Strategic Cybersecurity Imperatives and Digital Resilience

20th Caribbean Internet Governance Forum

ARIN/LACNIC/CTU Public Policy Forum

23 August 2024

kevon@lacnic.net

lacnic

www.lacnic.net

Topics Covered

Presentation Outline

01 Cybersecurity in a National Context

02 Focus Areas Based on Best Practices

03 Measuring The Impact of Efforts

04 Recurrent Pain Points

lacnic

What is Cybersecurity?

Several national and international definitions of the term “cybersecurity” exist. For current purposes, the term “cybersecurity” is meant to describe the **collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies** that can be used to **protect the availability, integrity and confidentiality of assets** in the connected infrastructures pertaining to **government, private organisations and citizens**; these assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data in the cyber-environment.

Source: International Telecommunication Union

National Context for Cybersecurity

an expression of the vision, high-level objectives, principles and priorities that guide a country in addressing cybersecurity

an overview of the stakeholders tasked with improving cybersecurity of the nation and their respective roles and responsibilities; and

a description of the steps, programmes and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience

Source: International Telecommunication Union

lacnic

Cybersecurity v. Cybercrime (Prevention) Strategies

National interests and security, trust, resilience, reliability of ICT		Rule of law, human rights, and crime prevention and criminal justice	
Cybersecurity strategies		**Cybercrime strategies**	
Non-intentional ICT security incidents	Intentional attacks against the confidentiality, integrity and availability of computer systems and data	Computer-related and content-related offences	Any offence involving electronic evidence

Source: UNODC (2013). *Draft Comprehensive Study on Cybercrime* , p. 228.

FOCUS AREAS FOR NATIONAL CYBERSECURITY

RISK MANAGEMENT AT A NATIONAL LEVEL

Risk management approach; common methodology for managing cs risk; sectoral cs risk profiles; cs policies

CRITICAL INFRASTRUCTURE SERVICES AND ESSENTIAL SERVICES

Risk management approach to protect CIS; governance model w responsibilities; minimum baselines; market levers; PPPs

LEGISLATION AND REGULATION

Cybercrime legislation; safeguards for individual rights and liberties; compliance mechanisms; CB for LEAs; inter-org processes; international coop for cybercrime

01

02

03

04

05

06

07

GOVERNANCE

Ensure highest level of support; competent cs authority; intragovernmental cooperation; inter-sectoral cooperation; dedicated budget & resources; plan

PREPAREDNESS AND RESILIENCE

Cyber incident response capabilities; contingency plans and cs crisis management; info sharing; cs exercises

CAPABILITY, CAPACITY AND AWARENESS BUILDING

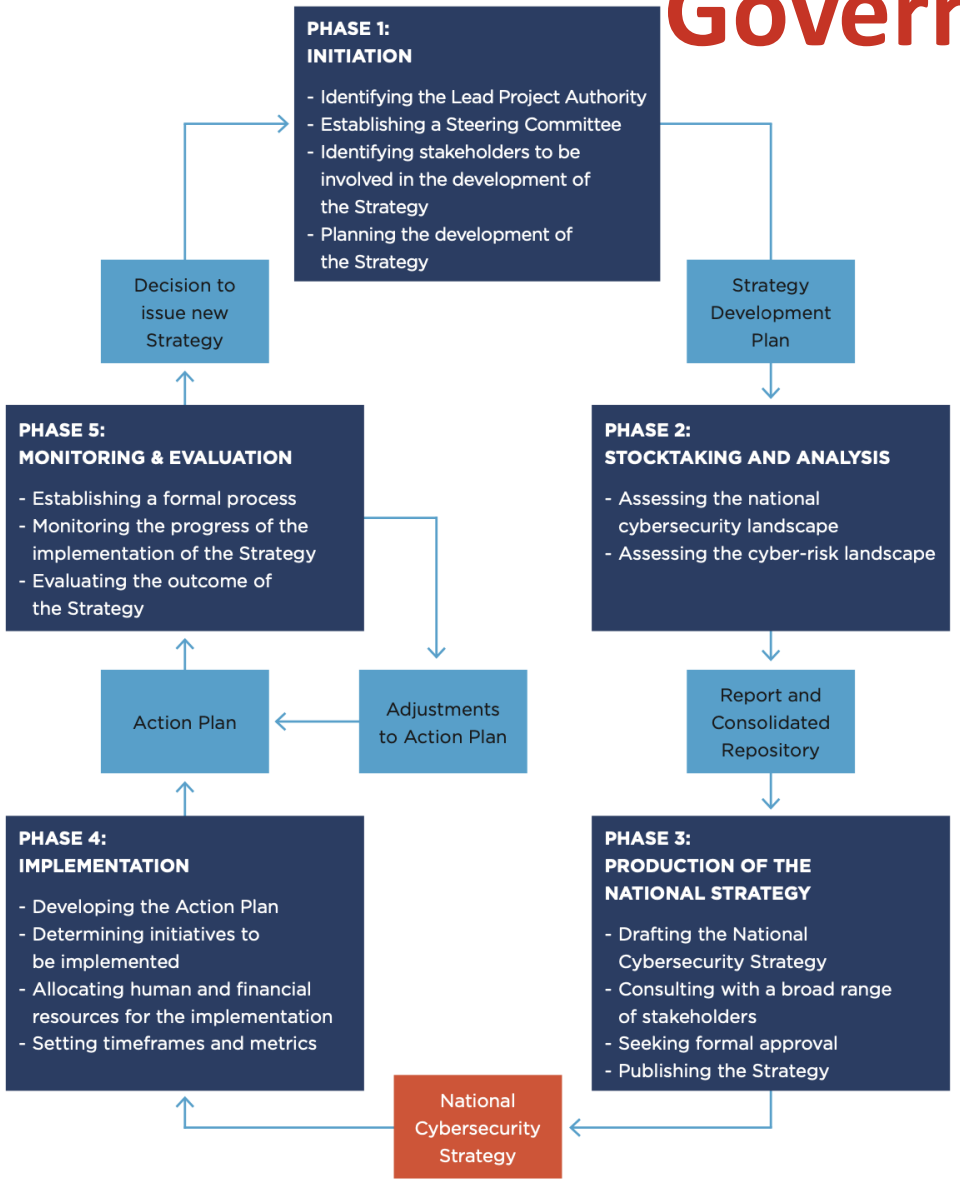
Develop cs curricula; skills development & workforce training; coordinated awareness raising programme; RD+i

