rica

- **Ransomware attacks shut down IT systems** in over a dozen ministries (including finance, digital and social security).
- **Major disruptions in key public services** (e.g., payrolls for civil servants, pension payments, customs).
- **More than US \$125 million of losses in a few weeks.**
- **State of national emergency declared.**



Albania

- **Cyberattacks shut down e-government services**, including tax payments and civil registries.
- **Undermined the trust of citizens in digital transformation.**
- **Disrupted critical sectors** (e.g., telecommunications operators) and operations of Parliament.



Vanuatu

- **Hackers compromised Vanuatu's government systems**, knocking offline, government services for over a week
- Data bases of the **parliament, police, Prime Minister's office, schools, and hospitals were taken down**
- **Anyone with gov.vu was affected**



Philippines

- **Ransomware attack on the national health provider (PhilHealth)**, compromised sensitive data of up to 20 million members
- The attackers, demanded \$300,000 as a ransom, prompt the temporary shutdown of PhilHealth online systems and services
- In a different incident the 1.2 million police records (mainly administrative) were leaked

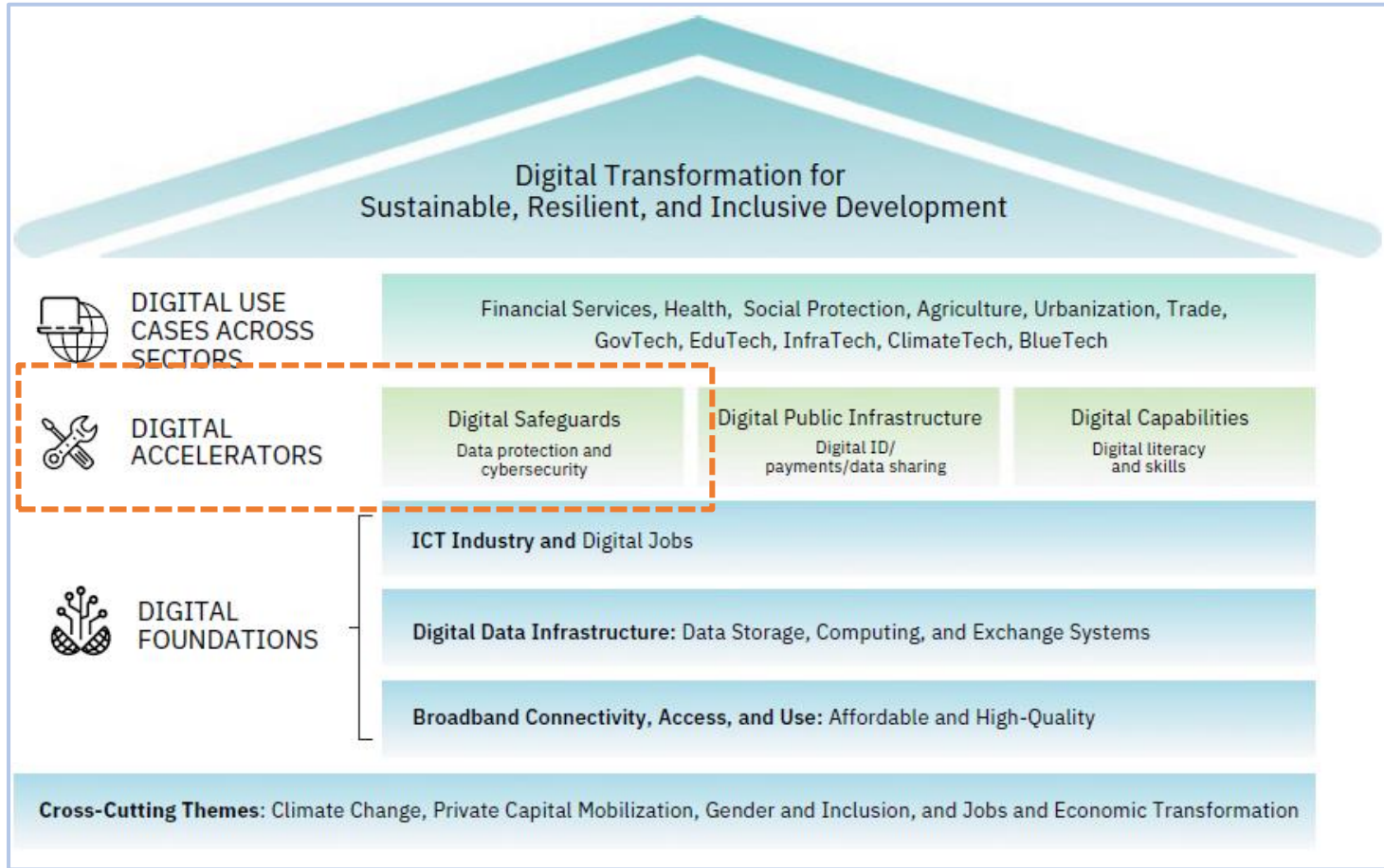
A photograph of two people working at a desk. In the foreground, a person's hands are typing on a white laptop keyboard. In the background, a woman wearing a black hijab and a striped shirt is looking at a smartphone. To the left, there is a white pot containing a green plant. The scene is lit with soft, natural light from a window in the background.

