# Cybersecurity for the Inclusive Finance Sector, during COVID-19 and beyond

SPTF
Promoting standards & practices
for responsible inclusive finance

the smart campaign

Suricate Solutions
Security & Payments

*30 April 2020*

*Speakers: Jean-Louis PERRIER (Suricate); Isabelle BARRES (Smart Campaign), Amelia GREENBERG (SPTF)*

# Agenda

- Welcome and introductions (5 minutes).
- Cybersecurity for FSPs: guidance from Suricate Solutions (40 minutes)
- Cybersecurity and client protection: guidance from Smart Campaign (10 minutes)
- Conclusion (5 minutes)

# Meet your speakers

- Amelia GREENBERG, Directrice Adjointe de la **SPTF**
- Jean-Louis PERRIER, Co-fondateur et Associé**, Suricate Solutions**
- Isabelle Barres, VP Directrice de la **Smart Campaign @ CFI**

# Responsible Inclusive Finance Facility for Sub-Saharan Africa and the Middle East / North Africa (RIFF-SSA/MENA)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

LUXEMBOURG
AID & DEVELOPMENT

AFD

- Offers introductory and specialized trainings for FSPs and others on consumer protection, responsible finance, and DFS.
- Makes co-financing grants to FSPs to carry out assessments, upgrade projects, and certifications or ratings.
- Governed by a steering committee that typically meets quarterly, but in this time of pandemic reviews cases virtually and makes decisions within two weeks
- Co-financing is up to 50% (normally) or up to 80% (for COVID-related projects)

Download applications: **https://sptf.info/resources/riff-ssa-mena**

# Safer remote working: Ten basic cyber security practices during CoVid-19, and beyond...

JEAN-LOUIS PERRIER, CO-FOUNDER & ASSOCIATE, SURICATE SOLUTIONS

Suricate Solutions
Security & Payments

APRIL 30, 2020

# About Us

- Suricate Solutions is a **pioneering cyber security company for financial inclusion** based in Luxembourg and Senegal

- First cyber Security Operation Centre for financial inclusion in Dakar

- Affiliate for Africa for one of the major players in Europe.

- Special focus on operational security, which is the ability to **detect, remediate and recover from cyber security incidents = cyber resilience.**

- Services are tailored for financial inclusion, e.g. **security supervision, vulnerability scanning, penetration testing, awareness campaigns, audits, advisory and a "cyber security flash diagnosis"** to assess the maturity of the organisation and identify priority actions.

- Contact: jlperrier (at) suricatesolutions (dot) com

# Introduction

- **Many people work from home : Sudden / First time / Unknown duration**.
- **Financial sector globally is one of the main targets for hackers**, organized in international criminal networks, with advanced skills and tools, **looking for cash**.
- **More and more frequent and severe cyber risks**.
- **Is the appropriate level of cyber security in place ?** infrastructures, processes, policies, and employees' preparedness
- Financial inclusion institutions
  - ○ large agent networks
  - ○ emerging digital services
  - ○ weaker defences than larger institutions.

# Introduction

- **Employees and agents** are **excellent channels for intrusions**
  - using company or personal devices (PC, Tablet, and Smartphone)
  - scattered location
  - access to Core Banking System, Digital Financial Services management and other critical business applications.

# Introduction

- **Recent surge in attacks with many Covid related scams all over the world**
- Financial inclusion has to face a **long lasting cyber security challenge**
- proliferation and mix of techniques : phishing attacks, malicious documents, fraudulent websites, impersonation of government and international organizations' identities, Ransomware, social engineering, fake selling of masks, fake charity donations...
- Incidents can **endanger the institutions and customer protection: financial losses, data breaches, business discontinuity, reputation damages.**
- **Employees' outstanding behaviour will be the first line of defences**
- **Basic easy and cheap cyber security practices** should be **consistently enforced for all your devices**

> “
>
> Cyber crime is the **#1 threat** to the development of financial inclusion(*) and potentially a **systemic risk**(**)
>
> ”

(*) AFI Alliance for Financial Inclusion Global Thought Leadership Conference, Abidjan, 1/3/2019, participants round table conclusion

(**) Call with AFI, Feb 2019

# Cyber (in)security overview of Africa (1)

## Attacks on FSP are more frequent and severe

- **$ 3.5 Bn** cost of cybercrime, **+20%pa, international criminal networks**
- FSP & Financial Inclusion: **major and vulnerable targets**
- **95%** of penetration tests grant system administration rights
- **200** days average detection time
- **Many # $ 1 M incidents**

## Low awareness, and a limited ecosystem

- **Boards, IT, Employees, Policy makers, Development Agencies, Donors, Investors**
- **No** mechanism to **report and share cyber threats**
- **Limited support** from **Government** and **Law Enforcement Authorities**

