Cybersecurity Resource Centers for the Financial Sector

Photo for CGAP by Muhammad M. Rahman

A proposed business concept

July 2020

CGAP

Authors:

Silvia Baur-Yazbeck, CGAP Financial Sector Analyst

David Medine, CGAP Senior Financial Sector Specialist

Jean-Louis Perrier, Consultant

Acknowledgments:

The authors would like to thank LuxDevelopment and the Ministry of Foreign and European Affairs of Luxembourg, SECURITYMADEIN.LU, the University of Luxembourg, Excellium Services in Luxembourg, and Suricate Solutions in Senegal for their technical inputs and sharing of experiences.

Disclaimer

This work was funded in whole or in part by CGAP. Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP. Any conclusions or viewpoints expressed are those of the authors, and they may or may not reflect the views of CGAP staff.

Executive Summary

Cybersecurity is key for advancing financial inclusion

Trust and confidence in financial services is a key ingredient for sustained financial inclusion. But confidence takes time to build, is easily broken by rumors or poor media coverage, and if trust is broken, it may set back advances in financial inclusion by decades.

Many consumers in developing countries make financial transactions through **USSD channels, which are insecure**.

Poor people are more likely to fall victim to social engineering attacks.

Poor people can least afford to loose money.

In most developing and emerging countries, **the customer is liable for losses** associated to a cyber incident or the burden of proof is on the customer.


Photo for CGAP by Trung Vo

Learn more about cyber vulnerabilities in mobile financial transactions CGAP (2018) "Cybersecurity for Mobile Financial Services: A Growing Problem"

Problem statement and proposed solution

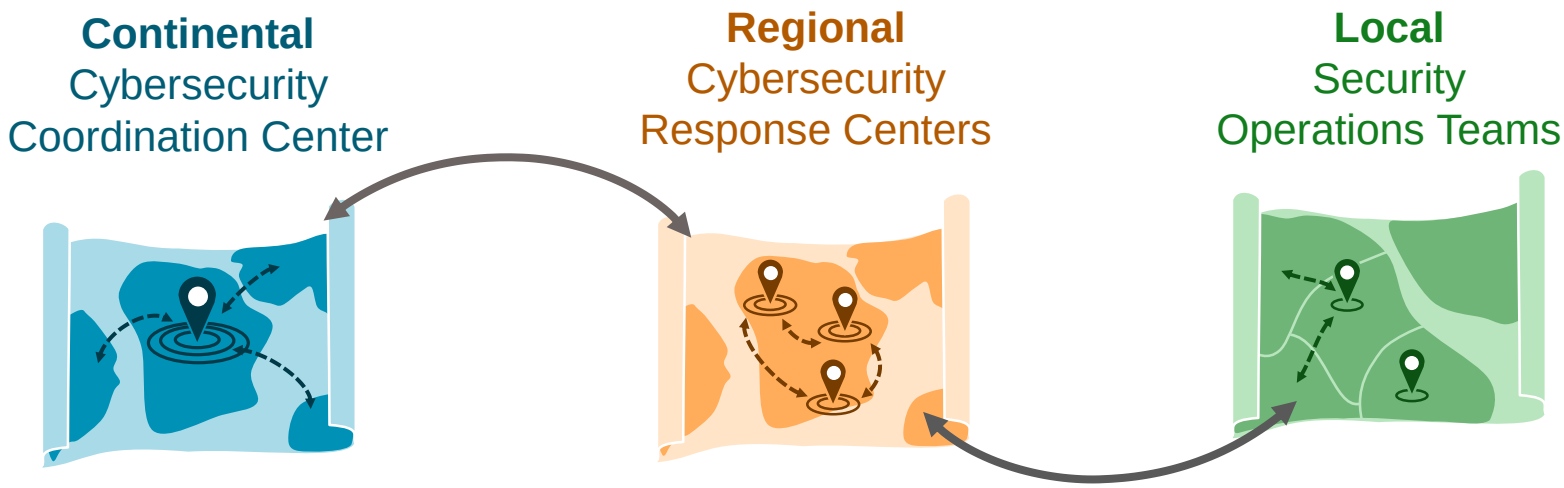
Problem: Growing cybersecurity risks threaten financial sector stability and integrity, as well as financial consumer protection and financial inclusion. Financial sector policymakers and providers need specialized support to build and manage cyber resilience. But many developing countries lack affordable and reliable cybersecurity resources and capabilities, especially specialized skills in financial sector cybersecurity.

Solution: Multiple countries in a region pool their resources and create ***shared cybersecurity resource centers*** to benefit from economies of scale. Centers focus on the financial services sector and offer:

- Intelligence about cyber threats and risk management
- Timely, accessible, and affordable emergency response
- Relevant and personalized guidance and capacity building
- Information about international trends and best practices
- Neutral platform for regional and local collaboration, including public and private sector actors
- Support to existing cybersecurity service providers and initiatives

See CGAP Report (2019) "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion".

Cybersecurity resource centers operate at the continental, regional and local levels



Cybersecurity resource centers have three main parts - one continental cybersecurity coordination hub, two or more regional response centers and several in-country, local security operations teams. The continental, regional and local entities may be completely separate, or in some instances combined to economize. They may also build on existing Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), but with a financial sector focus. Each entity provides a different set of complementary services, including services to each other. Together they support the financial sector to prevent, detect, respond to, and recover from cyber incidents.

Cybersecurity resource centers can become self-sustaining within a few years

Budget forecasting for a Pan-African Cybersecurity Resource Center estimates break-even within 3-4 years and profits by the 5th year *(see p. 60-62)*.

Continental Coordination Center	**Years I–III** (aggregate) *60–200 paying users* *25–35 staff*	**Years IV-V** (aggregate) *200–350 paying users* *40–42 staff*
Revenues	4,357,000	5,660,000
Expenses	6,113,530	4,795,312
EBIT	(1,756,530)	864,688

Regional and Local Centers	**Years I-III** (aggregate) *80–300 paying users* *16–51 staff*	**Years IV-V** (aggregate) *400–500 paying users* *60–68 staff*
Revenues	3,194,400	7,490,400
Expenses	6,139,040	6,701,061
EBIT	(2,944,640)	789,339

The continental coordination center and regional response centers become self-sustaining as their customer base grows, the range of services expands, and efficiency increases through economies of scale in part from mutualizing resources and expenses across regions and countries.

EBIT: Earnings Before Interest and Taxes

Cybersecurity resource centers address important development objectives

They advance **financial consumer protection** by reducing the risk of financial and psychological harm caused by cyber incidents. Risk reduction is critical to the expansion of digital finance and sustained financial inclusion. *(see p.18, 58)*

They contribute to a number of **sustainable development goals** by building local professionals' skills in high-paying technology fields, enhancing job opportunities for professionals from lower income countries, including youth and women. *(see p.19, 20, 59)*

They address not only the cybersecurity capacity gap, but contribute toward **building a cybersecurity market** in the region. *(see p.22, 23)*

They require upfront capital investments but **can become self-sustaining** after 4-5 years. *(see p.34-44, 60-62)*

Development funders, implementers, and facilitators can support cybersecurity resource centers

They can **convene and engage** with stakeholders in the target region or target countries to build local support for the concept and identify existing local initiatives and capacities that can be leveraged.

They can **support market assessment**, including an evaluation of the need for cybersecurity, and the supply of existing providers, initiatives and working groups, regional capacity, incentives and relationships that may support or hinder establishment of cybersecurity resource centers.

They can **facilitate dialogue and build partnerships** among public sector stakeholders and between public and private sector stakeholders.

They can **support planning, initiation, and implementation** of cybersecurity resource centers as a neutral convener and by providing technical expertise, advocacy, and financial support.

They can **drive social impact** mission of cybersecurity resource centers with specialized technical assistance, advocacy, and financial support.

Why It Matters

Cyber risks, trends and needs

CGAP

Cyber crime is on the rise, and developing countries need help

Cyber crime is on the rise globally, but developing countries are significantly less prepared to prevent, detect, address, and recover from cyber attacks.

For example, a vulnerability assessment of Africa's banking sector in 2017 revealed:

- **US $1.048 trillion lost from cyber attacks**
- 75% of organizations did not carry out security testing techniques
- 60% of organizations did not keep up to date with cyber security trends and attacks
- 96% of cyber security incidents went unreported or unresolved
- 75% of vulnerabilities within organizations were missing patches
- **Huge talent gap:** limited number of qualified cybersecurity experts.

The mobile banking sector is even more exposed.