World Bank Cybersecurity Activities

The World Bank Support on Cybersecurity

The World Bank aim is to maximize the benefits of digitalization for all, while mitigating the risks. Digital Development can be fully established and further accelerated only if digital safeguards, i.e. cybersecurity and data protection, are in place.

World Bank Framework for Digital Development



The World Bank instruments to support cybersecurity

- Financing
- Advisory Services
- Knowledge and Tools
- Convening Services



Country support for cybersecurity is growing in line with governments demand

From 2012 to 2023, **68** Digital Development Projects have included dedicated cyber capacity building activities covering a total of **56** countries with a total lending amount of over **\$200 Million**.

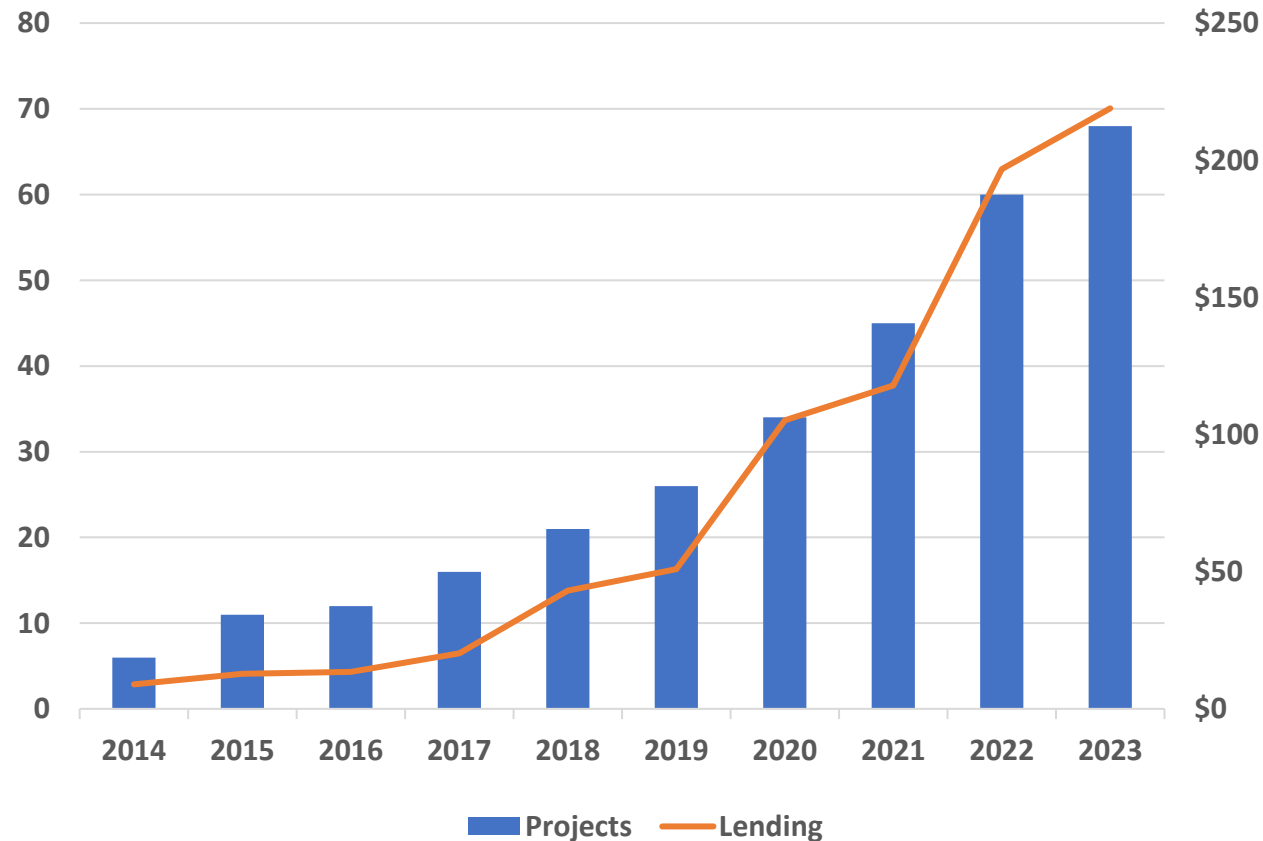
Financing

Advisory Services

Knowledge and Tools

Convening Services

Cybersecurity Operational Lending Portfolio



By Region:

Africa East and West - 53%

South Asia - 19%

Latin America - 17%

Asia Pacific - 10%

Middle East - 1%



Country support for cybersecurity is growing in line with governments demand

From 2012 to 2023, **68** Digital Development Projects have included dedicated cyber capacity building activities covering a total of **56 countries** with a total lending amount of over **\$200 Million**.