# Cyber (in)security overview of Africa (2)

## Limited skills, high turnover

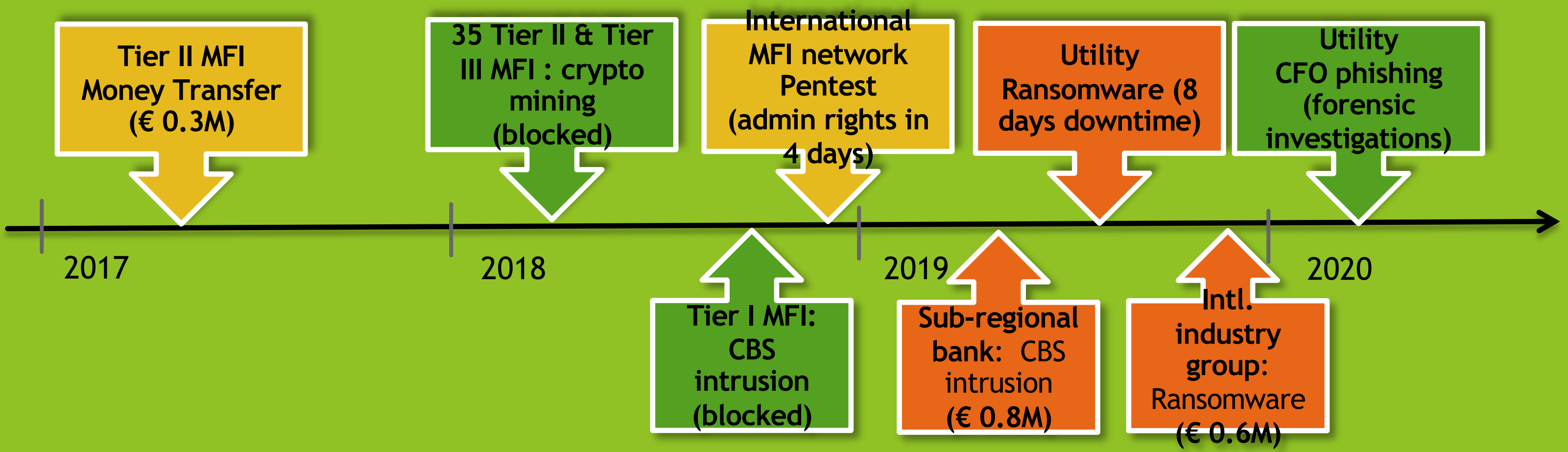
- **10.000 security engineers** vs 700.000 in USA + 300.000 open positions
- 3 security engineers for 250 MFI in Senegal
- **No** or limited specialized **higher education**
- **Top profiles** subject to **emigration**

## Lack of financial resources and inadequate distribution

- **$ 1.5 Bn Cyber security spending**
  = 4 largest US banks
- **High costs** of existing Software / Hardware / Services
- 98% of spending on prevention (technology and governance) **2% on detection and remediation** (source IBM)

# Recent incidents from WAMU

*managed by members of our consortium*



2017

Tier II MFI Money Transfer (€ 0.3M)

2018

35 Tier II & Tier III MFI : crypto mining (blocked)

Tier I MFI: CBS intrusion (blocked)

International MFI network Pentest (admin rights in 4 days)

2019

Sub-regional bank: CBS intrusion (€ 0.8M)

Utility Ransomware (8 days downtime)

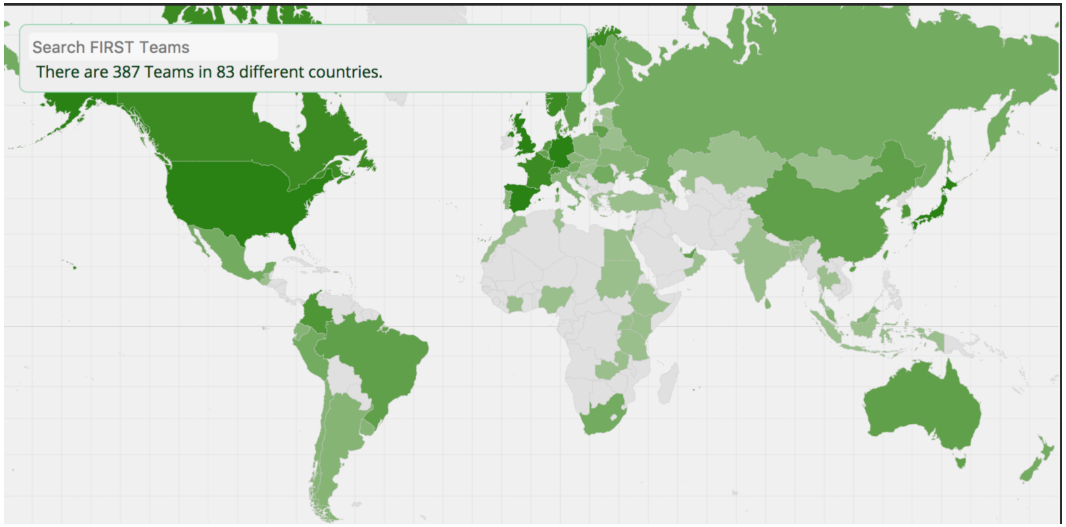
Intl. industry group: Ransomware (€ 0.6M)

