ACRC
Africa Cybersecurity Resource Centre

Africa Cybersecurity Resource Centre for Financial Inclusion (ACRC)

Séminaire FRATEL Brazzaville 23 Mai 2022

LUXEMBOURG AID & DEVELOPMENT

AFRICAN DEVELOPMENT BANK GROUP
GROUPE DE LA BANQUE AFRICAINE DE DÉVELOPPEMENT

adfi
Africa Digital Financial Inclusion Facility

Sommaire

Sources : Verizon, IBM, Banque mondiale

Contexte Le secteur financier africain et l'inclusion financière sont fortement exposés à la cyber-(in)sécurité

ACRC
Africa Cybersecurity Resource Centre

MENACES GLOBALES

86%
motivation financière

55%
crime organisé

70%
externe

280 jours
de la détection à l'endiguement

SECTEUR FINANCIER AFRICAIN

3 000 institutions financières et fintech, **42** banques centrales

>250 mio
clients fragiles

78 % des régulateurs citent la cybersécurité dans les 3 risques majeurs

71 % des responsables des risques citent la cybersécurité dans les 2 risques majeurs

RESSOURCES CYBER LIMITÉES

10.000 experts en Afrique contre 700.000 aux USA

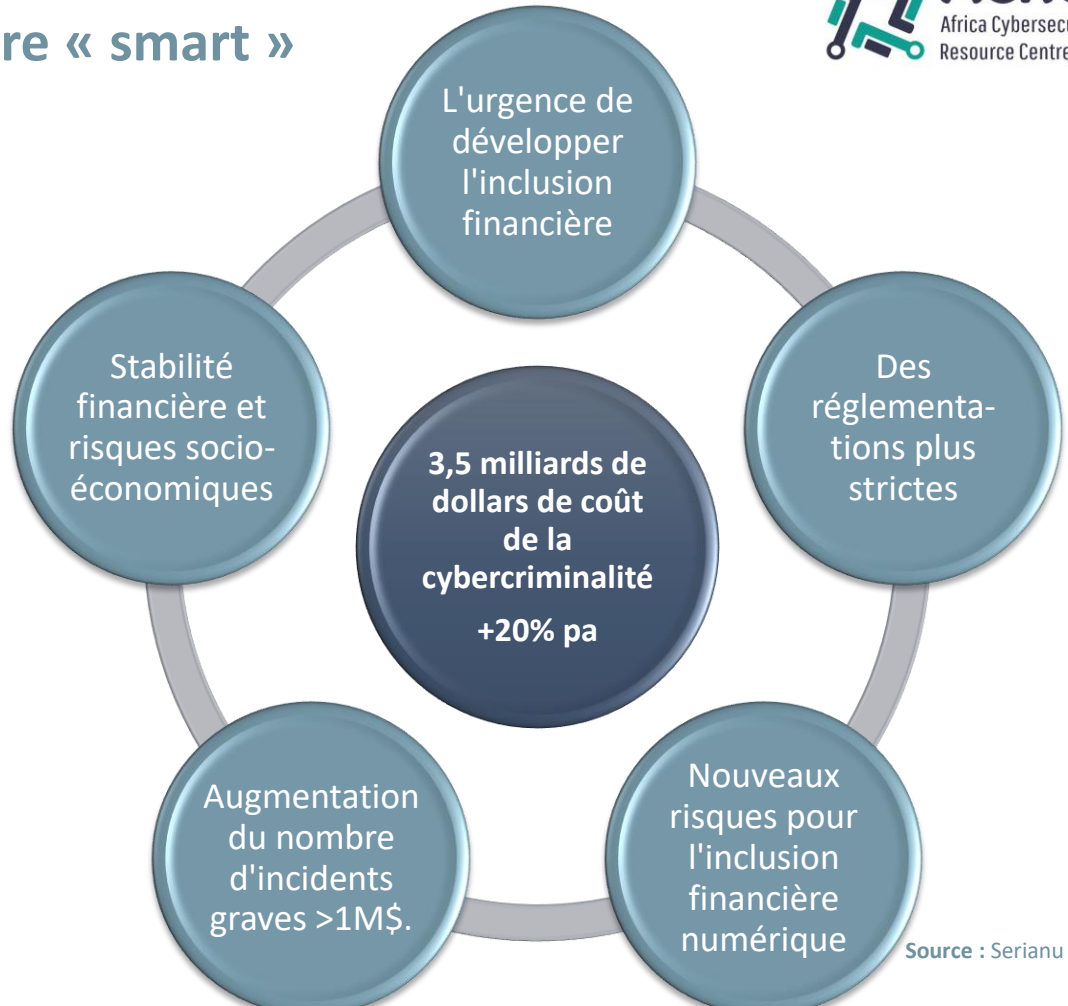
1,5 Md $= dépenses de cybersécurité des 4 premières banques américaines