Financing

Advisory Services

Knowledge and
Tools

Convening Services

EAP Regional Portfolio

\$20+ million investment in cybersecurity, so far

9 active lending projects **2** project in preparation

Micronesia - 2 projects

Tonga

Tuvalu

Kiribati – 2 projects

Marshall Islands

Indonesia

Mongolia

Philippines

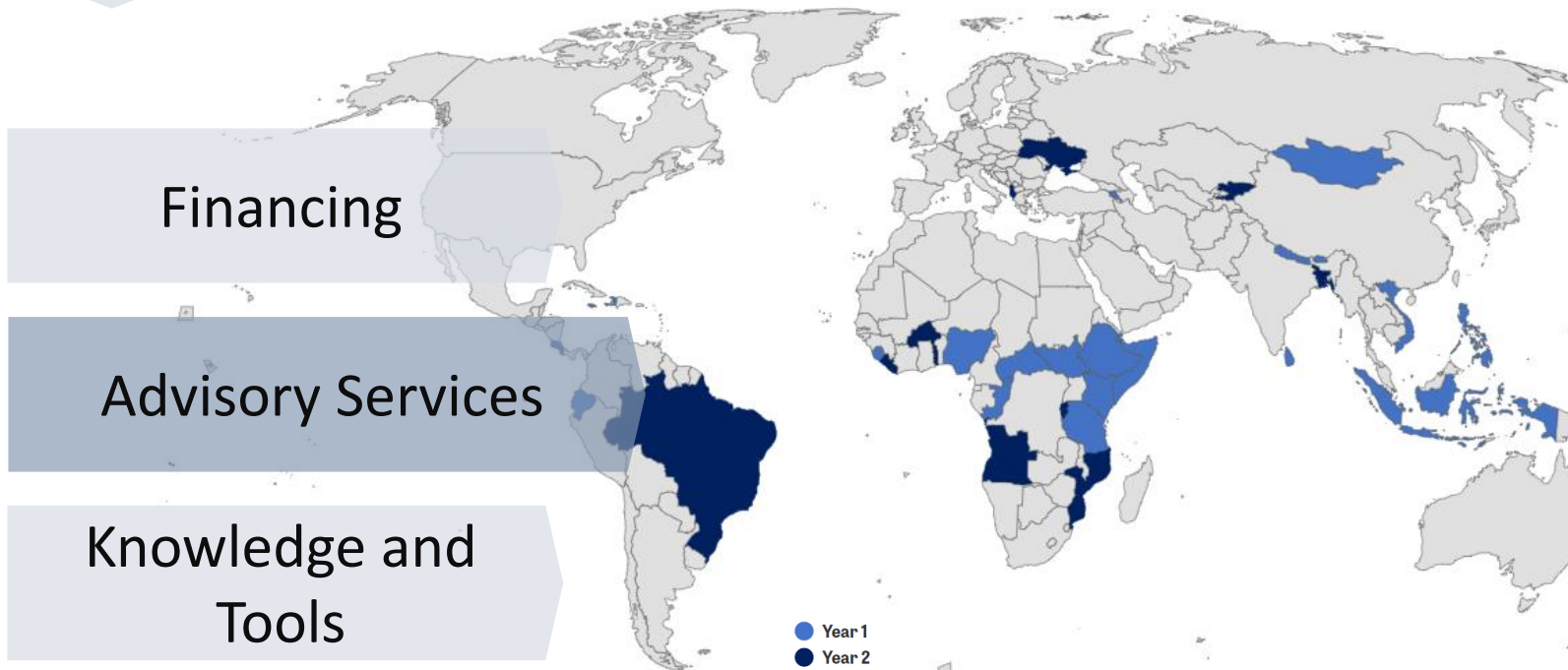
Samoa

with over **\$40** million investment



The Cyber Multi-Donor Trust Fund has been a key enabler of country support

Since 2022, the MDTF has enabled the World Bank to provide in-depth technical assistance to many client governments and has contributed to advancing policy dialogue and capacity-building



37 countries benefited as of 2023