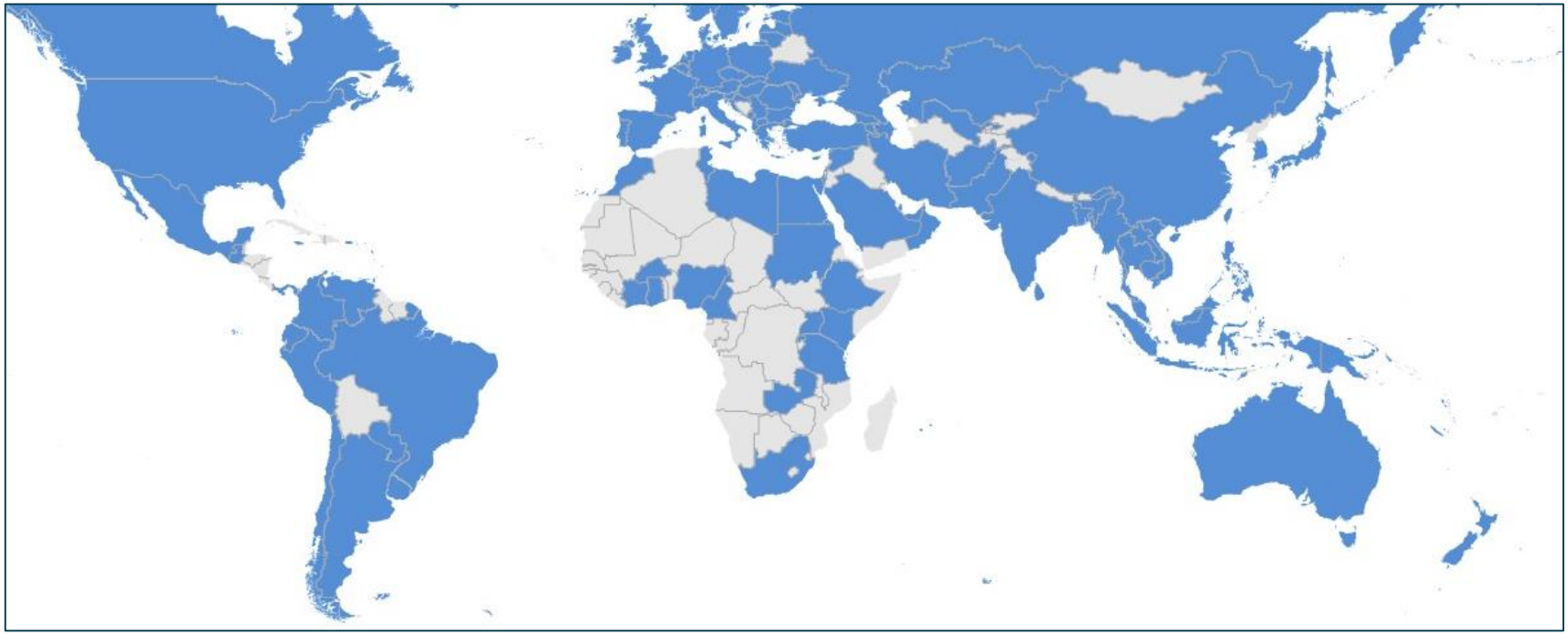
- Most mobile money applications lack basic security controls, such as data encryption
- The most common types of fraud in mobile transactions include SIM card swapping, social engineering attacks (resulting in identity theft), and insider fraud attacks
- Mobile banking users frequently fall victim to social engineering attacks, especially with the increased number of betting and Ponzi schemes

See CGAP Report (2019) "Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion".

Some cybersecurity structures are already in place – but there are big gaps in Africa

There is a growing network of national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

But in developing countries, many of them have **low capacity, limited services, and often only serve public sector agencies.** Also, there are **very few CERTs or CSIRTs that focus on the financial sector.**



Countries marked in blue have a national CERT or CSIRT. Source: ITU (2019) National CIRT

African stakeholders say they need relevant and affordable cybersecurity support services

Due to the prominent resource gap in Africa, CGAP interviewed dozens of regulators, supervisors, payments system operators, financial service providers, and experts from across Africa, in 2018. Here's what we learned:

Limited availability of services in their country and, where available, services are too costly.

- Users all told us they need help and are willing to pay, but they need more affordable services

Smaller providers lack incentives to invest in cyber security

- Seldomly acknowledged and addressed at management level
- Incentives increase after experience a malicious incident or introduction of regulations

No/little access to threat information, best practices and guidance for building cyber resilience

Public-private dialogue needs strengthening

Consumers lack awareness and education to protect themselves

There was overall positive feedback on the idea of an African cybersecurity resource center. Yet it was emphasized that emergency response and security monitoring needs to be offered locally to build customer relationships and trust. There is openness to collaborate with public and private sector actors. Government support and endorsement was also highlighted.

Existing cybersecurity support structures in Africa

Emergence of national CERTs, but slow in becoming operational; very limited range of services (e.g., Ghana, Nigeria, Rwanda, South Africa)

National public-private working groups focused on financial fraud increasingly touch on cybersecurity (e.g., Ghana and Nigeria)

National advisory committees, mostly public sector led (e.g., Ghana, Zambia)

Private-sector driven support services (e.g., Kenya, Rwanda, South Africa, Uganda)

Discussions to date at regional level, more political and less action-oriented (e.g., Association of African Central Banks (AACB), African Data Protection Network, African Union

Main service gaps include:

- No 24/7 security monitoring and emergency response service
- No industry-wide and regional threat information sharing
- No policy-specific advisory services
- No financial sector-specific advisory service; and no specialized services for digital financial services
- No education programs for businesses and individuals

A Proposed Business Concept

for shared cybersecurity resource centers
for the financial sector

CGAP

Strategic Plan:

Operating principles, theory of change, and market development

CGAP

Operating principles

1. **Build on and enhance existing structures, skills and technology**
2. **Work towards self-sustaining business operations**
   - Initial setup requires high capital investment; operational costs will gradually be covered by service fees
   - Phased expansion of services and customers across region(s)
3. **Offer inclusive and fair pricing of services**
   - Services and products to be accessible to financial service providers of all sizes and forms
   - Pricing of services to be competitive but also proportional to user capacity and resources
4. **Foster national and international dialogue**
   - Provide platform for dialogue, collaboration, and sharing of good practices among public and private sector actors
5. **Promote innovation and local talent development**
   - Provide platform for innovation and testing of cybersecurity solutions for the financial sector
   - Promote development and use of open source solutions for prevention, detection, and remediation of cyber incidents
   - Collaborate with universities, support educational programs, and offer Technical and Vocational Education and Training (TVET) and internship opportunities for local talent development

Theory of change

Sustained usage of (digital) financial services

- Public confidence and trust in the financial marketplace is increased and maintained.
- Customers' financial transactions and assets are protected.

- Improved cyber resilience of payment systems, financial services providers, and financial service delivery channels.

- Financial services providers and policymakers in developing countries have the resources, knowledge, and confidence to effectively prevent, detect, and respond to cyber attacks.
- Financial services providers and policymakers have effective structures and processes in place for managing cyber risks.

- Financial services providers and policymakers collaborate and exchange threat information nationally and internationally.
- Relevant, affordable, and reliable cybersecurity resources are available to financial services providers and policymakers.

Links to the Sustainable Development Goals

#4 Quality Education: Develop cyber education programs, including higher education programs; increase number of cybersecurity post graduate students who will form tomorrow's teachers; increase number of digitally-skilled people, including technical and vocational skills, relevant for employment and entrepreneurship.

#5 Gender Equality: Promote women in ICT related education and employment programs; promote equal employment and promotion opportunities; reward gender-sensitive practices through discounts and promotions.

#8 Decent Work and Economic Growth:

- Support innovation and expansion of more affordable, accessible and suitable financial services and payment systems through adequate and secure use of customer data and by reducing the cost of using digital technologies.
- Stimulate growth of micro-enterprises and SMEs in the ICT sector and the financial sector through affordable ICT and cybersecurity services.

#9 Industry, Innovation and Infrastructure

- Facilitate establishment of sustainable and resilient infrastructure by strengthening financial, technological and technical support.
- Increase access to ICT technologies and ensure that all people have access to the internet.

#16 Peace, Justice and Strong Institutions: Support building institutional trust through public-private dialogue and through supporting national institutions in building cyber resilience; support development of effective regulatory reform processes.

#17 Partnerships for the Goals: Promote public-private partnerships and collaboration at national and international levels in ICT and cybersecurity.

SDG 5 in focus: promoting gender equality

The ICT and cybersecurity sectors are among the best-paying sectors, with a high and growing demand for specialists. But there is a stark gender disparity: women represent less than 20% of the workforce.

The centers can promote gender equality and women's empowerment and contribute to reducing the ICT and cybersecurity workforce gender gap in a variety of ways:

Hiring processes: Ensure equal and fair hiring processes that promote women's participation and professional development.

Capacity building and training: Raise awareness and encourage women's participation in educational training (at secondary school, graduate and post-graduate level), through specialized outreach to women professionals and students, job fairs for women, scholarships, internship programs and technical and vocational education and training (TVET) for cybersecurity. Luxembourg's Women in Digital Empowerment (WIDE) or the CyberWayFinder programs are examples that could be expanded to or adopted in other regions.