14/54 pays dotés d'agences nationales de cybersécurité

0 données et coordination embryonnaire

Sources : Verizon, IBM, Banque Mondiale

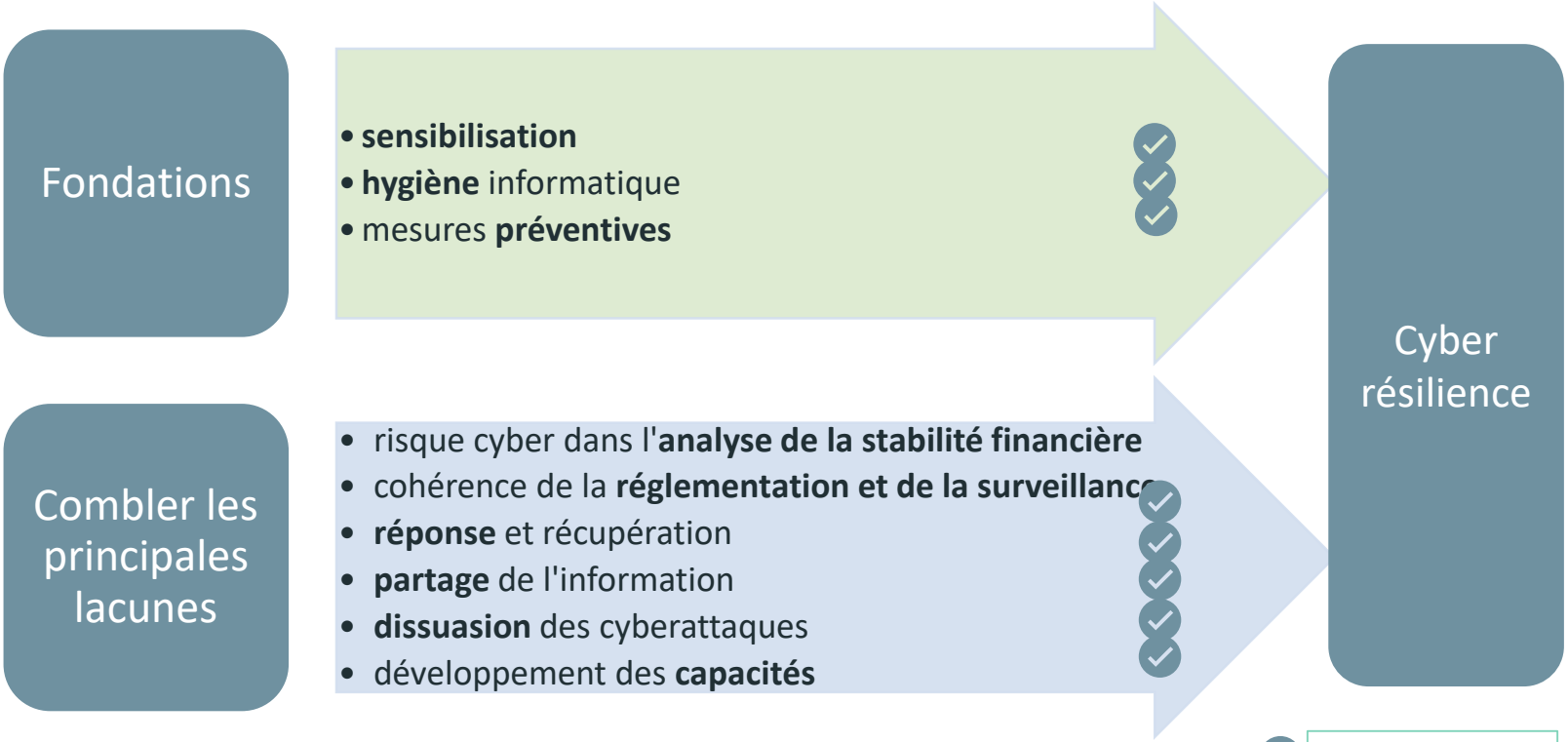
Le problème : le secteur doit renforcer radicalement la cyber-résilience de manière « smart »