The MDTF is also enabling a scale-up of capacity-building efforts across critical sectors, supporting the development of sector-specific cybersecurity knowledge and tools

- Financing
- Advisory Services
- Knowledge and Tools
- Convening Services

- Year 1
● Year 2
- East Asia and Pacific (EAP)
- Indonesia
 - Mongolia
 - Philippines
 - Viet Nam
 - Kiribati
 - Samoa
 - North Pacific



Sectoral Cybersecurity Maturity Model (SCMM)

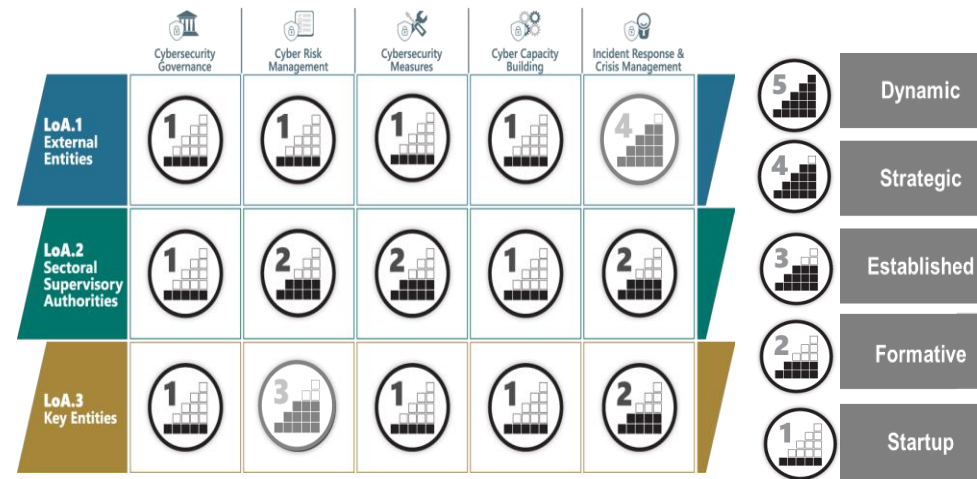
The SCMM Version 1.0 was published in June 2023. It helps analyze cybersecurity maturity in critical sectors to gain insights into current gaps and identify the capabilities needed to strengthen sectoral cyber resilience