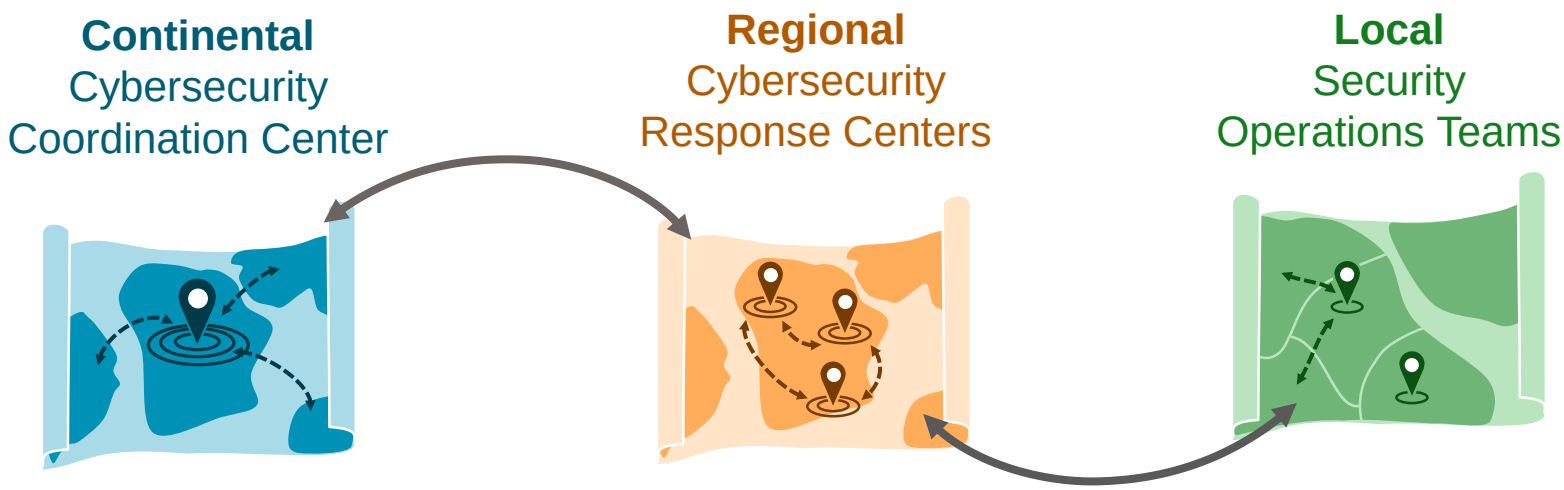
Preferential services/discounts for gender-centric FSPs: Facilitate affordable access to cybersecurity resources for providers that advance women financial inclusion (e.g., via special discounts, award programs, TA,…).

Women-led innovation: Promote women's participation in the development and design of cybersecurity services and solutions, through hackathons, innovation labs, or startup contests.

Partnerships with gender advocacy bodies: Develop partnerships with international and national development partners and advocacy bodies with focus on gender equality and women's rights.

Sources: PRNewswire (2017) "Biennial Women in Cybersecurity Report" and European Data Journalism Network (2018) "The ICT sector is booming. But are women missing out?"

Cybersecurity resource centers operate at the continental, regional and local levels



Cybersecurity resource centers have three main parts - one continental cybersecurity coordination hub, two or more regional response centers and several in-country, local security operations teams. The continental, regional and local entities may be completely separate, or in some instances combined to economize. They may also build on existing Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), but with a financial sector focus. Each entity provides a different set of complementary services, including services to each other. Together they support the financial sector to prevent, detect, respond to, and recover from cyber incidents.

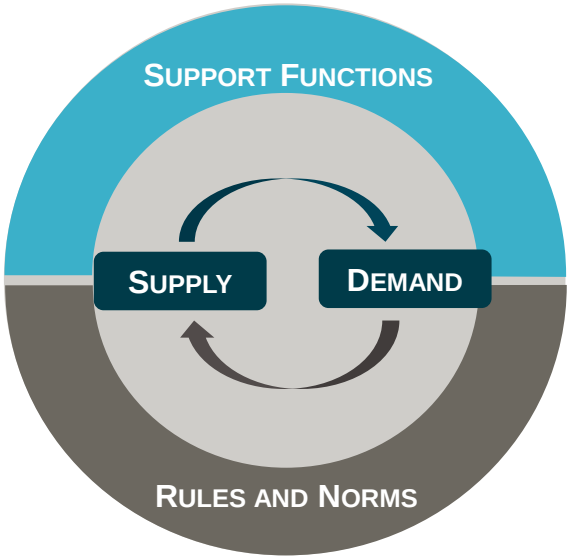
Cybersecurity resource centers can contribute to building sustainable cybersecurity markets

To address the cybersecurity resource gap effectively, interventions in the aggregate need to aim at building a robust and sustainable cybersecurity market system. A market system includes supply (service providers) and demand (users), and multiple support functions, rules and norms that influence both supply and demand of cybersecurity support services. Before choosing an intervention, existing constraints and dysfunctions in the market system have to be assessed and interventions prioritized.

Cybersecurity Market System

Market Support Functions

- Information and data
- Research and development
- Relevant software and hardware
- Capacity building
- Professional certification
- Public-private dialogue
- Sectoral dialogue
- Talent and skills development
- Global partnerships
- Public awareness campaigns



Market Rules and Norms

- Law enforcement
- Policies, regulations and guidelines (cybersecurity, IT, data protection, data localization, consumer protection, etc.)
- Industry standards
- Law enforcement
- Social norms and behaviors

Cybersecurity resource centers can address many market-level challenges, but not all

Simply creating or funding a cybersecurity support center is not enough. The centers themselves rely on market demand, access to local talent, and relevant support functions and rules in order to operate sustainably. Complementary interventions will be needed to address remaining gaps and dysfunctions in the cybersecurity market system.

Market level challenges	Mitigating measures
There might be limited demand in the target market(s) due to limited awareness and willingness to use and pay for cybersecurity services.	Demand may be influenced by working with policymakers, regulators, supervisors, and legal enforcement agencies to implement regulatory guidelines and standards that set incentives or requirements for using this type of service. Awareness campaigns and training programs will help spur demand and build users' skills to apply cybersecurity measures.
The centers rely on qualified and skilled staff to operate, which is scarce in most regions, especially in lower income countries, and skilled staff is difficult to retain.	The centers can partner with education and training institutions (universities, training institutes, professional associations, etc.) and offer vocational training and trainee programs to build local workforce skills and for professional development. Continuous on-the-job training and career opportunities will be essential for retaining employees.
The centers may compete with existing cybersecurity service providers or policy and industry initiatives with similar objectives.	The centers should complement and support existing initiatives and resources (CERTs and CSIRTs, local cybersecurity service providers, etc.) by partnering or providing services that are not yet present.
There might be resistance to collaborate and share information with other countries or regions.	The centers should leverage and partner with existing global and regional bodies that have a good standing and are perceived as neutral and acting in the interest of both the public and private sectors.
The centers may loose sight of financial inclusion and social development impact mandates.	A governance structure that includes representatives from the financial inclusion sector (funders, implementers, support organizations, etc.) will help the centers maintain focus.

Operating Plan:
Target customers and services

CGAP

Target customers

Cybersecurity resource centers will specialize in the financial sector, serving banking, insurance, payments, investment, pension and all other financial sector actors.

All financial sector providers will benefit from the services, including those serving lower income consumers:

- Threat intelligence and information sharing improved with broad participation
- Cybersecurity issues similar for small and large providers
- Broad range of users needed for centers to become self-sustaining
- Lower income consumers use services of a variety of providers, including banks, microfinance institutions, fintechs, etc., and all need the services.

Centers can promote financial inclusion by:

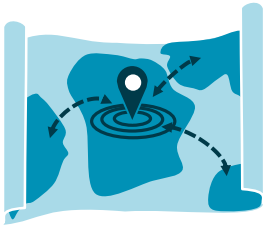
- Making cybersecurity services more affordable
- Helping providers who serve lower income consumers address the risks posed by less secure transmission channels, lower digital literacy, and limited cyber threat awareness
- Offering specialized training and information for providers serving low-income populations or newly banked.

Primary customers: Financial service providers, financial and payment system operators, financial sector regulators and supervisors, financial sector fraud and cybersecurity initiatives

Secondary customers: National and regional CERTS and CSIRTs, law enforcement agencies, service providers and public sector agencies from other sectors

Services at the continental level:

Cybersecurity Coordination Center



Services to Regional Response Centers, international and regional cybersecurity networks, policymakers, industry bodies, individual financial services and infrastructure providers, local CERTs and CSIRTS.