Source : Serianu 2017

La **cyber-résilience** pour réduire considérablement le cyber-risque et contribuer à la stabilité financière (*)

ACRC
Africa Cybersecurity Resource Centre



(*) FMI, décembre 2020 *"Cyber Risk and Financial Stability : It's a Small World After All".*

Empreinte ACRC

Evolution de la règlementation
Exemple de la COBAC pour l'Afrique de l'Est

ACRC
Africa Cybersecurity Resource Centre

Directive Commission Bancaire de l'Afrique Centrale du 21/01/2022
Tous établissements de crédit, de microfinance et de paiement de la CEMAC
Délai **30/06/2022**
Sanctions

La situation
« Plusieurs cyberattaques ces derniers mois de plus en plus sophistiquées, avec le plus souvent des complicités internes, entrainant des pertes financières considérables susceptibles vue leur ampleur et leur récurrence de **mettre en péril la stabilité de notre système bancaire et financier »**
« Ces actes criminels résultent très souvent de la négligence et/ou de la mauvaise application des règles élémentaires en matière de sécurité informatique »

« Recommandations »
Audit organisationnel
Tests d'intrusion interne et externe réguliers
Politique de sécurité conforme ISO 27001 + Certification PCI DSS (si cartes bancaires)
Sensibilisation du personnel
Partage de renseignement sur la sécurité informatique **Comment ?**
Plan de continuité d'activité
Déclaration des incidents, mode opératoire, pertes

COMMISSION BANCAIRE DE L'AFRIQUE CENTRALE
Secrétariat Général
Avenue Jean Paul II
Boîte Postale 2-3-99 – Libreville
République Gabonaise
Tél. (241) 01 74 49 47

Libreville, le 21 JAN. 2022

Madame, Monsieur le Directeur Général

A tous les établissements de crédit, de microfinance et de paiement de la CEMAC

LC-COB/ clq.

Objet : *Renforcement du dispositif de maîtrise des risques informatiques (sécurité des systèmes d'information et cybersécurité).*

Madame, Monsieur le Directeur Général,

La crise sanitaire du Covid-19 a eu un impact sur le secteur bancaire et financier. Les restrictions des déplacements et les mesures de distanciation ont amené les établissements de crédit et de microfinance à accélérer leur plan de transformation digitale élaboré d'une part à la faveur du règlement n°04/18/CEMAC/UMAC/COBAC relatif aux services de paiement dans la CEMAC, et d'autre part pour mieux répondre à l'évolution des attentes du marché.

Bien que ces évolutions technologiques et les dispositions réglementaires mis en place par la COBAC permettent de réduire certains risques opérationnels, notamment les risques d'erreurs d'exécution, l'expansion des réseaux et des technologies, l'ouverture des systèmes d'information aux échanges extérieurs et la croissance des transactions électroniques, contribuent à accroitre de façon substantielle les risques liés à la cybercriminalité. Les établissements de crédit et de microfinance y sont particulièrement exposés avec le développement soutenu de la dématérialisation de leurs produits et services bancaires qu'ils rendent accessibles *via* leur site internet et les applications mobiles.

Je constate que les établissements de crédit et de microfinance de la CEMAC ont, ces derniers mois, fait l'objet de plusieurs cyberattaques de plus en plus sophistiquées, avec le plus souvent des complicités internes, entrainant des pertes financières considérables. Celles-ci, vu leur ampleur et leur récurrence, sont susceptibles de mettre en péril la stabilité de notre système bancaire et financier.

ACRC un projet et une équipe pour construire une organisation africaine

Consortium en partenariat public-privé à but non lucratif

Équipe pluridisciplinaire expérimentée avec >400 experts

SECURITYMADEIN.LU: Agence de Cyber sécurité du Ministère de l'Economie du Luxembourg (35 experts), CERT CIRCL, MISP Malware Information Sharing Platform

SnT/UNIversité de Luxembourg: Interdisciplinary Centre for Security, Reliability and Trust, une priorité stratégique de recherche en cyber sécurité (>200 chercheurs)

Excellium Group : Leader de la cybersécurité au Luxembourg (>150 experts), CERT.XLM, SOC, Groupe Thalès (2.500 experts)

Suricate Solutions: Partenaire Excellium, leader cybersécurité en Afrique Ouest, 1er SOC de la sous-région depuis 2016 à Dakar, solide expérience en inclusion financière et opérateurs critiques (>15 experts)

Objectifs et approche de ACRC

ACRC
Africa Cybersecurity Resource Centre

Objectifs

Améliorer la cyber-résilience des institutions d'inclusion financière et protéger les clients contre les cyber-attaques.