Financing

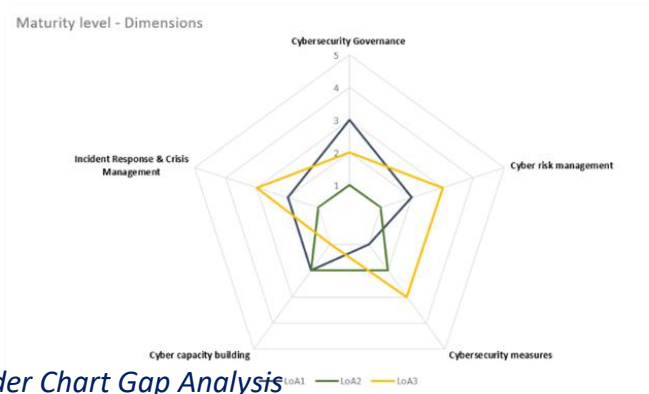
Advisory Services

Knowledge and Tools

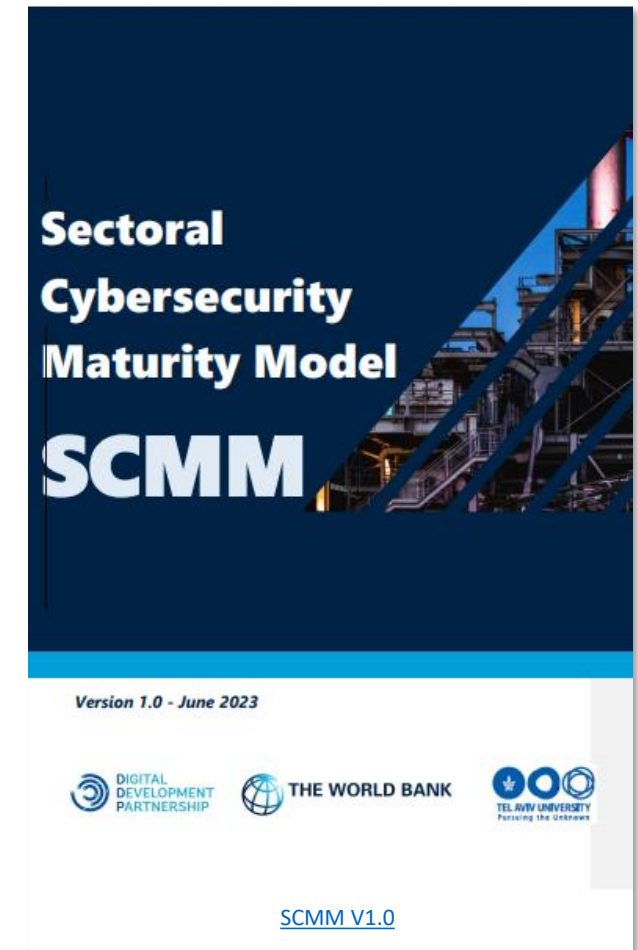
Convening Services



SCMM's Maturity Heatmap



SCMM's Spider Chart Gap Analysis



The SCMM helps develop an actionable, feasible, and prioritized roadmap to enhance sector's resilience and capacity