2020

Utility CFO phishing (forensic investigations)

# Scarce cyber incident response capability

*Few CERT/CSIRT teams in Africa, often focusing on Public Sector issues, while attackers have gone global*



There are 387 Teams in 83 different countries.

Source Forum of Incident Response and Security Teams (FIRST)

# Some tools and practices

# Regular backup

- **Weekly backup** your documents to protect you against the loss or stealth of your device, as well as from corruption or encryption by a malware.
- Backup should include **all your professional documents** including emails, contacts, pictures
- Backup on company servers, online backup service, USB Hard Disk, or USB memory stick.
- Disconnect mobile backup media after use and store it apart the device in a safe place.

# Strengthen your passwords

- **Change default passwords** (“0000”, “admin”, “1234”, “password” for all your devices, including mobile phones’ PIN
- Use **long and complex passwords**, preferably the recommended secure passwords. Paraphrases are easily memorized alternatives e.g. “It is time to go to work, John” will become “Iit2gtw,J”.
- **Never communicate your passwords** to anybody, either by phone, email, a website formular or on a Post It on your screen.
- **Regularly change** the passwords.
- Use two factors or biometric authentication whenever possible.
- **TIP** Free Password management software will help you with this critical task.

# Use genuine software, updated to the latest available version

- **Check the installed version** for each device (laptop, tablet, smart phone). If a recent version is not available for your device, as it is often the case for older Android smart phones, stop using this device for professional purposes.
- **Use genuine software**: Illegally copied software is often downloaded from compromised websites. Download the software only from reputable editors' official websites.
- **Update systematically to latest version**. Updates containing security fixes should be immediately installed. Check that "automatic update" is selected in your system configuration.
- **TIP** There are reliable and comprehensive **Open Source** equivalents for most software, including office suite (e.g. LibreOffice).

# Avoid phishing attacks 1/2

- **Phishing emails** contain **links to compromised websites or malicious documents** that will activate malwares if you click or open them, and eventually steal your credentials. These emails usually have the following characteristics:
  - **Impersonification**: the email looks like it has been sent by a trusted party (a bank, a network operator, government services, charities, express forwarder), both in the sender email address and the design of the mail (company logos, text)
  - **Sense of urgency:** to urge you to activate the content ("you have received a prize or a donation", "Your account is about to be suspended", "special sales", "check your bank account data", "urgent invoice", "send money in emergency to"...).

# Avoid phishing attacks 2/2

- **Upon reception of an email from an unusual sender or suspect content,** do not open the attached document or click on the link and **delete the mail** immediately. In case of doubt
  - **Check the sender address**: set the cursor over the sender name and the full address will be displayed (may differ between mail clients). The address maybe one of a real person that has been compromised, or one made for purpose, e.g. @paypalinvoice
  - **Check the content** with your search engine, scams have often been shared by cyber experts, check the orthographic.
  - If the mail appears to be legitimate, do not click on the link but connect through your browser entering the full address e.g; www.paypal.com.
- **TIP** Your IT team can give you **additional support on the checks**, and **what to do in case you inadvertently activated a malicious content**.

# Secure web browsing

- **Steer clear of sites or apps with no established reputation**; they are often compromised (games, gambling, software copies, music or video download, illegal or adult contents).
- Be extremely **vigilant when you use payment & banking applications**, set low credit limits.
- Avoid websites using the non secured protocols http (http**s** is secured).
- Take care of personal, professional information and digital identity including email addresses.

# Secure your Wi-Fi access

- Set a **strong password** to replace your Wi-Fi router’s default password.
- Activate a **strong protocol (WPA2)** and disable Wi-Fi Protected Setup (WPS).
- Create a **guest account** for guests, children, etc with limited access rights. Never share your credentials.
- **Disable remote access** to the router.
- When travelling: avoid using public Wi-Fi networks unless your organization provides a VPN (Virtual Private Network) to encrypt communication, use 3G/4G mobile hot spots instead.

# Take care of all your devices and data

- **Install an antivirus and enable automatic updates**. An antivirus will not protect you from everything, but it is a decent basis.
- **Never leave a device unattended** at home, at the office or when you travel.
- Make sure sessions are automatically closed after a few minutes of idleness.
- **Do not use a USB memory stick** to share data, use an on line secured file transfer rather.
- **Protect your workplace**: check for shoulder surfing, never use public computers.
- **TIP**: there are excellent free antivirus softwares.