Strategic advisory on implementation of global standards, policies and guidelines

Research, development, and innovation in collaboration with international and local universities

Global coordination and partnerships, including convenings and working groups

Capacity building and training, including crisis simulation exercises and red teaming*

Threat intelligence management, including sharing at international and regional level

Elevated crisis management in support of regional response centers

**A 'Red Team' is a group of people authorized and organized to emulate a potential cyber attack with the objective to improve an organization's cybersecurity by demonstrating the impacts of successful attacks and what works for the defenders (i.e., the Blue Team) in an operational environment.*

Services at the regional level:

Cybersecurity Response Centers

Services to Local Security Operations Teams, local policymakers, local financial services and infrastructure providers, and possibly public and private sector actors from other sectors.

Threat information sharing
and sharing of best practices
at regional level

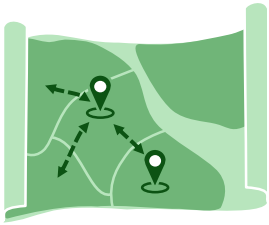
Emergency response support,
including incident analysis, forensic, remediation, recovery, crisis simulation and management, red teaming, etc.

Operational advisory,
including security strategies, policies, maturity assessment, risk management, etc.

Advanced Training Services,
including penetration testing, application security, etc.

Services at the local level:

Cybersecurity Operations Teams



Services to local policymakers, financial services and infrastructure providers, and possibly public and private sector actors from other sectors.

Security Operations Center (SOC) offering 24x7 security monitoring and detection and customer support hotline

Emergency response and crisis management for local customers

Technical advisory and support, including vulnerability scanning, support to local interventions and forensic analysis

Implementation of continental and regional advisory and threat information sharing

Public awareness campaigns and education programs

Different types of customers will need and want different types of cybersecurity services

Larger providers benefit particularly from international and regional threat information exchange, R&D, and dialogue with national, regional and international standard setting bodies.

Smaller providers benefit particularly from employee capacity building and training, system monitoring and threat detection services, vulnerability testing and sharing of best practices.

Incumbents benefit particularly from innovation challenges and hackathons.

Universities and scholars benefit from research partnerships and vocational training opportunities.

Regulators and supervisors benefit from advice on implementation of international standards, regulatory and supervisory advice, information about regional and international trends, feedback about sectorial cybersecurity maturity, and advice and support to secure their own systems.

Entire financial sector community benefits from sharing of information about cyber incidents, threats, best practices and opportunities for collaboration in research and innovation.

Customers can choose a personalized service package

Customers can access the full range of services, but can choose a set of services based on their individual risk profile, risk appetite, budget and compliance requirements. Below is an example of selected cybersecurity services that may be relevant for certain types of customers.

Service package elements (selected list of services)	**Small Customer**	**Medium Customer**	**Large Customer**
Chief Information Security Officer (CISO) as a service	✓	✓	
Support in improving basic cyber hygiene	✓	✓	
Cybersecurity awareness and training	✓	✓	✓
Incident response support	✓	✓	✓
Vulnerability assessment	✓	✓	✓
Penetration testing, application security	**(✓)**	✓	✓
Risk management framework & audit*	✓	✓	✓
24/7 security operations monitoring and supervision	**(✓)**	✓	✓
Forensic investigations		✓	✓
Crisis simulation, red teaming			✓

** Risk management framework development and review to be recommended to all customers. Yet, larger institutions may want also an ISO27001 certification.*

Services can be provided as online resource or through a one-on-one interaction (remotely or in-person)

Service	Cybersecurity service provider*	Online resource	One-on-one support**
Training	CCC, RRC	✓	✓
Threat information sharing	CCC, RRC	✓	
International and regional convenings and workshops	CCC		✓
Information on international standards & frameworks	CCC	✓	
Advisory and best practices: FAQs, news from the community, working groups, research, webinars	CCC	✓	
Awareness campaigns and simulations for employers & employees	CCC, RRC	✓	✓
Elevated emergency incident response & assistance to recovery	CCC, RRC		✓
Technical advisory: Governance, audits, maturity assessment, review of strategies and policies	RRC		✓
Forensic services	RRC, LSOT		✓
Technical assessments, penetration testing, vulnerability scanning	LSOT		✓
Emergency Incident Response & Assistance to recovery	LSOT		✓
Security supervision, log monitoring	LSOT		✓
Physical security assessments	LSOT		✓

** Continental Coordination Center (CCC), Regional Response Center (RRC), Local Security Operations Teams (LSOT)*

*** One-on-one support may be offered in person or through virtual video-conferencing and screen sharing*

Service platforms for threat information sharing and collaboration

Trust communities for threat information sharing and collaboration across the sector and across regions are key for building strong cyber resilience. Providing a platform to build trust communities is one of the most important services that the centers can offer.

There can be **closed and open trust communities** depending on decision and information sensitivity (e.g., closed communities for detailed exchange about threats among trusted peers).

Trust circles or working groups, involving a limited number of peers for highly confidential sharing of information. Individual trust circles can collaborate within a network of trust circles to share less confidential or anonymized information about trends and threats.

policymakers benefit from participating in private sector communities for transparency and early warning, but with limited and anonymized access to the threat information to protect the private sector and maintain their high trust circle.

Regular virtual and physical meetings help build trust and allow sharing of concerns and learnings.

Important to allow sufficient time to build trusted communities and/or acquire access to existing trust communities.

How to make a trust community platform more inclusive?

- Use simple language and include technical translation for less skilled participants
- Offer additional languages beyond English
- Reduced or tiered fees
- Full service spectrum, including not only detection but also support for prevention, response, and recovery
- Provide access to (automated) threat intelligence tools that are easy to adopt and integrate

Examples of existing trust communities for threat information sharing and collaboration

	The Euro Cyber Resilience Board for pan-European Financial Infrastructures	**AFI Cyber Security Working Group**	**Cybersecurity Resource Centers**	**GSMA Fraud and Security Forum**	**FS-ISAC** (Financial Sector Information Sharing and Analysis Centre)
Public or private initiative	Public (chaired by European Central Bank)	Public (owned by AFI members)	Public-private partnership	Private (owned by GSMA members)	Private (owned by financial services providers)
Footprint	Euro zone	Emerging markets	Lower income markets/region	Global	Global (50 countries)
Participants/ members	30 public agencies and financial market infrastructure (FMI)	99 financial regulators and supervisors from 88 countries	2500+ financial sector companies and public agencies*	750 mobile network operators and 400 ecosystem players	7,000 banks, investment, insurance and security firms
Services	Strategic forum for high level information sharing, sector resilience, FMI preparedness and vulnerability assessment	High level information sharing, development of policy frameworks and guidance	Platform for public and private information sharing, dialogue, R&D, capacity building and high-level advisory	High level and in-depth information sharing, assessment framework and shared standards	High level and in-depth information sharing and capacity building

** Number of participants depending on region and maturity*

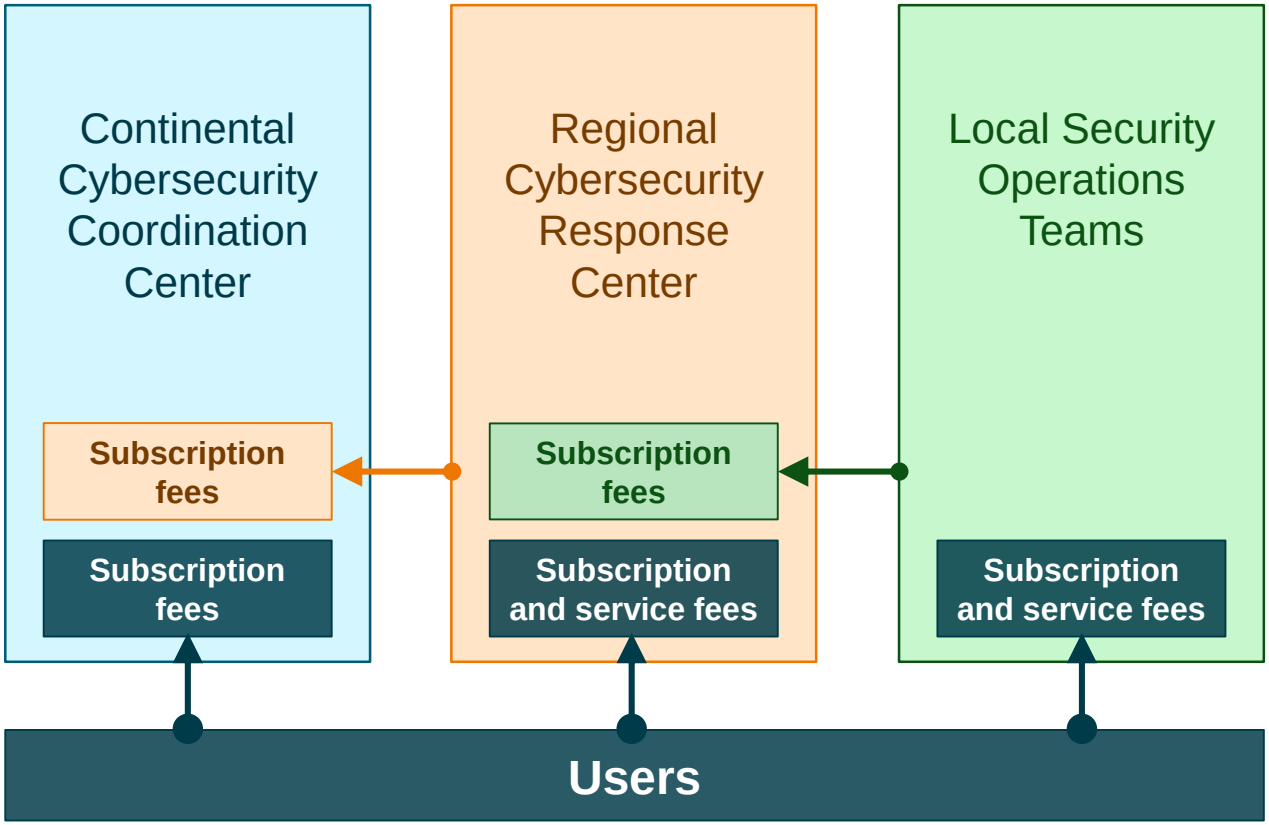
Financial Model:

Revenues, expenses and funding needs

CGAP

Sources of revenues

The main revenues will be generated from annual, or multi-month, subscription fees as well as service fees for users. Due to cross-support between the continental, regional and local entities, there will also be subscription fees between them. User fees will grow as the customer base and the range of services offered expand.



Service pricing models

Subscription fees (annual or multi-month plans)

- Subscription plans can bundle different services, including all-inclusive premium plan, advanced plan, or standard subscription plan
- Subscription fees will be most appropriate for the participation in trust circles and threat information sharing communities provided by the continental coordination center to encourage multi-month participation (important to build trust circles)
- May also be applicable for recurring technical support and vulnerability assessments

Pay-as-you-use service fees

- One-off service fee for ad-hoc technical support, training programs, etc.

Pricing matrix considering customer's transaction volumes, number of ICT assets (complexity), number of customers and sector contributory capacity

Discounts for new users, trial periods, and awards for inclusive and responsible financial services providers

Costs: Continental Coordination Center (for Years I-III)

	Opex*	Capex**
Governance & program management	• 3 Full Time Equivalent (FTE) • PPP organization constituency costs • Executive and Advisory Board meetings	
Strategic advisory	• 1 FTE + Short Term Consultants	
Capacity building and training	• 7 FTE • Large scale on-line awareness program for FSP employees • E-learning courses with partner universities • Gender action activities	• Crisis simulation room
Global and continental coordination and partnerships	• 2 FTE • Regional community conference (quarterly)	
Research, development and innovation	• 3 FTE • Scholarships for MSc and PhD students at local universities with scholarship and accommodation during research abroad	
Threat information sharing and threat analysis	• 6 FTE	• Threat intelligence platform • Advanced forensics lab

** includes training, coaching, travelling to research conferences, rent, insurance, etc.*
*** excludes office furniture, equipment and software licenses*

Costs: Regional Response Centers and Local Security Operations Teams (for Years I-III)

Regional Response Centers (costs per center)	**Opex***	**Capex****
Management	• 1 FTE	
Technical support services and training	• 2 FTE	• Training room and forensic lab
Threat sharing	• 1 FTE	• Membership/participation fee for global threat sharing networks
Research, development and innovation	• 2 PTE (interns)	• Partner university cybersecurity labs
Local Security Operation Teams (costs per team)	**Opex***	**Capex****
Business development, customer relationship management, technical support services, 24/7 monitoring	• 10-12 FTE • Open source detection software maintenance • Data center hosting	• Open source detection software industrialization for productivity and efficiency • Data center equipment

** includes training, coaching, travelling to research conferences, rent, insurance, etc.*
*** excludes office furniture, equipment and software licenses*

Cost sharing for economies of scale

Shared management

- Include multi-disciplinary expertise (business management, cybersecurity governance, forensics, technical auditors and pen-testers, …)
- One team with all required skills will be working for a number of customers, with strong confidentiality and ethical rules in place

Shared service platforms

- Powerful technical platforms need regular upgrades
- Shared software license for continental, regional, and local entities
- Shared hardware for continental coordination and regional response centers

Shared R&D and skills development

- Collaboration with local and international partners on R&D
- Build on young local talent for R&D

Shared policies and processes

- Shared data protection and security policies and processes, following international standards and guidelines

Medium-term sustainability model

Break even after 3-4 years of operation: As the centers' reputation and number of participants grow, revenues will increase and cover more and more of the operational expenses. Also, after building the base, the marginal cost of expansion will be lower due to shared capital expenses and shared infrastructure. The objective is to make the centers' operations financially sustainable in the medium term (3-5 years).

Growing user base and revenues: The customer base will grow continuously and more customers will be willing/able to subscribe, helping the centers to cover operational expenses.

Project is easily scalable: Regional response centers and local security teams have relatively simple organizational structures, procedures, and tools and can be easily replicated as "CSIRT in a box" or "Security Operations Center (SOC) in a box" as per demand.

Cybersecurity resource centers have an initial funding gap

Setup is capital intensive: establishment of physical centers, software investment needs, setup of labs and training facilities

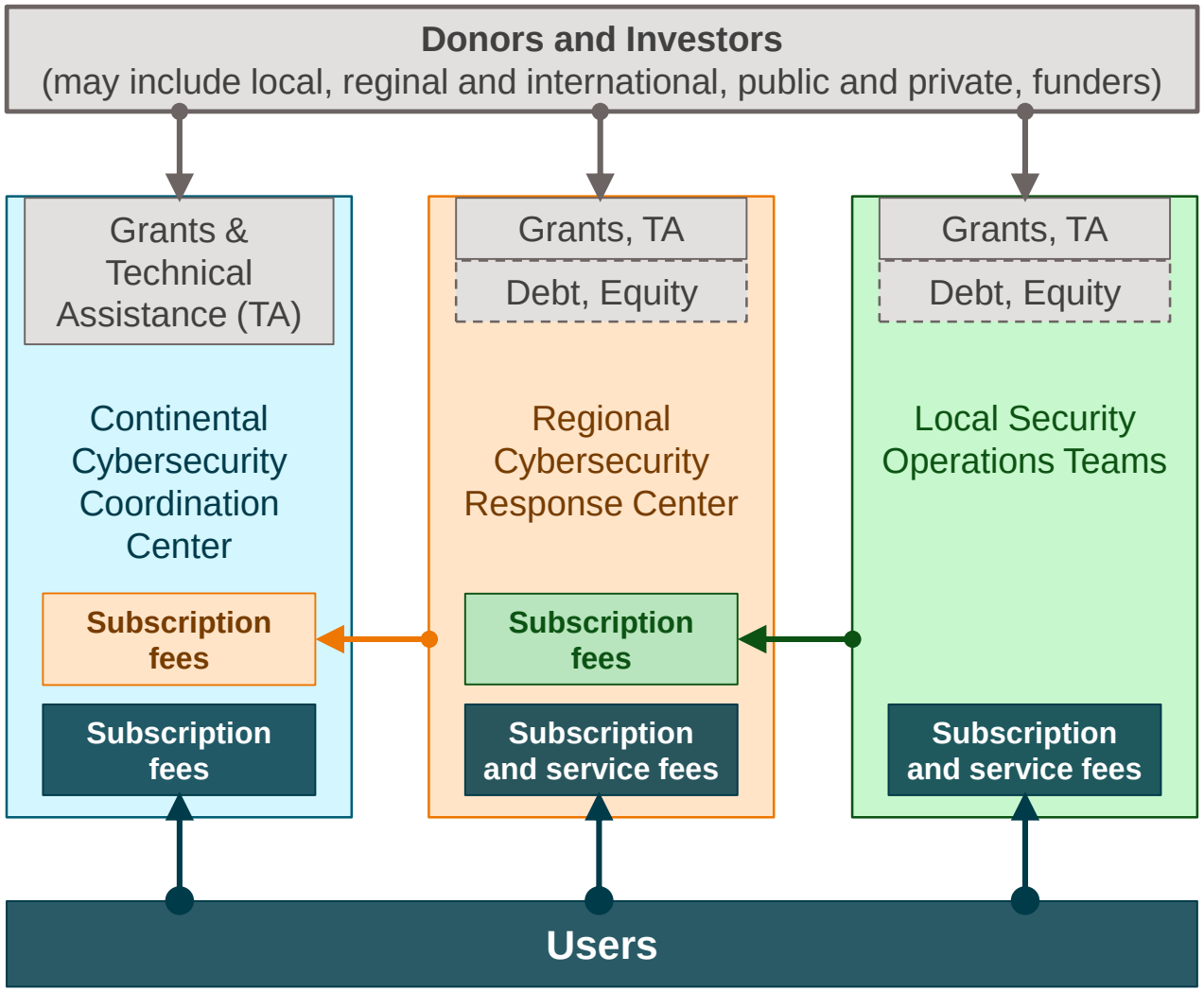
Initializing operations is capital intensive: large geographical footprint requires establishment of relationships with multiple local partners and customers through convenings and outreach activities

First years of operation require patient capital and grants:

- Time needed for awareness raising, to hire experts and build up skills, and to build trust
- Time needed to expand customer base and for services to grow profitable
- Ability to implement specialized R&D programs, e.g., to promote professional development for women, or training programs for financial service providers that target lower income segments

Setup and implementation require expert advice: implementation and monitoring of social impact agenda requires support from development experts

Possible sources of revenues and financing



Because revenues from subscription and service fees will not sufficiently cover the cybersecurity resource centers' capital investments and operational expenses during the first years of operation, financial and technical support will be needed until the centers achieve higher cost efficiency through economies of scale and scope.