Knowledge Work: Practitioners' Notes, Case Studies

Ghana has substantially increased its national cyber posture and resilience with long term world bank financial and technical support

Financing

Advisory Services

Knowledge and Tools

Convening Services

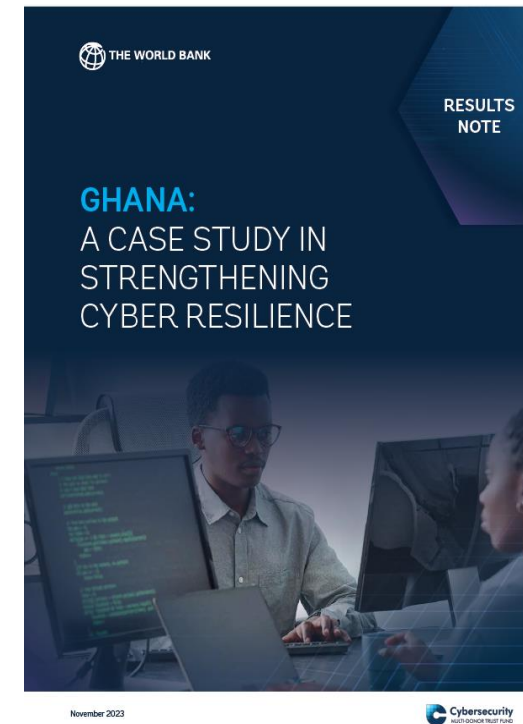
Cyber Skills Gap Practitioner Note



- Demand for cybersecurity grew by 76% in Brazil and 55% in Indonesia, against an average of 35% in 2022.
- Nigeria and Mexico rank 1st with 34 percent women in their cybersecurity workforce.
- One innovative measure to reduce the gap is to leverage the untapped potential of ethical hackers.

Source: [World Bank](https://www.worldbank.org/)

Ghana Case Study



World Bank Investments and Technical Assistance enabled

National cybersecurity maturity assessment (CMM)



Stable funding at the early stages of capacity building



Leveraging best practices and innovative models



Knowledge transfer through international expertise





Leveraging partnerships & convening to maximize impact for clients

The World Bank is leveraging partnerships with key stakeholders to maximize the outreach of its knowledge products and deliver value to developing countries' governments through knowledge-sharing events such as the GC3B.

Financing

Advisory Services

Knowledge and Tools

Convening Services

10+ CyberTalk seminars

featuring ~80 speakers with over 1700 live participants on key topics for enhancing cyber resilience in developing countries.



The Bank co-organized the **Global Conference on Cyber Capacity Building (GC3B)** in Accra, Ghana (November 2023) in partnership with the Global Forum on Cyber Expertise (GFCE), World Economic Forum (WEF) and Cyber Peace Institute (CPI).

700+ participants from **94** countries including dozens from the Pacific



Cybersecurity Workstreams - What Topics Do We Cover?

Cybersecurity Workstreams

Digital Samoa Project Data Governance

1 Cybersecurity Governance and Institutions



2 Risk Management & Critical Infra Protection



3 Incident Response & Preparedness



4 Skills Development & Awareness Raising



5 Industry & Private Sector Development

6 Cross-Border Cooperation

A rustic wooden house built on stilts over a body of water. The house has a dark, rusty corrugated metal roof and walls made of various materials, including wood and colorful corrugated metal. The structure is supported by numerous wooden posts. In the background, there are mountains under a cloudy sky.

Thank you

Cybersecurity Intranet: <https://worldbankgroup.sharepoint.com/sites/DS/>

Cybersecurity external web: <https://www.worldbank.org/en/topic/digitaldevelopment/brief/cybersecurity>

Hagai Mei-Zahav: hmeizahav@worldbank.org | LinkedIn: **Hagai Mei-Zahav**