Making Finance Work for Africa | ipc partner for development | HORUS DEVELOPMENT FINANCE | iecd semeurs d'avenir | European Investment Bank

This project is funded by the European Union

Sujet 6 :

Les défis de la cybersécurité pour les institutions financières dans le contexte de l'expansion des services financiers numériques.

Les panélistes seraient invités à partager leur point de vue sur les questions suivantes :

- Introduction aux principaux risques de cybersécurité
- Risques accrus dus aux services financiers numériques
- Étapes clés pour protéger les IF et leurs clients
- Étapes clés à suivre avant et pendant un processus de numérisation.

Date	**Le 20 Janvier 2022**
Heure	**13h00 - 14h30 (GMT)**
Plateforme	**Zoom Meetings**

Inscrivez-vous
https://afdb.zoom.us/webinar/register/WN_vAV1C4vWRyKdxlWPdAhyUA

Panélistes :

Ghislain Nkoudjou
Directeur SIS, CCA Bank

Eric Malm
Directeur IT, Access Liberia Bank

Stéphane Konan
Conseiller principal au ministère de la défense de Côte d'Ivoire

Jean-Louis PERRIER
Directeur du programme, Africa Cybersecurity Resource Center

Pour plus d'information, visitez : https://www.msmefinanceta.eu/?lang=fr/

NOTRE WEBINAIRE DÉBUTERA SOUS PEU …

#MFW4A/EIBWEBINARSERIES

SOMMAIRE

- INFORMATIONS PRATIQUES
- MFW4A
- PANÉLISTES
- PRÉSENTATIONS
- Q&A

MFW4A/EIB WEBINAR SERIES

INFORMATIONS PRATIQUES

- La durée du webinaire de ce jour est de 75 minutes, incluant les questions et réponses
- Pour un meilleur confort d'écoute, tous les micros des participants seront désactivés pendant la durée du webinaire
- Les questions peuvent aussi être soumises via "Q & A"
- La traduction simultanée sera disponible en FR/EN/FR
- Les diapositives et un enregistrement du webinaire seront distribués au terme de la session
- Envoyez un message aux organisateurs si vous rencontrez des problèmes techniques
- N'oubliez pas de remplir le questionnaire qui apparaîtra automatiquement sur votre navigateur à la fin de la session

MFW4A: Plate-forme pour l'harmonisation et la facilitation du développement du secteur financier et le partage des connaissances

Objectifs: Contribuer à la réalisation du plein potentiel du secteur financier africain

Stimuler le développement économique et de réduire la pauvreté en Afrique

NOS DONATEURS

AFRICAN DEVELOPMENT BANK GROUP
GROUPE DE LA BANQUE AFRICAINE DE DÉVELOPPEMENT

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

AFD

Banque européenne d'investissement
La banque de l'UE

Federal Ministry for Economic Cooperation and Development

AFREXIMBANK

European Commission

Ministerie van Buitenlandse Zaken

secretariat@mfw4a.org
www.mfw4a.org

REMERCIEMENTS À LA BANQUE EUROPEENNE D'INVESTISSEMENT ET À L'UNION EUROPÉENNE

PROGRAMME D'ASSISTANCE TECHNIQUE DE LA BEI POUR LES OPÉRATIONS DU SECTEUR FINANCIER EN AFRIQUE DE L'OUEST ET CENTRALE

Objectif : Améliorer l'inclusion financière responsable en créant un accès aux services financiers à moyen et long terme pour les MPME, par le biais de prêts et d'une assistance technique aux banques et aux institutions de microfinance.