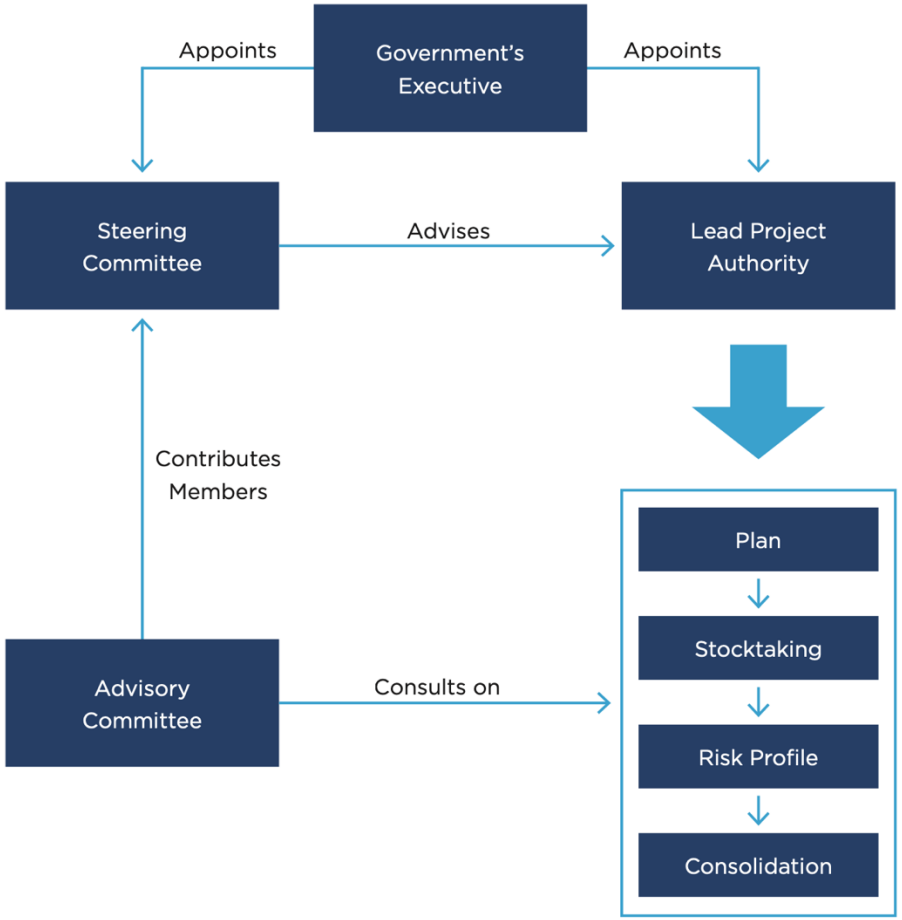
INTERNATIONAL COOPERATION

CS as a foreign policy imperative; international discussions; formal and informal cooperation; align domestic and international efforts

lacnic

National Cybersecurity Strategy Lifecycle & Governance (ITU)





Measuring the impact of efforts - GCI

Overall Score developed through measuring:

