Existing country and regional initiatives

Silvia Baur-Yazbeck, CGAP
Rahav Shalom-Revivo, Ministry of Finance, Israel
Jean-Louis Perrier, Suricate Solutions
Protecting the Financial Ecosystem

Rahav Shalom-Revivo, Ministry of Finance, Israel
Financial-Cyber Activities

- Financial CERT
- The Fintech-Cyber Inno. Lab
- Financial Supply Chain
- National Financial Center
- Digital Bank Guidance
- International Cooperation
The Financial CERT
Israel’s Financial Eco-System

Banking Supervision
Ministry of Finance
The Capital Market, Insurance and Savings Authority
Israel Securities Authority
Bank of Israel
Financial CERT’s Concept

PROACTIVE
TRACKs THREATs

NAVIGATE
CHOOSEs THE SAFEST WAY

REACTIVE
HELPs IN CASE OF NEED

“Get the best route, every day, with real–time”

“Nothing can beat real people working together”

Contribute for the cyber defence effort
Key Principals

- **JOINT VENTURE**
- **TRUSTED ZONE**
- **VOLUNTARY BASIS**
- **RETURN OF INVESTMENT**
Focus on Critical Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>STOCK EXCHANGE TRADING</td>
<td></td>
</tr>
<tr>
<td>CREDIT CARD TRANSACTIONS</td>
<td></td>
</tr>
<tr>
<td>FINANCIAL TRANSACTIONS</td>
<td></td>
</tr>
<tr>
<td>CASH FLOW</td>
<td></td>
</tr>
<tr>
<td>ALLOWANCE PAYMENTS</td>
<td></td>
</tr>
<tr>
<td>DATA LEAK/ FRAUD</td>
<td></td>
</tr>
</tbody>
</table>
Major Activities

Information Sharing & Cooperation

Incident Handling

Situation Estimation

Cyber Financial Resilience
Our global reach

75
INTERNATIONAL
CERT’S

35
COLLABORATION WITH
INTERNATIONAL
COMPANIES

6
INTERNATIONAL
EXERCISES

260
HOSTING FOREIGN
DELEGATIONS
Promoting Innovation Through Cyber Security

- Fintech Cyber Lab
- Energy Lab
- Smart Transport Lab
- Medisec Hospital Lab
- 5G Network Lab
- POC University Lab
Thank You!

RAHAV SHALOM-REVIVO
Manager, Fintech & Cyber Innovation
Jean-Louis PERRIER
November 20, 2019
## Cyber (in)security overview of Africa

### Cyber attacks increase & target FSP

- **$ 3.5 Bn** cost of cybercrime, +20%pa, criminal networks
- **FSP & Financial Inclusion**: major and vulnerable targets
- 95% of penetration tests grant sys admin 200 days avg detection

### Low awareness from ecosystem

- Boards, IT, employees, Policy makers, Devt. Agencies, donors, investors
- No mechanism to report and share cyber threats
- Limited support from Government and LEA

### Limited skills, high turnover

- 10,000 security engineers vs 700,000 in USA + 300,000 open positions
- 2 security engineers for 250 MFI in Senegal
- No specialized higher education

### Lack of financial resources

- $ 1.5 Bn Cyber security spending = 4 largest US banks
- 98% of spending on prevention 2% on detection and remediation
- High costs of existing SW / HW / Services

---

**CGAP**

**giz**

**Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) gGmbH**

**EUROPEAN MICROFINANCE WEEK**

**Connecting the inclusive finance world**

14
Cyber crime is the #1 threat to the development of financial inclusion (*) and potentially a systemic risks (**)
Vulnerable Users and institutions of financial inclusion deserve the same level of protection of their financial and information assets as in more advanced countries.

Leapfrog international best practices after adaptation to the context and resources.

Primary focus on security supervision that immediately reduces the risk exposure and allows sustainable customer support (capacity building and financially).

Build a community and involve stakeholders with Public Private Partnership.
Dakar Cyber Security Operation Centre

History
- 2016: met all stakeholders of financial inclusion in Senegal; diagnosis, solution
- Project funded by Luxembourg North/South PPP private sector development initiative & EIB
- Partnerships with MFI Professional Association in Senegal, UCAD Dakar University, Luxembourg
- 2017: setup the centre in Dakar, focusing on operational security
  - Mutualized Security Supervision Center, Vulnerability Scanning
  - Incident Response
  - Coaching customers
- 2018: POC and start of operations
- 2019: Preparing for scale up
  - Massive training for 100 banks with BCEAO
  - First regional banking customers
  - New services: Cyber Security Maturity Assessment, Governance, Pentest, large scale awareness program for 5,000 employees
  - Open Source detection systems
  - Design continental program with our partners
April 2018: 5PM: Private Cloud of a group of 35 Tier II & Tier III MFI
- Intrusion after user downloaded malicious content from social networks, undetected by Antivirus.
- Malware started **crypto currency mining in China**, detected in a few minutes before spreading

December 2019: Intrusion in the Core Banking System (CBS) of one of the largest MFI in WAMU.
- Phishing to the CIO email granted systems access with privileged accounts!
- Fraudulent transactions immediately started, stopped after detection by Suricate

March 2019: Intrusion in the CBS of a regional bank in WAMU. Losses # € 0.8M.
- Accounts opened fraudulently, intrusion allowed to perform fraudulent transfers undetected for several weeks, multiple withdrawals. 6 arrested, hackers from international criminal organization still running.
- Now a customer ;-) 

April 2019: Large Scale RansomWare attack for one of the largest utilities in Senegal.
- 80% of servers infected, including backup system, **IT and operations down for 8 days**
- Recovery assistance by our Cyber Security Incident Response Team.

November 2019: Penetration test on new web banking of a large international MFI network
- All systems admin reached in 4 days, app launch postponed until application fixed ($$) and new round of pentest
Dakar Cyber Security Operation Centre

Lessons learned

- Diagnostic validated and mutualized solutions adapted & adopted
  - Traditional Banking infrastructure as well as DFS at risk
  - Infrastructure under constant scanning from China, North Korea, Russia, Ukraine, US, Brazil, Africa
  - Numerous risky behaviour / mistakes from employees, and eventually compromises
  - Each alert or incident: opportunity to improve infrastructure, policies, processes, capacity, awareness, training

- Capacity building is a key component
  - Teams proximity => learning by doing
  - Awareness raising is time and $$ consuming
  - Assisted University of Dakar in creating the first two regional MSc in cyber security

- Sustainable business model established: partial subsidies for investments, institutions pay for services

- Formally mobilizing the Technical and Financial partners of financial inclusion, development agencies, central banks, longer than expected: programs by country, customer segment, or by gender or by institutions but limited framework for regional/sub regional projects

- Professional Associations are eager that pragmatic solutions be brought to their members
African Cyber Security Resource Center for financial inclusion in SSA is on its way.

Suricate, EOY 2019: 8 countries, 47 MFI, 1.2 M end customers

Suricate, EOY 2021 Burkina MFI + CIF Network: 10 countries, 67 MFI, Fintech 5.4 M end customers

African Cyber Security Resource Centre
Consortium at funding stage: 1 coordination organisation, 3 sub regional centres, 50 countries, x00 FSP: MFI, Fintech, Micro Insurance, x0 M end customers
Thank You