Critical Infrastructure Protection (CIP) as example of a multi-stakeholder approach.

By
Christopher Ganizani Banda
ICT Development Manager
Malawi Communications Regulatory Authority

24-26th July ,2016

MACRA
Promoting Universal ICT Access

Khartoum, Republic of Sudan, 24 – 26 July 2016

Presentation Outline

- Introduction.
- Some Definitions
- CIP Stakeholders
- Protecting critical infrastructure
- 7 Steps for CIP Protection
- CIP Goals and Roles
- Identify and Prioritize Critical Functions
- Continuously Assess and Manage Risks
- Establish and Exercise Emergency plans
- Create Public-Private Partnerships
- Build Security/Resiliency into Operations
- Update and Innovate Technology/Processes
- Malawi Experience
- Conclusion

INTRODUCTION

- Modern life is increasingly reliant on a wide-ranging set of functions.
- These includes services, systems, and assets, commonly referred to as infrastructures.
- Governments view several of these infrastructures, such as communications, banking, energy, transportation, and healthcare etc, as critical .
- The disruption, destruction, or loss of integrity of these can impact a nation’s stability hence the need for protection.
- Critical infrastructures are often thought of as physical assets but have now integrated information and communications technology (ICT).

Some Definitions

- **Critical infrastructure:** The key systems, services, and functions (IT or physical) whose disruption, destruction, or exploitation could have a debilitating impact on public health and safety, commerce, and national security, or any combination.
  - Critical Infrastructure Protection: Concepts and Continuum, Microsoft
- **Critical information infrastructure (CIIs) :** are communications and/or information services whose availability, reliability and resilience are essential to the functioning of a modern economy.
  - Critical Information Infrastructure Protection, A Report of the 2005 Rueschlikon Conference on Information Policy
- **Critical infrastructure protection (CIP):** CIP consists of the proactive activities to protect the indispensable people, physical assets, and communication/cyber systems from any degradation or destruction caused by all hazards.
  - The Emergency Management and Response—Information Sharing and Analysis Center 2007

Critical Infrastructure Protection (CIP) Stakeholders

- Government agencies,
- The Private sector, (Technology vendors)
- Research agencies (Academia),
- The Defense/Military/intelligence agencies
- All IT workers
- International organizations.

Protecting critical infrastructure

- Principles that form a CIP continuum:
  - **Establishing trustworthy policies and plans** for protecting critical infrastructure in today’s dynamic environment.
  - **Managing risk:** Fostering capabilities for protecting, detecting, and responding to risks to promote operational resiliency.
  - **Promoting innovation and investments:**

    By learning from policy and operations that can guide the allocation of resources for practices, programs, education, and research related to CIP