#MFW4A/EIB WEBINARSERIES

MODÉRATRICE

Edwige TAKASSI
Experte en Finance Inclusive, IPC GmbH

INTRODUCTION

Nikolaos MILIANITIS
Chef de la délégation de la BEI en Afrique Centrale

La cybersécurité pour Institutions Financières : challenges et solutions dans un contexte d’expansion des services financiers numériques

#MFW4A/EIBWEBINARSERIES

PANÉLISTES

Eric MALM
Directeur IT, Access Bank Liberia

Stephane KONAN
Conseiller principal du Ministère de la défense, Côte d'Ivoire

Ghislain NKOUDJOU
Directeur SIS, CCA Bank

Jean-Louis PERRIER
Directeur de programme, Africa Cybersecurity Resource Center

Cybersecurity Pandemic

Eric Malm - CIO

AccessBank Liberia

Agenda

- Impact of COVID-19
- Response of the Financial Sector
- Revived Cyber attacks
- Protection in the new normal for Cybersecurity

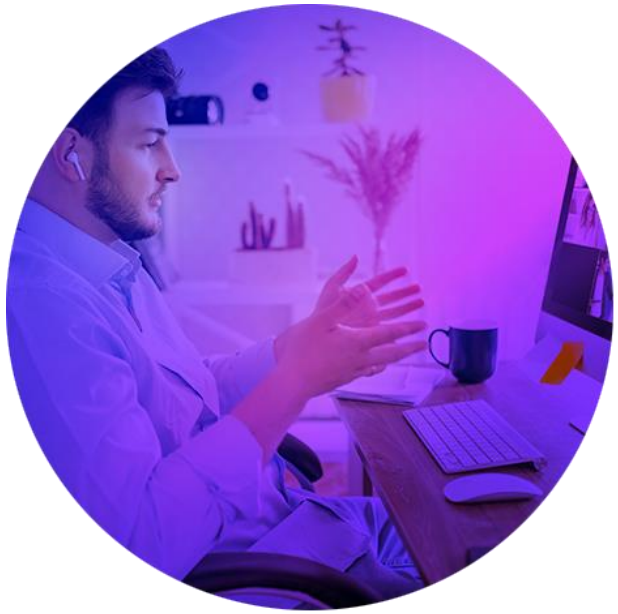
Impact of COVID-19

- 95% of cybersecurity breaches are caused by human error - Cybintsolutions
- There is a hacker attack every 39 seconds - Cybintsolutions
- 43% of cyber attacks target small business - Cybintsolutions
- Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes - Cybintsolutions
- 9.7 Million Records healthcare records were compromised in September 2020 alone - Cybintsolutions
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021 (* Africa GDP 2.6 Trillion) - Cybintsolutions
- Coronavirus Related Attacks Reach 200,000 Weekly – Checkpoint Software technologies

https://www.cybintsolutions.com/cyber-security-facts-stats/
https://www.checkpoint.com/pages/cybersecurity-protect-from-cyber-pandemic/#cyber-attack-trends

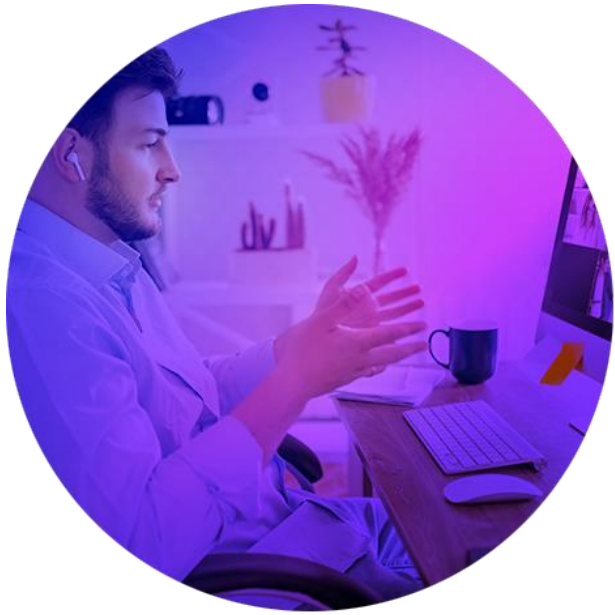
Response of the Financial Sector – Working Environment

- Social Distance – Encourage employee to work from home
- Virtual meeting – Zooming
- Lessen of iron curtains of corporate restrictions
- Fast adoption of BYOD (Bring Your Own Device)
- Sharing of confidential info on the Public Domain
- Fast adoption of Fintech and new tech ideas
- Acceleration of digital transformation