- favoriser l'inclusion financière
- assurer le développement des services financiers numériques
- permettre la mise en place de systèmes de paiement interopérables

Approche

Sectorielle
cybersécurité pour le secteur financier africain

Régionale
Effet d'échelle et contribuer à la durabilité, à la qualité et au délai de mise sur le marché

Évolutif et durable
construire un écosystème durable et le répliquer sur tout le continent, composants open source

Inclusive
desservir les institutions de microfinance rurales de niveau III aux réseaux bancaires internationaux et aux banques centrales

Indépendance et éthique
pour des échanges de confiance entre pairs, de l'agilité et de la cohérence

Collaborative
avec les partenaires et les autorités locales, internationales et multilatérales

Qualité
services de classe mondiale, à des coûts abordables, mutualisation

Le capital humain est essentiel
>100 experts sur 3 sites en 3-5 ans, programmes de MSc, PhD, initiatives pour

Écosystème ouvert et cohérent

Composants et organisation

"Services de base“ bien public

au service de la cybersécurité de la communauté financière africaine

Partenariats catalyseurs et synergiques

Associations professionnelles, universités, organisations multilatérales, les initiatives relatives à l'écart entre les sexes ou les hackathons, les forces de l’ordre, les autorités, les donateurs, les prestataires de services, etc.

Un réseau de proximité de partenaires commerciaux de référence dans les sous-régions

- Réponse aux incidents (CSIRT)
- Surveillance de la sécurité (SOC)
- Autres services commerciaux

Déploiement ACRC
Premières étapes

ACRC
Africa Cybersecurity Resource Centre

1er Financement ADFI Africa Digital Financial Inclusion Facility (BAD)

AFRICAN DEVELOPMENT BANK GROUP
GROUPE DE LA BANQUE AFRICAINE DE DÉVELOPPEMENT

adfi
Africa Digital Financial Inclusion Facility

donateurs

BILL & MELINDA GATES foundation

AFD
AGENCE FRANÇAISE DE DÉVELOPPEMENT

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE LA RELANCE

THE GOVERNMENT OF THE GRAND-DUCHY OF LUXEMBOURG
Ministry of Finance

Mobilisation des parties prenantes

- **Approche partenariale** avec des réseaux internationaux, banques centrales, des associations professionnelles locales / régionales / internationales de banques / microfinance / fintech, GSMA, des organisations multilatérales (FMI, Banque mondiale, Interpol, Alliance for Financial Inclusion, Association africaine des banquiers centraux, Union postale universelle)…
- **11 événements et plus de 1000 personnes sensibilisées** (Infine, ADA/SAM, Boulder Institute of Microfinance, Accion, Digital Frontiers Institute, Banque Européenne d'Investissements, Paris Peace Forum, Lhoft, projet UE OCWAR-C, …)

Embauche et formation d'experts

Afrique de l'Ouest et de l'Est (15 immédiatement, # 33 en Y3, # 109 en Y5)

Déploiement sous-régional progressif

Selon financement, services disponibles à partir du Sénégal dans l'intervalle

	Sénégal (Fr)	Afrique de l'Est (En)	Afrique de l'Ouest (En)
Étape 1 ADFI	ACRC Suricate		
Étape 2			
Étape 3			

Déploiement ACRC
"African Finance Cybersecurity Conference 2021"

Conférence annuelle sur le partage de l'information, la recherche et l'éducation

Kigali, 20-22 octobre 2021

60 participants sur place (restrictions Covid-19) et 140 inscriptions en ligne

Secteur public et privé : Fonds Monétaire international, Interpol, GSMA, Alliance for Financial Inclusion, Global Forum on Cyber-Expertise, CyberPeace Institute, CERT Mauritius, South Africa Bank Risk Information Centre, Africa Fintech Forum, Rwanda National Cyber Security Agency, équipe ACRC…

6 banques centrales couvrant 13 pays : Rwanda, Burundi, Afrique du Sud, Union monétaire ouest-africaine, Kenya, Tanzanie.

Principales banques et institutions de microfinance mondiales, internationales ou régionales, fintech et telcos.