7 Steps for Critical Infrastructure Protection Microsoft Model.

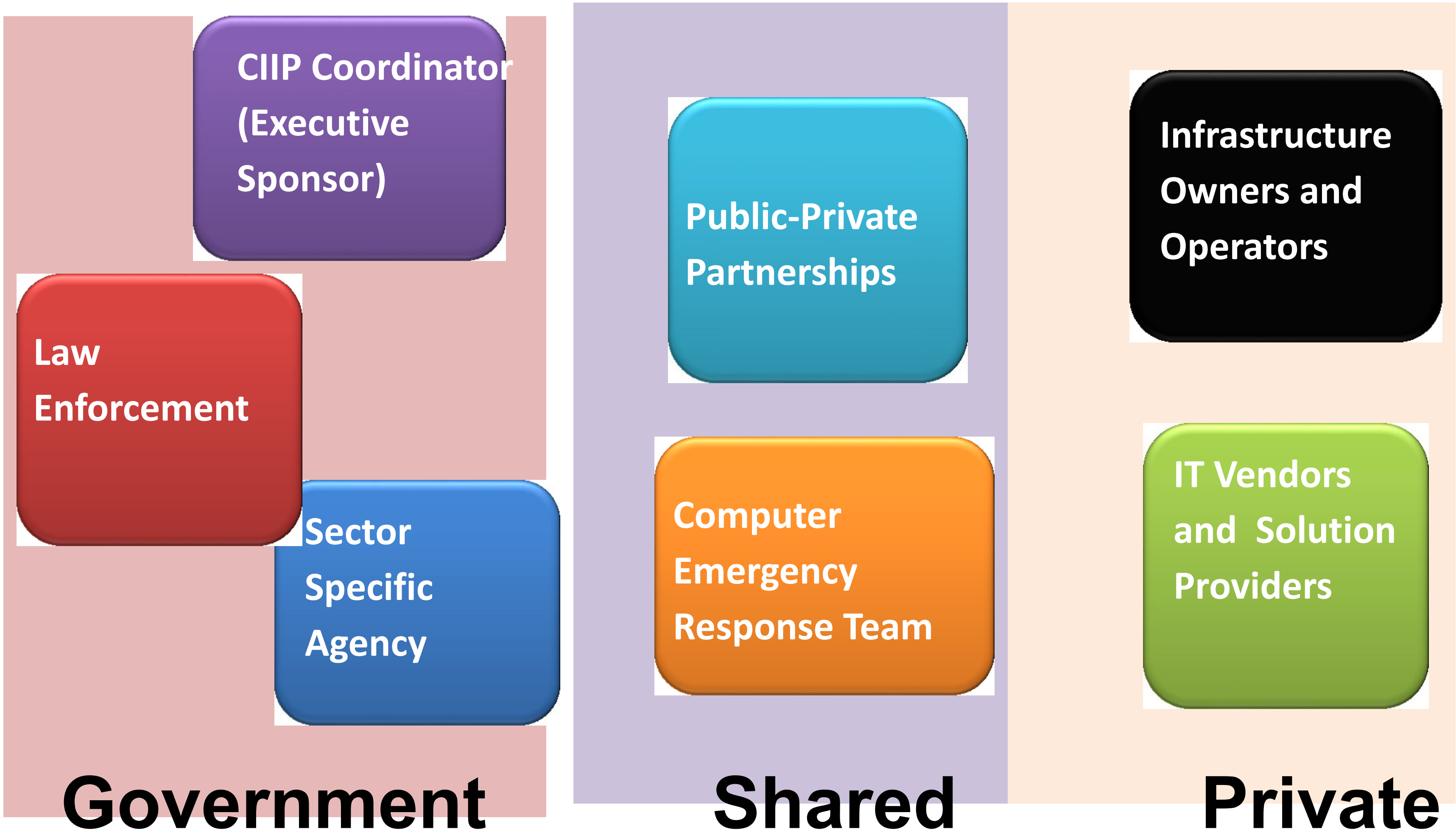
1. Define Goals and Roles
2. Identify and Prioritize Critical Functions
3. Continuously Assess and Manage Risks
4. Establish and Exercise Emergency plans
5. Create Public-Private Partnerships
6. Build Security/Resiliency into Operations
7. Update and Innovate Technology/Processes

1a.CIP Goals.

Establishing Clear Goals is Central to Success

Policy Elements	
Critical Infrastructure Importance	Provide the essential services that support modern information societies and economies. Support critical functions and essential services so vital
Critical Infrastructure Risks	Any Compromised can affect national security and economic well-being.
CIP Policy Goal/Statement	The aim is to Prevent or minimize disruptions to CIIs,. In the event disruptions do occur, they should be infrequent, of minimal duration and manageable.
Public-Private Implementation	Implementing the National CIIP framework includes government entities, as well as, voluntary public private partnerships involving corporate and nongovernmental organizations.

1b.Define Roles



CIIP Coordinator (Executive Sponsor)