Response of the Financial Sector – Digital Banking

- New Digital Customer Experience
- Servicing vs engagement
- Next tech generation
- Introduction of digital product to non ready customers



Revived Cyber attacks

- Fake corona virus news websites
- Selling of stolen video conference credentials
- Uninvited guests to meeting
- Malicious employees working from home
- Increase attacks due to the use of own devices
- Home WIFI
- Sophisticated Phishing (Machine Language capabilities)
- Usage of various channel SMS, Vishing (Voice phishing)
- Sophisticated ransomware (combination of data leakage and ransomware)

Protection in the new normal for Cybersecurity

- Staff Awareness
- Time-outs in key system
- Enhancing controls to apply four eyes principles
- Enforcing segregation of duties
- Automated controls
- Host checking
- Antivirus protection for both corporate and home
- Home network security – Stronger password on home WIFI
- Usage of VPN
- Identify weak spots – Patch the most critical vulnerabilities
- Frequent reviews –Evaluate cybersecurity risk
- Review Business continuity plan with Cyberattack scenario
- Allocate Budget for Cybersecurity
- Well defined role of CISO / ISO (Chief /Information Security Officer) in the Company
- Zero Trust – only authenticated and authorized users or devices are permitted


Thank
you

#MFW4A/EIBWEBINARSERIES

Q&A

Soumettez vos questions via le "Chat" ou "Q & A"

LA SECURITE DES DONNEES EN ENVIRONNEMENT BANCAIRE

STEPHANE KONAN
pour le compte de **MFW4A (AFRICAN DEVELOPMENT BANK)**
JANVIER 2022
Utilisateur Final:
MFW4A

DEFINITIONS ET PRINCIPES

- LES DONNEES ET LEUR SECURITE
- CLASSIFICATION DES DONNÉES ENVIRONNEMENT BANCAIRE

LES DONNEES ET LEUR SECURITE

- Les données sont l'**actif le plus précieux** de toute entreprise.
- Les banques et établissements financiers traitent à la fois leur **données « corporate » propres** et les **données personnelles** (de leurs clients)
- Malgré une attention croissante portée à la cybersécurité, le nombre de violations de données augmente.
- **La classification des données est une composante essentielle de tout programme de sécurité et de conformité de l'information**.
- La première étape consiste à élaborer une politique de classification des données afin de définir quelles sont les données sensibles, et d'établir des règles pour leur protection.

LA CLASSIFICATION DES DONNEES EN ENVIRONNEMENT BANCAIRE

- Les organisations qui stockent et traitent des données commerciales utilisent 4 niveaux de classification des données, dont trois niveaux confidentiels (secret, confidentiel, utilisation commerciale seulement) et un niveau public.
- La même règle s'applique aux organisations médicales et éducatives:
  - **Usage restreint**
  - **Données confidentielles**
  - **Données internes**
  - **Données publiques**

LA PROTECTION DES DONNEES PERSONNELLES

- RISQUES LEGAUX ET REGLEMENTAIRES
- CONSÉQUENCES ET IMPACTS SUR LES ACTIVITÉS

RISQUES LEGAUX ET REGLEMENTAIRES

- **RGPD Règlement Général pour la Protection des Données**: applicable dans tous les États membres de l'Union européenne mais aussi application extraterritoriale: principe du consentement explicite et volontaire
- **LOI 2013-450 sur la Protection des données personnelles**: proscrit la collecte et/ou le traitement de donnée telles que l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses, l'appartenance syndicale, la vie sexuelle, les données génétiques et sanitaires.
- **LOI 2013-451 relative à la lutte contre la cybercriminalité**
- **LOI 93-661 relative au secret bancaire**: l'acte de révélation ou de divulgation du secret est un délit.

