

Cyber Capacity Comes In Many Forms

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Software Engineering Institute

Carnegie Mellon University

© 2016 Carnegie Mellon University

Cyber Capacity Comes In Many Forms

REV-03.18.2016.0

Infrastructure and Policy Considerations

Infrastructure

- The amount of and speed that information is moving continues to grow.
- Our global dependence on information continues to grow.
- A nation's economy and national security depends on information.
- Building a resilient, flexible and manageable national infrastructure is key.
 - Need redundancy as well as diversity.

Policy

- National Cybersecurity Policies/Strategies/Legislation
- Government Support

Operational Considerations

Computer Security Incident Response Teams

- Need to be empowered
 - Can support and provide
 - Cyber hygiene support
 - Technical guidance around infrastructure and policy
 - Provide situational awareness and alerting
 - Investigate and/or respond to cyber incidents
 - The initial focus
 - Foundation and Fundamentals
 - Then Operational Capabilities

Capacity Development Implementation

Factors to Consider

- Cost effective
- Environmental constraints
- Leverage opportunities and differences from country to country
- Prioritization of countries with potential to assist others in the region

Mentoring Model

- Enables flexibility to support capacity development efforts at various levels
- Advice and experience sharing are very valuable to recipients and relatively easy to deliver for mentors

Capacity Development Implementation-2

Promoting and collaborating with local experts

- Local experts provide key insights for appropriately shaping initiatives
- Often have a track record of success in related areas
- Able to connect relevant stakeholders

Fostering regional cooperation

- Technical exchanges for cybersecurity practitioners
- Create a medium for regional working groups and initiatives
- Enable regional leaders to lead

Facilitating Mentorship of National CSIRTs

- Africa CERT Workshop, Tunis
 - TunCERT
 - Resources
- Forum for Incident Response and Security Teams (FIRST), Technical Colloquium, Accra
 - CERT GH (Ghana)
 - Services
- CI-CERT (Cote d'Ivoire)
 - FIRST Assessment in Partnership with TunCERT
 - Regional Cooperation
- Botswana
 - Focus is on national strategy first; no national CSIRT yet
 - Enables alignment of national CSIRT with strategy from beginning

Contact Information

Office of the Coordinator for Cyber Issues

U.S. Department of State

Office Number: (202) 647-5849

Email: SCCI@state.gov

<http://state.gov/s/cyberissues>

International Cybersecurity Initiatives

CERT Coordination Center

Software Engineering Institute

Carnegie Mellon University

Email: international-team@cert.org

<http://www.cert.org/>