Law Enforcement

Sector Specific Agency

Government

Public-Private Partnerships

Computer Emergency Response Team

Shared

Infrastructure Owners and Operators

IT Vendors and Solution Providers

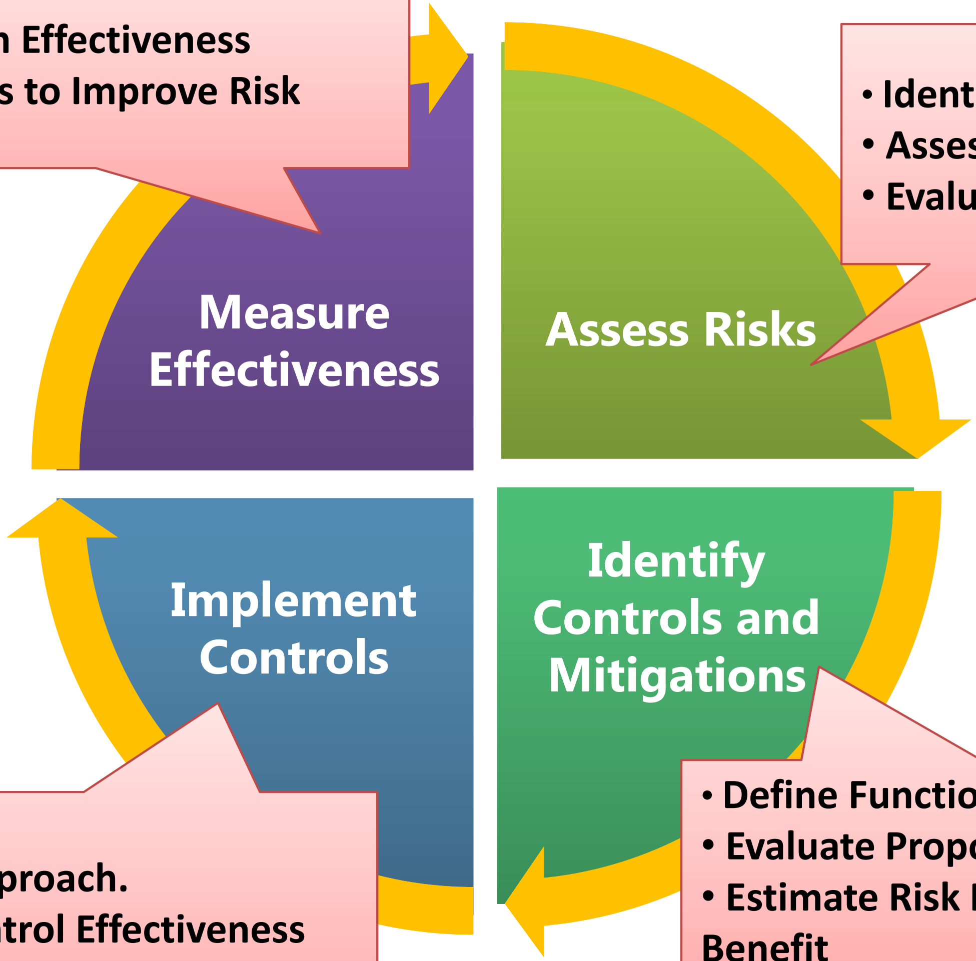
Private

2.Identify and Prioritize Critical Functions

- Establish an open dialogue to understand the critical functions, infrastructure elements, and key resources necessary for
  - delivering essential services,
  - maintaining the orderly operations of the economy, and
  - ensuring public safety.

3. Establish and Exercise Emergency plans.

Protection is the Continuous Application of Risk Management



- Evaluate Program Effectiveness
- Leverage Findings to Improve Risk Management

- Identify Key Functions
- Assess Risks
- Evaluate Consequences

- Define Functional Requirements
- Evaluate Proposed Controls
- Estimate Risk Reduction/Cost Benefit
- Select Mitigation Strategy

- Seek Holistic Approach.
- Organize by Control Effectiveness
- Implement Defense-in Depth

4. Establish and Exercise Emergency plans

Improve Operational Coordination

- Form joint plans for managing emergencies – including recovering critical functions in the event of significant incidents, including but limited to natural disasters, terrorist attacks, technological failures or accidents.

- Effective emergency response plans are generally short and highly actionable so they can be readily tested, evaluated, and implemented.

- Testing and exercising emergency plans promotes trust, understanding and greater operational coordination among public and private sector organizations.

- Exercises also provide an important opportunity to identify new risk factors that can be addressed in response plans or controlled through regular risk management functions.

5. Create Public-Private Partnerships

- Voluntary public-private partnerships
  - Promote trusted relationships needed for information sharing and collaborating on difficult problems,
  - Leverage the unique skills of government and private sector organizations, and
  - Provide the flexibility needed to collaboratively address today's dynamic threat environment

6. Build Security and Resiliency into Ops

- Organizational incentives can drive security development lifecycle principles into all line of business

- Leveraging the security lifecycle promotes secure and resilient organizations and products

7. Update and Innovate Technology/Processes

- Cyber threats are constantly evolving
- Policy makers, enterprise owner and operators can prepare for changes in threats by
  - Monitoring trends
  - Keeping systems patched
  - Maintaining the latest versions of software that have been built for the current threat environment.

Malawi Experience

- Growth of mobile and Internet penetration (Connectivity)
- Increase in reliance of internet for social, economic, political interactions.
- Mult stakeholder Approach to Cyber security
  - High level Cyber security Awareness workshops
    - COMESA/MACRA (April 2015)
    - MDF;Malawi Police and University (Sept 2015)
  - Cyber security Strategy Project (CTO/MACRA) (june2016 –May 2017)
- New E-Transaction and Cyber security Law (July; 2016)
- New Reviewed Communications Law (July; 2016)

CONCLUSION

- CIP is crucial and specific policies might be necessary.
- Multi-stakeholder approach crucial
- Harmonization of laws (regional & international) to enhance international coordination & elimination of safe harbors
- Innovation/Capacity building and Awareness equally crucial