11 Universités d'Afrique, d'Europe et des USA

13 pays africains, 6 d'autres continents

Déploiement ACRC
Services

Proposer une gamme complète de 50 services (annexe)

Inclusif, abordable, adapté et packagé pour les spécificités (taille, ressources humaines et financières, maturité en matière de cybersécurité, international/local...).

Lancement de 2 packs dédiés à la cybersécurité Micro finance/PME et Fintech

Favoriser la collaboration avec les associations professionnelles, les investisseurs et l'ACRC sur la sensibilisation à la cybersécurité, l'évaluation, les feuilles de route adaptées et le renforcement des capacités.

Développer la recherche, le réseau et le renforcement des capacités

- Préparer un document de recherche sur les **CBDC** (monnaies numériques des banques centrales).
- Établir un réseau continental de **Honeypots** pour identifier les nouvelles menaces
- **Élaborer le concept d'une organisation massive de renforcement des capacités pour les superviseurs et les régulateurs (finance, télécommunication, confidentialité des données).**

Conclusion Une approche plus intelligente pour suivre le rythme des criminels et accroître la cyber-résilience est possible

- **Partager les meilleures pratiques internationales de collaboration et de partage d'informations**, des services adaptés pour le secteur financier africain
- Intégrer des **partenariats public-privé** pour renforcer **l'écosystème** et réussir dans la durée
- Approche **sectorielle et régionale** pour réduire le temps de mise en œuvre et économiser de l'argent pour les secteurs critiques
- Compléter par une **collaboration intersectorielle** télécoms – secteur financier

Rejoignez cette communauté dès à présent !

BUILDING THE AFRICAN FINANCE CYBERSECURITY COMMUNITY #TOGETHER

ACRC
Africa Cybersecurity Resource Centre

Our partners:
ADFI is financed by:
Consortium members:

www.cyber4africa.org

Merci.

Jean-Louis PERRIER
Directeur du programme ACRC
jlperrier@cyber4africa.org

Plus d'informations
www.cyber4africa.org
www.adfi.org

Annexes: les services

ACRC
Africa Cybersecurity Resource Centre

Sources : Verizon, IBM, Banque mondiale

1x Centre régional de l'ACRC

Une approche holistique pour favoriser la cyber-résilience à grande échelle

ACRC
Africa Cybersecurity Resource Centre

Centre de partage et d'analyse des informations (ISAC)	• Plateforme de **partage d'informations** sur les logiciels malveillants (MISP) • **Interconnexion avec ISAC internationaux** (FS-ISAC, BCE, Interpol, ...) et les CERT. • Analyse et partage d' informations sur **menaces, vulnérabilités, bonnes pratiques** • **Gestion de crise** de haut niveau, exercices de simulation de crise
Coordination et partenariats	• Relations avec les parties prenantes et les partenaires au sein de l'écosystème • Conférences de partage de renseignements, groupes de travail, événements
Renforcement de Capacité	• **Sensibilisation**, **formation**, création de contenu avancé • Sessions sur site et en ligne • Contenu des événements et des initiatives transversales : Code Hackademy, hackathons, programmes de réduction de l'écart entre les sexes.
Recherche, développement et innovation	• **Partenariats académiques** • Éducation : **former des formateurs (doctorants) et des étudiants (MSc)** • R&D pour des clients publics ou privés • Diffuser les résultats de la R&D (conférences de recherche, articles, bulletin d'infor.)
Conseil stratégique et réglementaire	• Services de conseil aux **superviseurs et régulateurs** • Soutenir la definition et la mise en place de **réglementations "Smart"** • Initiatives à l'échelle du **pays ou du secteur** (par exemple, sensibilisation)

3x Centres sous-régionaux

Réseau de partenaires privés pour la proximité

ACRC
Africa Cybersecurity Resource Centre

Centre de Réponse aux incidents (CSIRT)	• Préparation et gestion de la réponse aux incidents • Gestion de crise • Investigations forensiques • Soutien de niveau 3 du C-SOC
Centre des opérations de sécurité (SOC)	• Supervision de la sécurité 24x7x365 pour identifier les attaques • Tests de pénétration et analyse de vulnérabilité
Services de conseil et formation	• Gouvernance (évaluation de la maturité, ISO 27k, PCI DSS, continuité des activités, gestion des risques...) • Formation commerciale et formation à la certification sur site
Autres services de cybersécurité	• Sur demande