# Strictly separate professional and personal uses

- **Company devices** should be **dedicated to professional activities,** not be used by relatives.
- **Do not install any software other than the ones prescribed by your IT** team**.**
- **Close applications or browser after use**, in particular access to critical business applications

# You are not alone

- **Contact your IT team** for support on configuring your devices and network access, for any issue or suspicious activity, or if you made a mistake.
- **Contact Law Enforcement Authorities** in case of an incident.

# From the company side

## Ensure you are implementing quickly the basic cyber hygiene measures for secured home working

- **Awareness raising** is a key component of Information Systems Security
- Provide a **point of contact and technical support** for employees (access, backup, antivirus, authorized software...)
- Setup **VPN remote access**
- Establish **a central file sharing with a cloud service provider**, with an appropriate folder structure, document naming and access settings
- **Check and limit access rights** for all the employees including the IT Team
- **Apply security patches** to fix known vulnerabilities
- **Monitor systems and networks** closely for abnormal behaviours

# Flash diagnosis 1/3

- Based on INTERNATIONAL STANDARD **ISO/IEC 27002** Information technology — Security techniques — **Code of practice for information security controls**
- Comprehensive and (relatively) light
  - Information Security Clauses (14)
  - Control Categories (35)
  - Controls (133)
- Practical and standard basis for audits, due diligences, maturity assessments, benchmarking, sectorial analysis
- Flash Diagnosis is a **maturity assessment** ( subset of about 80 relevant questions for Financial Inclusion), and **first level of recommendations** for **improving awareness and preparing specific action plan**
- 1 day remote assignment