Donors and investors can support with technical and financial assistance

Funding instrument	Purpose
Technical Assistance	• Facilitate dialogue and partnerships between international, regional and local partnerships • Advise on social impact and gender strategies • Advise on program management and M&E systems • Advocate for adoption of cybersecurity regulations and standards
Grants	• Cover capital investments for setup • Support education and R&D programs with local universities • Support training programs for smaller and lower capacity users to enable them to use services (e.g., participate in threat sharing) • Support creation of innovation labs and implementation of hackathons
Equity	• Support business model with low return expectations
Debt (including convertible debt)	• Support capital expenses and expansion through low-interest debt

Funding requirements are similar for each entity, but different in size

Continental Coordination Center	Regional Response Centers	Local Security Operations Teams
• Grants for setup (capex) • Grants or debt to cover operational losses during first years • TA and facilitation to build up partnerships, customer base and human resources • Equity and debt financing to help cover investment needs in medium- to long-term	• Grants for setup (capex) • Grants or debt to cover operational losses during first years • TA and facilitation to build up partnerships, customer base and human resources • Equity and debt financing to help cover investment needs in medium- to long-term	• Grants for setup (capex) • Grants or debt to cover operational losses during first years • Equity and debt financing to help cover investment needs in mid- to long-term
• Vision to break even after 4–5 years, covering opex through revenues	• Vision to break even after 3–4 years, covering opex through revenues	• Vision to break even after 2–3 years, covering opex through revenues

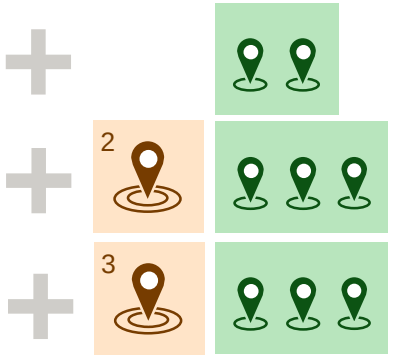
Phased scaleup of the regional structure

YEARS I-II

Build the base

- Prove business model
- Build partnerships
- Build trust circles

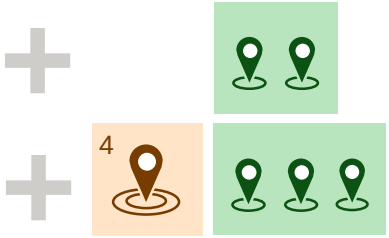
YEARS III-IV



Replicate and expand

- Optimize operations
- Expand customer base
- Strengthen and expand partnerships and trust circles

YEAR V



Optimize and break-even

- Optimize operations and reach break-even
- Expand customer base
- Strengthen and expand partnerships and trust circles

Detailed implementation and scale-up strategy

First of all, key stakeholders must be identified and crowded in on the concept. Then, international and regional partners must be identified to jointly design and implement the concept of regional cybersecurity resource centers. This can take several months, or even years.

Year I – Initiate:

- Set up continental coordination center and governance board, hire key managers and staff, build regional partnerships, start awareness and marketing campaigns, offer workshops to build trust communities, identify regional and local champions
- Develop or procure open source technology solutions
- Identify countries to establish regional response centers and local security operations teams

Year II – Roll-Out:

- Establish local security operations teams in first region
- Open first regional response center
- Expand services and customer base

Detailed implementation and scale-up strategy (ctd)

Year III – Replicate and Expand:

- Expand services and customer base
- Expand into further countries by establishing additional local security operations teams
- Open second regional response center and local security operations teams for second region

Year IV – Optimize, Replicate and Expand:

- Expand services and customer base
- Optimize operations of continental center and regional response centers
- Open third regional response center and local security operations teams for third region

Year V – Optimize and reach breakeven

- Expand services and customer base
- Optimize operations and funding needs towards self-sustainable model
- Open fourth regional response center and/or local security operations teams based on demand

Global scale-up opportunities

Start with one continent or region – as a proof of concept – and collect learnings for independent replications in other continents and regions

- Different market contexts (e.g., financial ecosystem, languages, security and risk culture, capacity, skills) require replications in other regions/continents rather than expansion to one global center
- Trust environment calls for regional rather than global solution
- However, collaboration and coordination between different regions'/continents' cybersecurity resource centers will be key, especially for information and threat sharing

Development funders and sector support organizations can help with facilitating stakeholder dialogue and collaboration for creating such centers, developing training materials and guidance notes, supporting R&D, and supporting replication and adaptation of the concept through facilitating peer exchange and study tours across regions.

Management Model:
Ownership, governance and partnerships

CGAP

Ownership and governance options

The continental, regional and local entities will need to collaborate based on a formal partnership, but they may operate as separate entities. They may be governed by public sector players, private sector players or a public-private partnership. Each option comes with advantages and disadvantages. The more technical services will benefit from private sector involvement, whilst the strategic advisory and regional coordination and collaboration will benefit from public sector and possibly multinational organizations' support.

	Purely private sector led*	**Purely public sector led**	**Public-private collaboration**
PROs	Cheaper and faster implementation; good for technical service provision	Political standing supports trust and use of services; good for policy and regional dialogue platforms	Establishes formal partnership and dialogue among public & private players; builds trust and confidence based on partnership; good for combining non-technical and technical service provision
CONs	Relies on partnerships and good standing to develop trust; usually no direct services to public sector; limited incentives to serve less developed and resource-constraint users	Relies on collaboration among multiple country governments; risk of too much regulatory and limited private sector perspective; implementation and operations may be slower due to political economy and national security issues	Establishment of partnership may require more time and possibly higher cost (e.g. for structuring a PPP)
EXAMPLES	FS-ISAC, GSMA Fraud and Security Forum, American Bankers Association Cyber & Information Security Working Group, South African Banking Risk Information Centre	AFI Cybersecurity WG	The Euro Cyber Resilience Board

** May be single private sector player or joint venture among multiple entities*

Governance model for continental cybersecurity coordination center

Cybersecurity resource centers will benefit from an inclusive and transparent governance structure that involves a variety of stakeholders.

Board of Directors

- Sets out strategic objectives and policies
- Selects, supports and reviews management performance
- Reviews and annual budgets, compensations and salaries
- Represents stakeholder interests

Members should be neutral partners from diverse stakeholder groups

Advisory Board

- Provides strategic direction
- Offers networks and expertise
- Oversees results monitoring and quality management

Membership should be inclusive of diverse stakeholder groups

Important regional and local partnerships

Partnerships with regional and local policy, industry and civil society organizations will be key for the success of the cybersecurity resource centers. Important stakeholders include:

- Policymakers and supervisors
- Existing financial fraud forums or initiatives
- Financial sector industry associations
- Cybersecurity industry bodies, CERTs and CSIRTs
  - A partnership with an established CERT or CSIRT would help the continental coordination center and regional response centers gain access to international threat intelligence networks more quickly. It requires time (a year or more) to be recognized as a peer among participants of an established threat sharing community.
- Consumer advocacy groups and civil society
- Academia, universities and higher education facilities