CONSEQUENCES ET IMPACTS SUR LES ACTIVITES

- **Amendes, Dommages et intérêts**: 198 amendes infligées en 2020, soit 141% de plus que l'année précédente, avec des pénalités totalisant 10,4 milliards de dollars.
- **Poursuites civiles et pénales** (y compris les recours collectifs)
- **Réputation (et perte de confiance)**: les dommages à la réputation causés par les cyberattaques peuvent être dévastateurs pour les entreprises du secteur financier
- **Baisse du cours des actions** (en bourse)
- **Cout d'indemnisation élevés**: les entreprises qui subissent une violation de données doivent faire face aux coûts considérables liés à la maîtrise de la violation et à l'identification des informations volées et des personnes affectées par la violation.

LA PROTECTION DES DONNEES D'ENTREPRISE

- EN ENVIRONNEMENT PROFESSIONNEL
- EN DEPLACEMENT
- DANS LE CADRE PRIVE

EN ENVIRONNEMENT PROFESSIONNEL

- Veiller aux éléments physiques d'identification (Badge et uniforme)
- Veiller au respect de la politique de classification de l'information
- Chiffrer les données et les communications
- Vigilance face au « PHISHING »
- Questionner la légitimité des requêtes
- Proscrire l'usage des réseaux sociaux et des forums internet
- Maintenir une vigilance sur les périphétiques: Imprimantes, Fax, Poubelles, Tableaux, Smartphones, Tablettes
- Veiller activement sur les nouvelles menaces

EN DEPLACEMENT

- Protéger les documents sensibles (chambres d'hotels, transports publics, « afterworks »)
- Veiller aux éléments physiques d'identification (Badges, « Stickers »)
- Restreindre les conversations : familiales, lieux publics, transports
- Chiffrer les supports digitaux (clés USB, Disques, Laptops)
- Proscrire le partage d'outils de communication (Smartphone, Laptop)
- Veiller activement sur les nouvelles menaces

DANS LE CADRE PRIVE

- Utiliser les réseaux sociaux de manière responsable (base de renseignement utiles aux attaquants)
- Protéger son identité numérique et sa e-Reputation
- Dissocier les usages privés et professionnels
- Proscrire les conversations privées et familiales (portant sur les activités de l'entreprise)

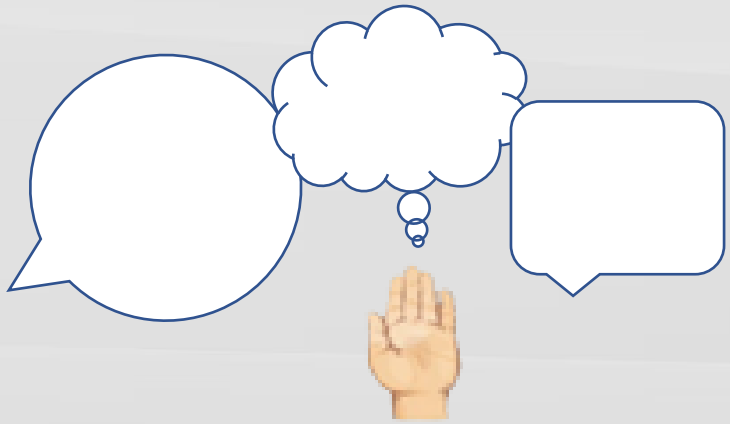
CONTACTS

COMPETENCES LDA
+2389823613
CEO@COMPETENCES-SARL.COM
WWW.COMPETENCES-SARL.COM

COMPETENCES LDA
pour le compte de **AFRICA DIGITAL CONNECT**
OCTOBRE 2021
Utilisateur Final:
SOCIETE GENERALE COTE D'IVOIRE.