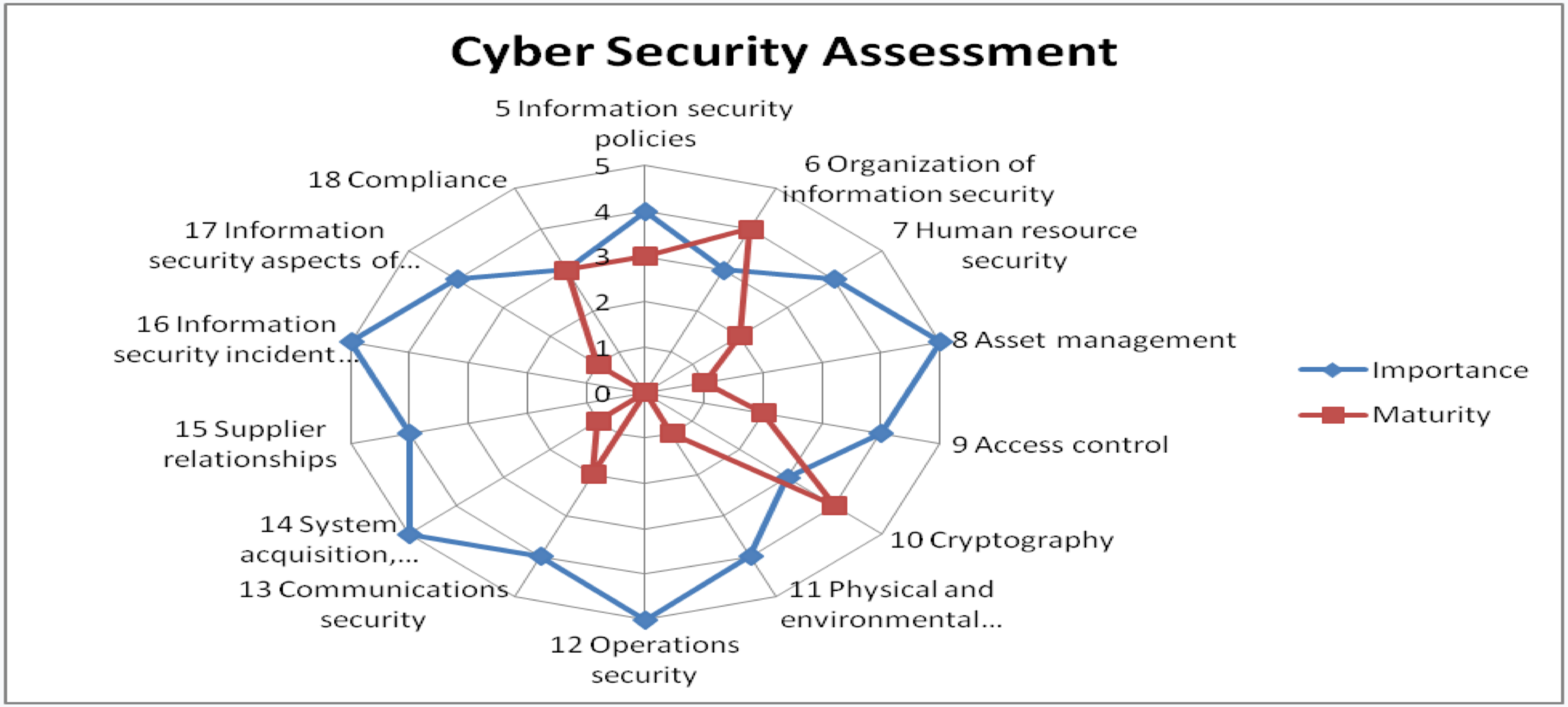
# Flash diagnosis 2/3

## 14 Information Security clauses

| |
|---|
| **5** Information security **policies** |
| **6 Organization** of information security |
| **7 Human resource** security |
| **8 Asset** management |
| **9 Access** control |
| **10 Cryptography** |
| **11 Physical** and environmental security |
| **12 Operations** security |
| **13 Communications** security |
| **14 System** acquisition, development and maintenance |
| **15 Supplier** relationships |
| **16** Information security **incident management** |
| **17** Information security aspects of **business continuity** management |
| **18 Compliance** |

# Flash diagnosis 3/3

## Presentation of results with balanced Scorecard



# African Cyber Security Resource Centre

Suricate Solutions
Security & Payments

# Project objectives

***Improve the resilience of financial inclusion institutions and protect their customers*** *against cyber attacks, to*

**(1) foster financial inclusion**

**(2) secure the development of Digital Financial Services**

**(3) enable building interoperable payment systems**

THINK BIG → START SMALL → SCALE FAST

# Project highlights

*A breakthrough for Financial Inclusion*

- Build & mobilise a **comprehensive** and **sustainable** cyber resilience **ecosystem** in 3 to 5 years
- Huge **capacity building** effort; Retain resources in Africa
- R&D & **Innovation** to understand future threats and prepare responses
- High **Impact** for financial inclusion and for the continent

# The consortium members

*An experienced pluridisciplinary* ***team***

*(365+ cyber security experts)*

***SECURITYMADEIN.LU***: Cybersecurity Agency of the Luxembourg Ministry of the Economy (35 experts)

***SnT/UNIversity of Luxembourg***: Interdisciplinary Centre for Security, Reliability and Trust, a strategic research priority in cyber security (>200 researchers)

***Excellium Group and Suricate Solutions***: Cybersecurity leader in Luxembourg with African affiliate (>130 experts)

# Our path to success

*North/South public-private partnership*

❖**Strong team** used to work together associated in a dedicated consortium (core team participants have **120+ years cumulative cyber security experience in FS/DFS**)

❖Based on **lessons learned** in the last 15 years in cyber security, in particular for the Financial Sector (IMF, BIS, ECB...) and Regional or Global cooperation

❖**Ability to deliver** fast ; **agile** implementation ; **open** cooperation ; **existing operations** in Africa

❖Thorough **Governance** and **Risk** management

❖Resource **mutualization** ; information and best practice **sharing** ; consortium lasting support

❖**Regional strategy with proximity teams**

❖**PPP to enable high impact, sustainable business model and lasting capacity building**

❖**Inclusivity: Quality services available to all size of FSP & Fintech at reasonable costs**

# Leapfrog the cybersecurity capacity in Africa

*A comprehensive, cost efficient and scalable 3 levels organisation based on lessons learned*

**1 regional coordination organization** with an **Information Sharing and Analysis Centre** (ISAC) linking to Rest Of the World and a governance with relevant stakeholders

+ 3 (sub-)regional **Computer Security Incident Response** (CSIRT or CERT)