Important global partnerships*

Type of partner	Examples	
Research institutions, think tanks	• Carnegie Endowment for International Peace • Center for Financial Inclusion, SmartCampaign	• CGAP • Social Performance Task Force
Education institutions	• Carnegie Melon University • Columbia Business School's DFS Observatory	• University of Israel • University of Luxembourg SnT
Capacity building institutions	• Toronto Center • United States Telecommunication Training Institute	• International Monetary Fund • ISACA • Global Forum on Cyber Expertise
E-learning providers	• Gateway Academy • Digital Financial Inclusion Institute	
Industry bodies and initiatives	• GSMA • World Economic Forum's Global Center for Cybersecurity and Cybersecurity Consortium for Financial Services • Financial Inclusion Global Initiative	• International Telecommunications Union • Regional and international industry associations and networks (e.g. microfinance networks, FinTech associations, banking associations)
Global policy making bodies and associations	• Alliance for Financial Inclusion • European Central Bank • Global Financial Sector Standard Setting Bodies (e.g., BIS, FSB, CPMI) • OECD Consumer Protection Task Force	• Global Partnership for Financial Inclusion • Regional Convening Bodies and Economic Unions (e.g., African Union)
Funders and development initiatives	• UN Programs and Agencies • Regional Development Banks • Bilateral Development Funders	• Multi-lateral development funders • Development Finance Institutions • Private Foundations/ Philanthropies
Others	• FS-ISAC and other finance oriented ISACs or CERTs	• Local CERTs and CSIRTS • Law enforcement agencies

**This is not a comprehensive list. Partnerships need to be identified and prioritized for each context.*

Exemplary Business Plan

How to set up a pan-African cybersecurity resource center for Africa's financial sector

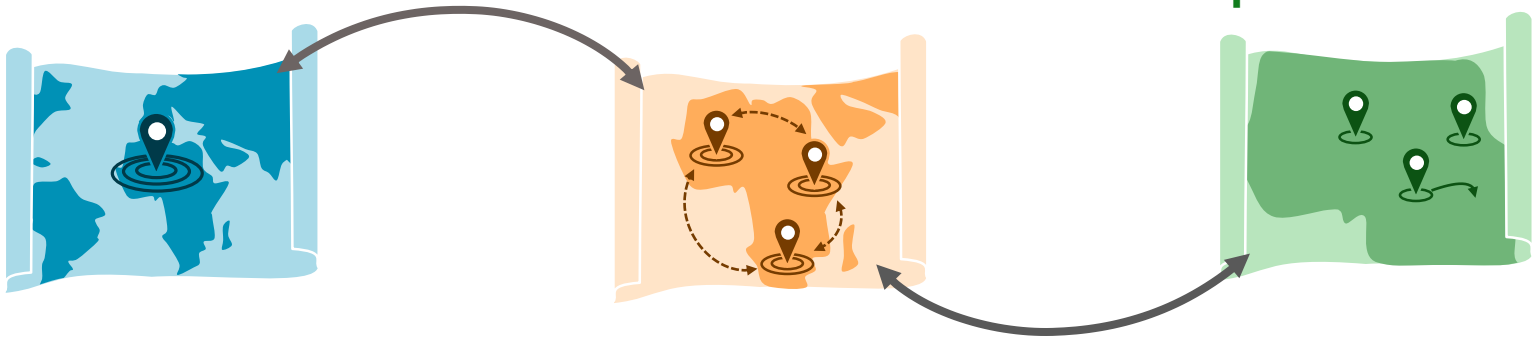
CGAP

A pan-African cybersecurity resource center would cover West, Central and East Africa

Pan-African Coordination Center**

Regional Response Centers

In-country Security Operations Teams



Research studies show that Africa's financial sectors are challenged by a growing number of cyber threats, for which they are weakly prepared. Due to scarce cybersecurity resources, the region would greatly benefit from a pan-African cybersecurity resource center. There could be a cybersecurity response center for each region, i.e., West Africa, Central Africa, East Africa, Southern Africa, Northern Africa; but initially, some may share a center. The pan-African center could be hosted by one of the regional response centers. Some in-country teams may provide services to neighboring countries that have too little demand to justify having their own security operations team. The structure could be expanded with additional regional response centers or in-country security operations teams to address the needs of diverse financial sector contexts and languages. The centers would build on and strengthen existing structures, where available.

Expected service reach across Sub-Saharan Africa

A consortium of cybersecurity experts from Luxembourg developed a business plan for a pan-African cybersecurity resource center, based on a number of assumptions, including the following:

	3 Years	5 Years
Countries covered (out of 46)	20	40
Nb. of continental coordination centers	1	1
Nb. of regional response centers	2–3	3–4
Nb. of local security operations teams	3–4	4–7
Nb. of employees	86	110
Nb. of customers served (FSPs, central banks, etc.)*	300	600
Nb. of information sharing community participants*	200	400
Nb. of financial sector employees trained (accumulated)	30,000	50,000
Financial consumers benefiting from improved cyber protection	20m	50m

** See following slides for more detailed information*

Expected cybersecurity service customers

The expected number of customers for the an-African center is based on an assumed reach of 25% of public and private financial sector actors in Sub-Saharan Africa.

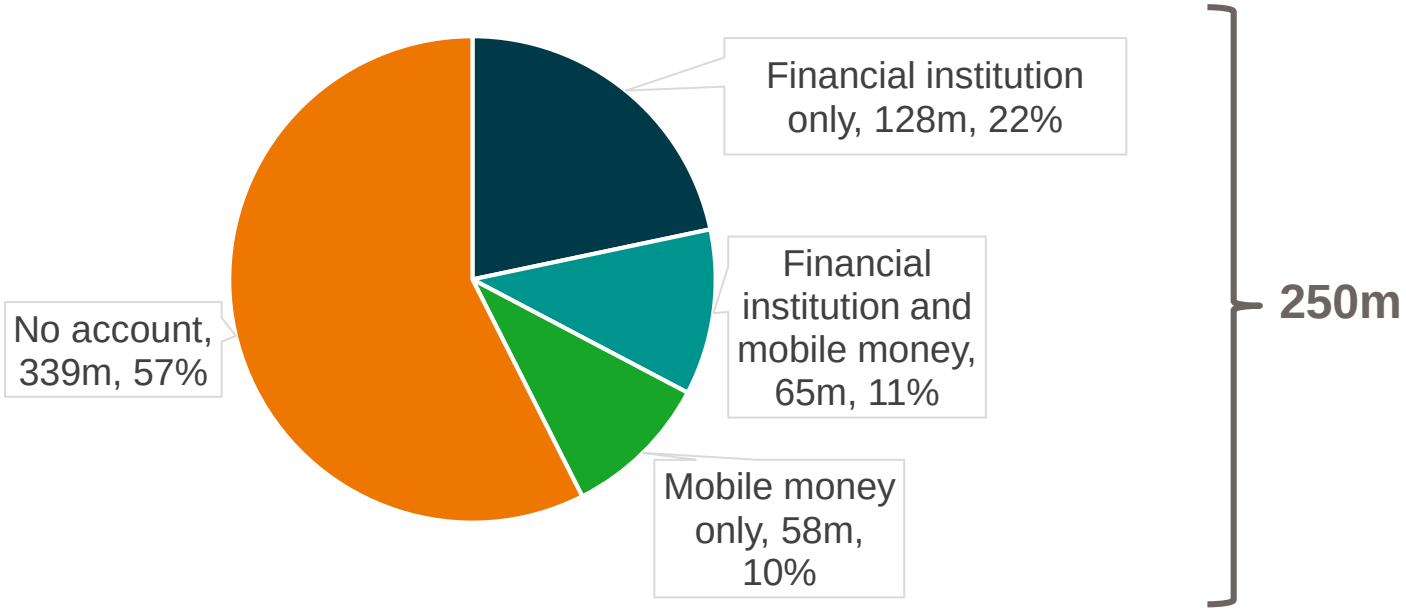
Financial sector user base	Average per country	Sub-Saharan Africa (48 countries)	Envisioned reach of Pan-African Center by Year V
Banks	15	720	180
Microfinance institutions, savings and loans companies, credit unions, SACCOs, cooperatives, etc.	15	720	150
Insurance providers (incl. microinsurance providers)	10	480	135
Mobile money providers and fintech companies	5	240	60
Financial infrastructure providers (e.g., payment schemes, settlement systems)	4	190	40
Central banks	1	41	35
TOTAL	50	2391	600

Thanks to the use of the Pan-African Cybersecurity Resource Center's services, users would be able to reduce their cyber incident detection time from currently 200 days to less than 1 day.

Potential impact on financial consumers

In Sub-Saharan Africa, around 250 million of adults (43% of total adult population) have access to an account. The objective is to reach at least 20% of Africa's financial consumers, i.e. 50 million, who can benefit from more secure financial transactions and better protection of their financial assets and personal data.