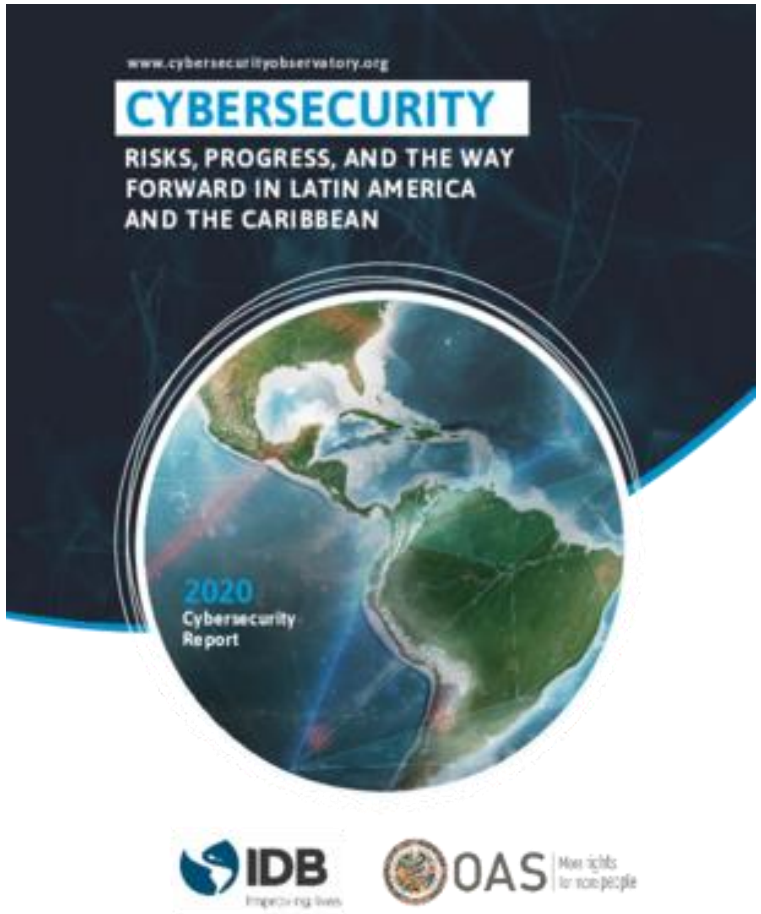
- Legal Measures
- Technical Measures
- Organisational Measures
- Capacity Development
- Cooperation

Measuring the impact of efforts - GCI

- Legal Measures
  - Countries with some form of cybersecurity legislation
  - Data Protection regulations
  - Critical Infrastructure regulations
- Technical
  - Active CSIRTs
  - Engaged in regional CSIRT
  - Child Online Protection Reporting mechanisms
- Organisational
  - National Cybersecurity Strategies
  - Cybersecurity Agencies
  - Child Online Protection strategies and initiatives reported
- Capacity Development
  - Countries conduct cyber-awareness initiatives
  - Countries with cybersecurity R&D programmes
  - Countries reported having national cybersecurity industries
- Cooperation
  - Countries engaged in cybersecurity Public-Private Partnerships
  - Countries with cybersecurity bilateral agreements
  - Countries with cybersecurity multilateral agreements

lacnic

Measuring the impact of efforts - CMM



Cybersecurity Capacity Maturity Model for Nations (CMM)

- Developed by Global Cyber Security Capacity Centre of the University of Oxford in 2013
- Five stages of maturity, ranging from most basic (Start- up) to most advanced (Dynamic)
- Five dimensions measured
  - Cybersecurity Policy and Strategy (devising cs strategy and resilience)
  - Cyberculture and Society (encouraging a responsible cs culture within society)
  - Cybersecurity Education, Training and Skills (developing cs knowledge)
  - Legal and Regulatory Frameworks (effective frameworks)
  - Standards, Organisations and Technologies (controlling risks through standards, organisations, and technologies)

lacnic

Internet Resilience

Pillars of the Internet Society's Internet Resilience Index (IRI)

Infrastructure

The existence and availability of physical infrastructure that provides Internet connectivity.

Performance

The ability of the network to provide end-users with seamless and reliable access to Internet services.

Security

The ability of the network to resist intentional or unintentional disruptions through the adoption of security technologies and best practices.

Market Readiness

The ability of the market to self-regulate and provide affordable prices to end-users by maintaining a diverse and competitive market.

lacnic

IRI - Enabling Technologies and Security

ENABLING TECHNOLOGIES

- IPv6
- HTTPS

ROUTING HYGIENE

- MANRS Readiness
- Upstream Redundancy

DNS ECOSYSTEM

- DNSSEC Validation
- DNSSEC Adoption

SECURITY THREAT

- Secure Internet Servers
- Global Cybersecurity Index (GCI)
- DDoS Potential
- SPAM Infections

lacnic

CARICOM-level planning

Some pain points for national cybersecurity in the Caribbean

- Unclear governance; limited mandate and budgets of involved agencies
- National strategies are not frequently updated and are not as strong as they could be
- Challenges in engaging, retaining and upskilling cybersecurity professionals
- Robust Public-Private Partnerships to facilitate threat analysis and mitigation
- Critical infrastructure sectors remain vulnerable to attacks
- Limitations to protecting personal privacy due to disparate implementation of modernised legislation
- Confusion concerning CS CB actors and available assistance

Questions?

Strategic Cybersecurity Imperatives and Digital Resilience

20th Caribbean Internet Governance Forum

ARIN/LACNIC/CTU Public Policy Forum

23 August 2024

kevon@lacnic.net

lacnic

www.lacnic.net