West Africa/French Speaking

East Africa

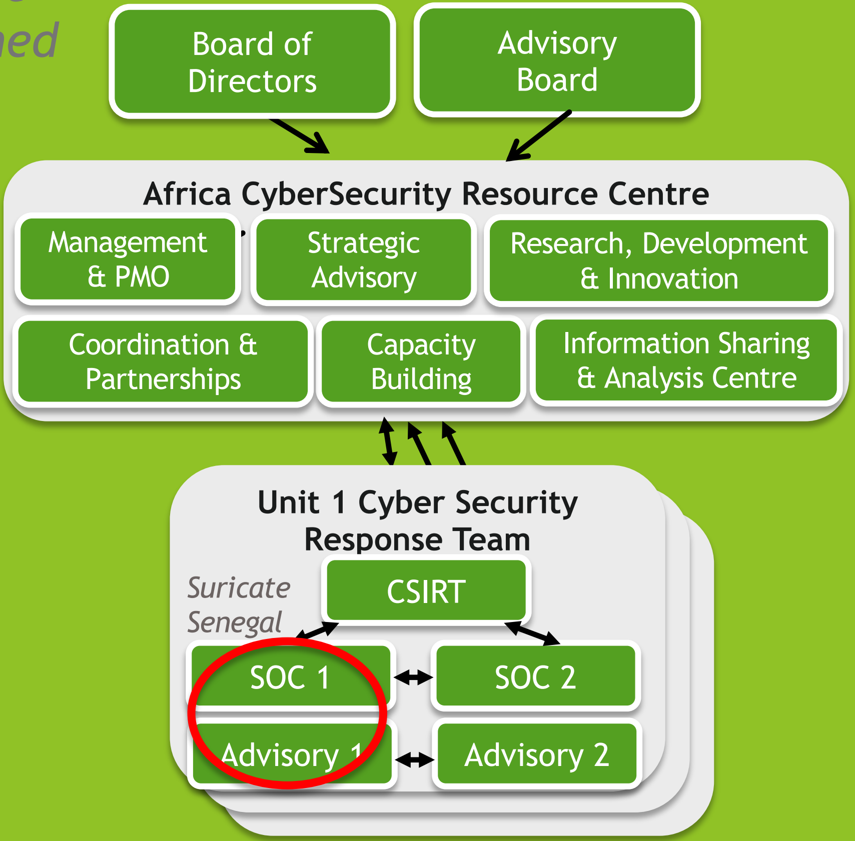
West Africa/English speaking

+ 3 local/proximity operational **24 X 7 Security Operation Centre** (SOC)