Financial access among adult population in SSA



Source: World Bank Global Findex Data of 2017

Potential human capital development impact

Development of cybersecurity and IT professionals

- 50 Master and PhD Graduates, including at least 15 women
- PhD students to become next generation of IT and cybersecurity professors
- Target for Year III: 30 MSc + 6 PhD
- Target for Year V: 50 MSc + 12 PhD

Collaborative cyber-innovation labs

Partnerships with universities for joint R&D activities, including for example:

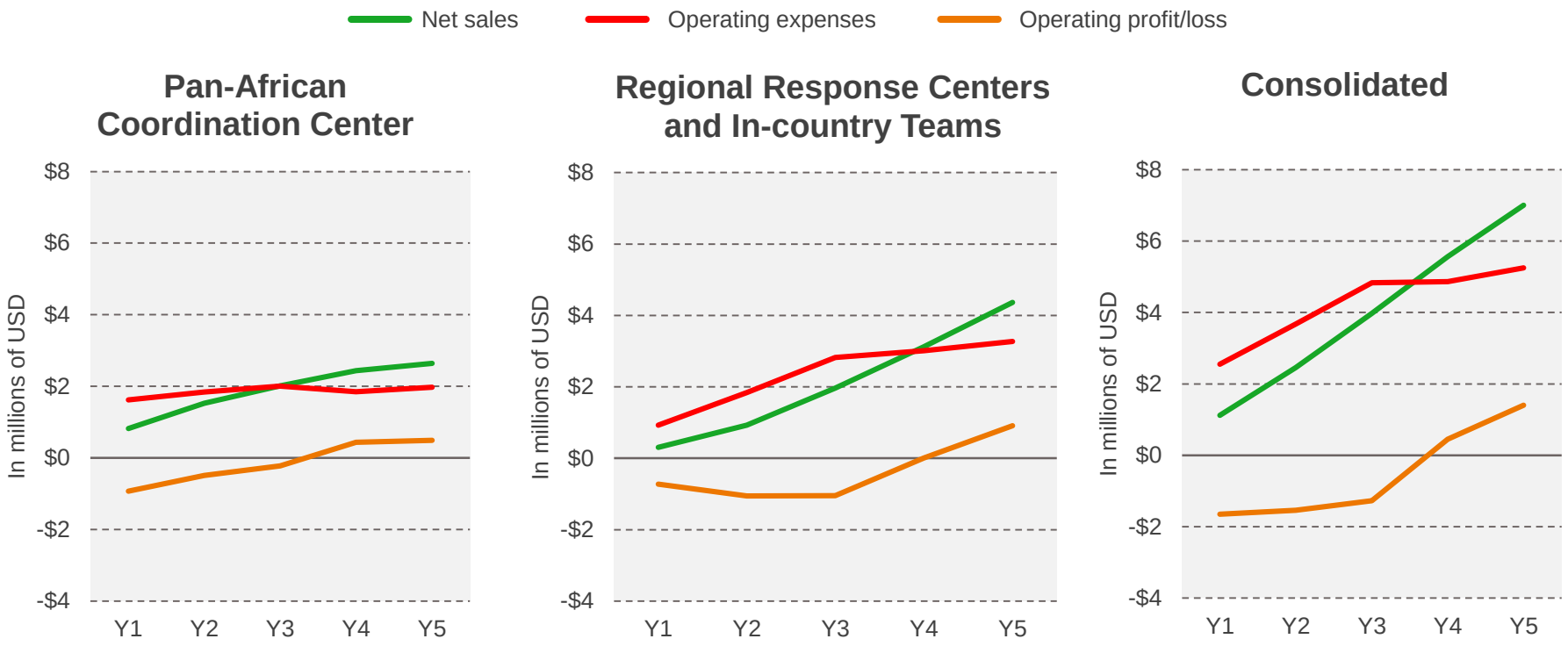
- Carnegie Mellon University Africa in Rwanda
- United States International University-Africa in Kenya
- Université Cheikh Anta Diop de Dakar in Senegal
- University of Ouagadougou

Job creation

129 new jobs created, including 35% female professionals

- Target for Year III: 83 new jobs
- Target for Year IV: 129 new jobs

Expected profits and losses over years I-V



Expected breakeven by Year IV

- Progressive expansion (capital investments) based on financial viability; additional in-country security operations teams to be added once existing ones break even.
- Additional revenues foreseeable from customers with higher purchasing power (incl. other sectors) or financial sector customers from other regions (e.g., international networks with affiliates abroad)

Budget estimates for Years I-V

The business plan expects total capital expenses of US $1.8 million, operating expenses of US $21.8 million, working capital requirements of US $1.5 million, and revenues of US $20.7 million over the first five years.

	Year I *in USD*	Year II *in USD*	Year III *in USD*	Year IV *in USD*	Year V *in USD*	Years I - III *in USD*	Years I - V *in USD*
PAN AFRICAN COORDINATION CENTRE							
Net Sales	$ 818,000	$ 1,529,000	$ 2,010,000	$ 2,650,000	$ 3,010,000	$ 4,357,000	$ 10,017,000
Cost of Goods Sold	$ (12,600)	$ (26,600)	$ (40,600)	$ (40,600)	$ (40,600)	$ (79,800)	$ (161,000)
Operating Expenses	$ (1,621,918)	$ (1,838,702)	$ (2,005,010)	$ (2,131,474)	$ (2,304,138)	$ (5,465,630)	$ (9,901,242)
Depreciation and amortization	$ (112,900)	$ (151,133)	$ (189,367)	$ (109,367)	$ (131,067)	$ (453,400)	$ (693,833)
EBIT	$ (929,418)	$ (487,435)	$ (224,977)	$ 368,559	$ 534,195	$ (1,641,830)	$ (739,075)
REGIONAL RESPONSE & IN-COUNTRY SECURITY OPERATIONS							
Net Sales	$ 304,800	$ 924,000	$ 1,965,600	$ 3,124,800	$ 4,365,600	$ 3,194,400	$ 10,684,800
Cost of Goods Sold	-	-	-	-	-	-	-
Operating Expenses	$ (925,640)	$ (1,836,280)	$ (2,826,720)	$ (3,012,444)	$ (3,272,516)	$ (5,588,640)	$ (11,873,600)
Depreciation and amortization	$ (100,500)	$ (139,433)	$ (183,467)	$ (102,633)	$ (182,734)	$ (423,400)	$ (708,767)
EBIT	$ (721,340)	$ (1,051,713)	$ (1,044,587)	$ 9,723	$ 910,350	$ (2,817,640)	$ (1,897,567)
CONSOLIDATED							
Net Sales	$ 1,122,800	$ 2,453,000	$ 3,975,600	$ 5,774,800	$ 7,375,600	$ 7,551,400	$ 20,701,800
Cost of Goods Sold	$ (12,600)	$ (26,600)	$ (40,600)	$ (40,600)	$ (40,600)	$ (79,800)	$ (161,000)
Operating Expenses	$ (2,547,558)	$ (3,674,982)	$ (4,831,730)	$ (5,143,918)	$ (5,576,654)	$ (11,054,270)	$ (21,774,842)
Depreciation and amortization	$ (213,400)	$ (290,567)	$ (372,833)	$ (212,000)	$ (313,800)	$ (876,800)	$ (1,402,600)
EBIT	$ (1,650,758)	$ (1,539,149)	$ (1,269,563)	$ 378,282	$ 1,444,546	**$ (4,459,470)**	**$ (2,636,642)**

EBIT: Earnings Before Interest and Taxes

Expected funding needs for Years I-III

Based on the expected capital requirements, operating expenses, working capital requirements and expected revenues, there would be a funding gap of around US $7-8 million.

Center setup will likely require support with facilitating stakeholder dialogue, crowding in public and private sector actors and setting up partnerships.

Center setup and first 3 years of operation will likely require around US $6 million investment.

Long-term operations and continued innovation will likely require equity and debt financing from local, regional and international investors. This may include public finance.

Support and implementation of graduate education programs, R&D and hackathons could be supported through dedicated funding and partnerships.

Stay connected with CGAP

www.cgap.org

@CGAP

Facebook

LinkedIn


IFAD
Investing in rural people


AFD


Federal Ministry
for Economic Cooperation
and Development


UDENRIGSMINISTERIET
MINISTRY OF FOREIGN AFFAIRS OF DENMARK


UKaid
from the British people


Ministry of Foreign Affairs of the
Netherlands


Global Affairs
Canada


Norad


BILL & MELINDA
GATES foundation


Sida


UNCDF


CREDIT SUISSE


CDC
Investment works


THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG


FMO
Entrepreneurial
Development
Bank


KFW


MetLifeFoundation


KOICA
Korea International
Cooperation Agency


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Agency for Development
and Cooperation SDC


JOA
JERSEY OVERSEAS AID


Australian Government
Department of Foreign Affairs and Trade


giz


USAID
FROM THE AMERICAN PEOPLE


flourish


IDB | LAB


UNDP


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP


Ministry of Foreign Affairs
and International Cooperation


IFC | International
Finance Corporation


AGENZIA ITALIANA
PER LA COOPERAZIONE
ALLO SVILUPPO


mastercard
foundation


European
Investment
Bank


npm
platform for
inclusive finance


IFU
INVESTMENT FUND FOR
DEVELOPING COUNTRIES