Cyber Incident Management
Research project proposal

GFCE Theme/Topic	Cyber Incident Management
Research Idea	Research is needed to identify a menu of practical, feasible and affordable individual, team, and group training options that increase the maturity and capabilities of national CSIRTs in low- income countries.[1]
Problem statement/Knowledge gap	Many low-income countries seek greater economic, social, and governance development by leveraging ICT capabilities. These capabilities provide significant benefits, but also increase risks to the nation that may stymie development goals, increase national security threats through cyberspace, and threaten the privacy of citizens. Technically competent national CSIRTs are needed to address the increasing risks of technology to a nation by increasing society's awareness of cyber risks, providing advice to governments on appropriate risk mitigation policies, responding to incidents, and helping all citizens and businesses to operate more safely in cyberspace. Many low-income countries do not have, and cannot afford to train, equip, and operate viable national CSIRTs that are capable of performing the essential CSIRT services described by the FIRST organization (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1). No compendium of affordable and achievable training, organizational and technical resources, that can be applied under an implementation framework tailored to address a variety of low-income country CSIRT development needs currently exists. Such a product would be a useful guide for developing national CSIRTs and increasing countries' ability to deal with cyber security issues. This product would also strengthen regional CSIRT ecosystems. This research effort should also ensure that this compendium of resources and framework for implementation is tailorable to multiple circumstances and is not a 'one-size-fits-all' solution.
Research question(s)	Primary Research Question: What are the affordable individual, team, and group training resources, organizational models, and technical tools available to support the development of CSIRTs in low-income countries, and how could a menu of these resources be configured/tailored and applied in an implementation framework to develop and increase the capabilities and maturity of low-income CSIRTs? Secondary Research Question: What are sound approaches for creating CSIRT training programs for low-income CSIRT individuals and teams that leverage existing best practice cyber security training and education models that identify required skills, knowledge, and abilities, and how can low-income CSIRTs best create personnel pipelines that supporting hiring, training and retaining qualified CSIRT.

[1] See 'Official Development Assistance' (ODA) list: http://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/DAC-List-of-ODA-Recipients-for-reporting-2020-flows.pdf

Research objectives	Primary Objective: To provide low-income countries with a practical, affordable, flexible, and achievable workforce training and development methods including a menu of resources mapped to CSIRT organizational, technical, and operational service requirements.
Suggested research approach (method)	The research approach should catalogue existing research related to this topic and leverage CSIRT workforce development research and processes that currently exist in the development of training options. It should identify the minimum activities of a functioning national CSIRT; establish baseline individual, team, and group training requirements to perform those functions, and map those training needs to a menu of affordable, and practical training resources. The research should also address the organizational and technical aspects of CSIRT development that support the creation and retention of a qualified CSIRT workforce. The research methodology should incorporate interviews of personnel from developing CSIRTs in low-income countries to determine their development approaches and identify training and organizational gaps and requirements. The research plan should identify comprehensive criteria for the selection of developing CSIRTs and personnel to interview. Ideally, researchers should have an extensive understanding of the CSIRT community, current measures of CSIRT capacities, and the challenges associated with national CSIRT development.
Research output	The output of this research should be a 45-page research paper that 1) identifies a tailorable menu of affordable training, organizational and technical resources for developing and maturing CSIRT capacities in low-income countries; 2) provides a flexible framework for assessing a CSIRT’s training, organizational, and technical needs, focusing on workforce development and retention, that enables a CSIRT to develop a plan of action to increase their capabilities and maturity.
Time estimate	6 months
Estimation of human resources needed	Two Full Time Equivalent CSIRT experts.
Selection Criteria	Two CSIRT experts from Academia/NGO.
Budget	$50K USD