Strategic

Tactical

Operational



Board of Directors

Advisory Board

Africa CyberSecurity Resource Centre

Management & PMO

Strategic Advisory

Research, Development & Innovation

Coordination & Partnerships

Capacity Building

Information Sharing & Analysis Centre

Unit 1 Cyber Security Response Team

*Suricate Senegal*

CSIRT

SOC 1

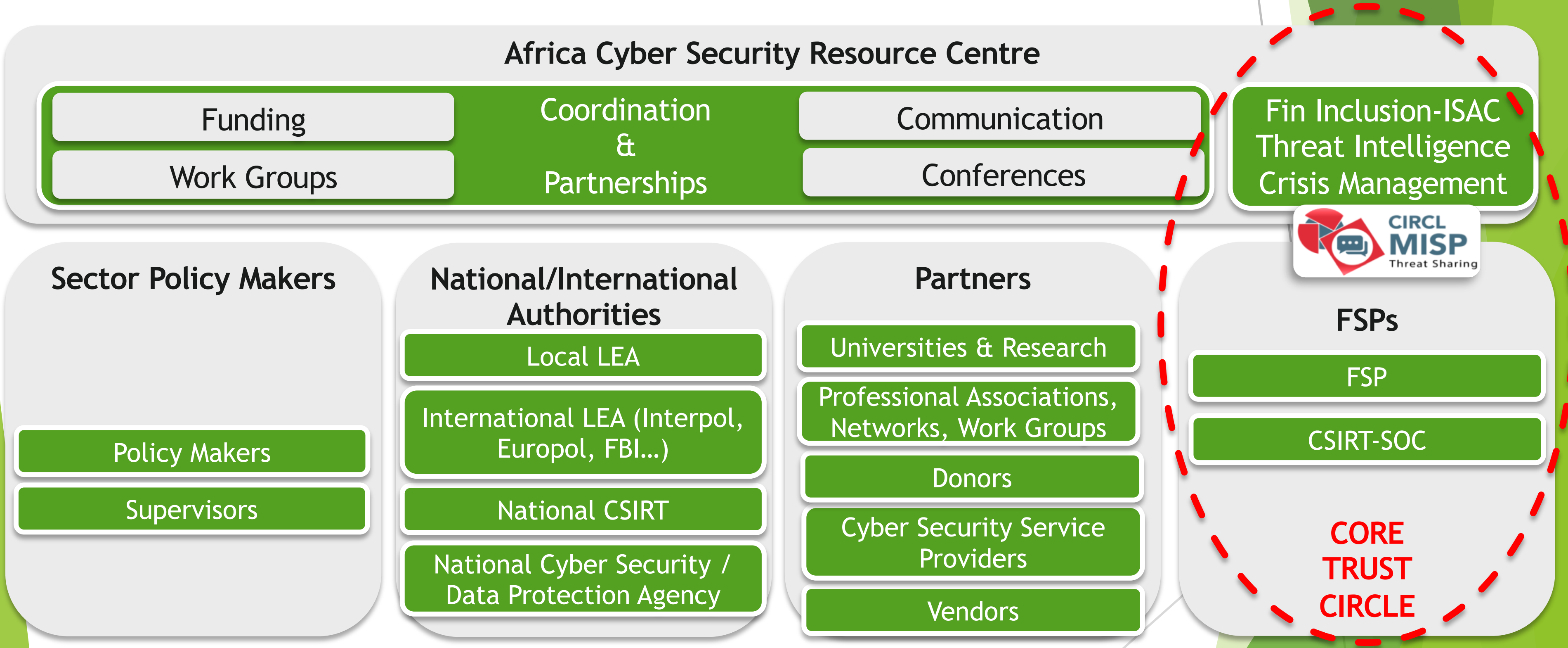
SOC 2

Advisory 1

Advisory 2

# Enable and leverage local capacity

*Open to all relevant regional or global stakeholders & initiatives*



Africa Cyber Security Resource Centre

Funding

Work Groups

Coordination & Partnerships

Communication

Conferences

Fin Inclusion-ISAC Threat Intelligence Crisis Management

CIRCL MISP Threat Sharing

Sector Policy Makers

- Policy Makers
- Supervisors

National/International Authorities

- Local LEA
- International LEA (Interpol, Europol, FBI…)
- National CSIRT
- National Cyber Security / Data Protection Agency

Partners

- Universities & Research
- Professional Associations, Networks, Work Groups
- Donors
- Cyber Security Service Providers
- Vendors

FSPs

- FSP
- CSIRT-SOC

CORE TRUST CIRCLE

★ Contacts made

# Envisioned partnerships with a clear focus

*1/ **Delivery** in Africa based on inputs from reference partners*

*2/ **feedback on lessons learned** on the field*

ada 25 ★ uni.lu UNIVERSITÉ DU LUXEMBOURG ★

ADA chair in Financial Law (Inclusive Finance, DFS)

Columbia Business School AT THE VERY CENTER OF BUSINESS™

DFS Observatory

UNESCO United Nations Educational, Scientific and Cultural Organization · UNEVOC International Centre for Technical and Vocational Education and Training

TVET

AFD AGENCE FRANÇAISE DE DÉVELOPPEMENT · INTERNATIONAL MONETARY FUND · THE WORLD BANK ★

LUX DEV Luxembourg Agency for Development Cooperation ★ · giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH ★ · AFRICAN DEVELOPMENT BANK GROUP

the smart campaign ★

Financial Inclusion Customer protection

CGAP ★

Financial Inclusion Customer protection

Cyber Security + Africa + Financial Inclusion + DFS + Implementation

smart africa CONNECT. INNOVATE. TRANSFORM ★

Policies, cooperation

★ afi

Financial Inclusion, Cyber Regulation, DFS, Financial Stability

★ EUROPEAN CENTRAL BANK

★ BILL & MELINDA GATES foundation · ★ GFCE

GSMA ★

DFS, ecosystem, Cyber security

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

DFS

★ CYBER READINESS INSTITUTE

GLOBAL CYBER ALLIANCE

Cyber security for SME

★ WORLD ECONOMIC FORUM

Future of cyber security & financial system

★ CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Cyber security for Financial System Small FSP / Financial Inclusion

# Key *contributions to*

SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD

2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONS CONSUM AND PRO
13 CLIMATE ACTION
14 LIFE BELOW W
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINA DEVELOPMENT GOALS

Ensure the access to **technical education** including at university-level
Increase the **number of cyber security post graduate students** that will form tomorrows teachers
Significantly increase the number of **digitally-skilled people (all ages), including technical and vocational skills, relevant for employment and entrepreneurship**

Support women's access to security engineering, ensure equal opportunities, **special support for financial inclusion institutions oriented towards women**

**Strengthen the capacity** of financial institutions **to extend access to Digital Financial Services** and **Interconnected Payment Systems**

**Stimulate the growth of micro-enterprises and SMEs** and their integration into the formal sector, including through **access to financial services**

**North South Public-Private partnership** investment and capacity building for **developing countries, especially in ICT / cybersecurity**

Facilitate the establishment of a **sustainable and resilient infrastructure** by strengthening financial, technological and technical support
**Increase access to ICT technologies** and ensure that all inhabitants have access to the Internet

Trusted Information sharing between FSP and with institutions
Support national institutions in the **fight against (cyber) crime** and **policy makers to develop adequate regulations**

# Key messages to clients during the COVID-19 crisis

ISABELLE BARRES, VP AND CAMPAIGN DIRECTOR, SMART CAMPAIGN @ CFI

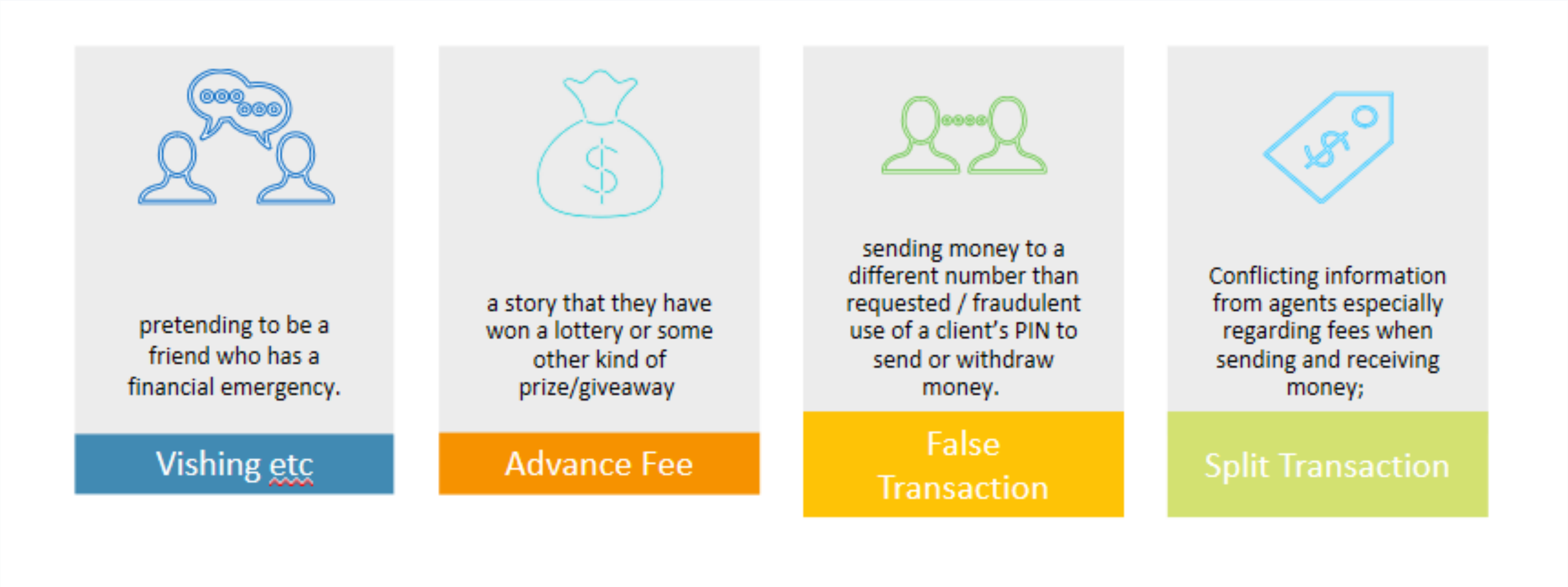
CENTER *for* FINANCIAL INCLUSION | ACCION

APRIL 30, 2020

# Increased consumer protection risks

- Deceptive marketing techniques
- Use of pressure sales techniques
- Excessive pricing
- Privacy violations
- Fraud and scams

# Examples of Fraud



pretending to be a friend who has a financial emergency.

Vishing etc

a story that they have won a lottery or some other kind of prize/giveaway

Advance Fee

sending money to a different number than requested / fraudulent use of a client's PIN to send or withdraw money.

False Transaction

Conflicting information from agents especially regarding fees when sending and receiving money;

Split Transaction

# What can providers do?

1. Reinforce key messages, especially the ones around data privacy and data security
2. Remind clients of complaints channels and encourage them to use them and report fraud or scams
3. Inform clients of known scams

For further tips and guidance, consult the Smart Campaign kit for welcoming clients:

- https://centerforfinancialinclusionblog.files.wordpress.com/2013/08/essential-docs-for-new-clients_version-2-01.pdf

  - Use this as a starting point. Focus on communication around data privacy, data security and how and where to complain.

# Reinforce key messages

**Help us keep you and your money safe**

- Read and/or discuss our Client Privacy Agreement and ask if you have questions
- Keep your information updated
- Store your financial records in a secure location and do not provide personal information (such as account information) over the phone unless you called the bank and know that you are speaking to a bank employee
- Keep account information secure and do not share your PIN numbers, passwords, or other ID codes with other people
- Inform us away if you think your personal information has been misused, misappropriated, lost, or stolen

**TIP!**: Consult Smart Campaign's resource *Essential documents for new clients* https://centerforfinancialinclusionblog.files.wordpress.com/2013/08/essential-docs-for-new-clients_version-2-01.pdf

# Remind clients of complaints channels

**Reach out – we're here to help**

- Tell us if you have a complaint or a question
- Give us a chance to correct our mistakes and answer your questions

## Inform clients of known scams

- Provide concrete examples of messages used by scammers to raise awareness for consumers
- Encourage clients to contact you if they have doubts about the legitimacy of the offer

# Thank you for your attention

Please stay in touch: info@sptf.info

SPTF

Promoting standards & practices
for responsible inclusive finance