#MFW4A/EIBWEBINARSERIES

Q&A



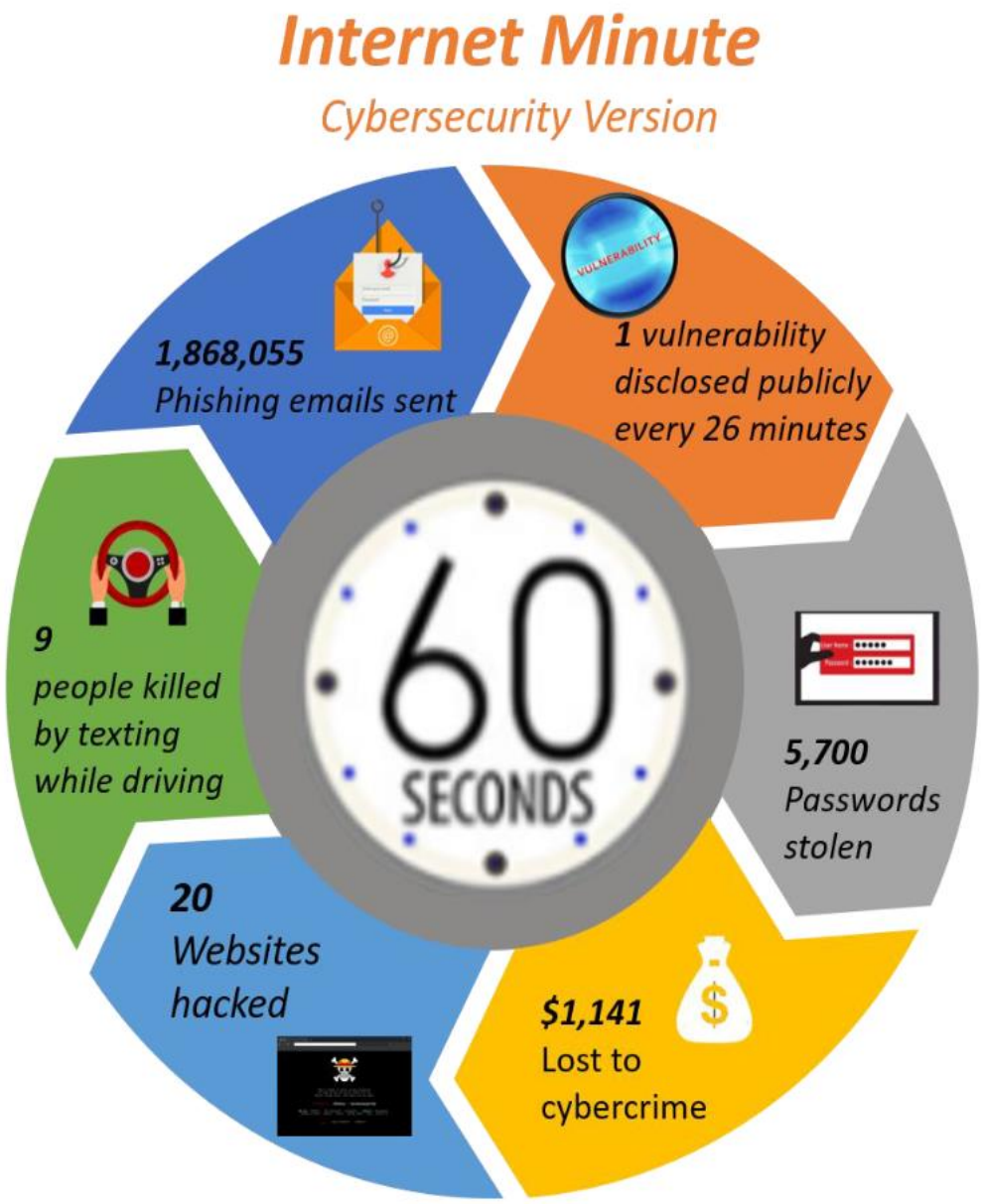
Soumettez vos questions via le "Chat" ou "Q & A"

Défis de la cybersécurité dans les banques au Cameroun

Un autre angle de vue…

Ghislain NKOUDJOU
Ingénieur Cryptographie et Sécurité Informatique
RSSI CCA-Bank
CISA | CISM | CHFI | CEH | ITIL
676053308 / 690605818

Internet / Minutes



1.9M
Phishing mails

9
killed while text driving

6K
Stolen passwords

1,141$
Lost to cybercrime

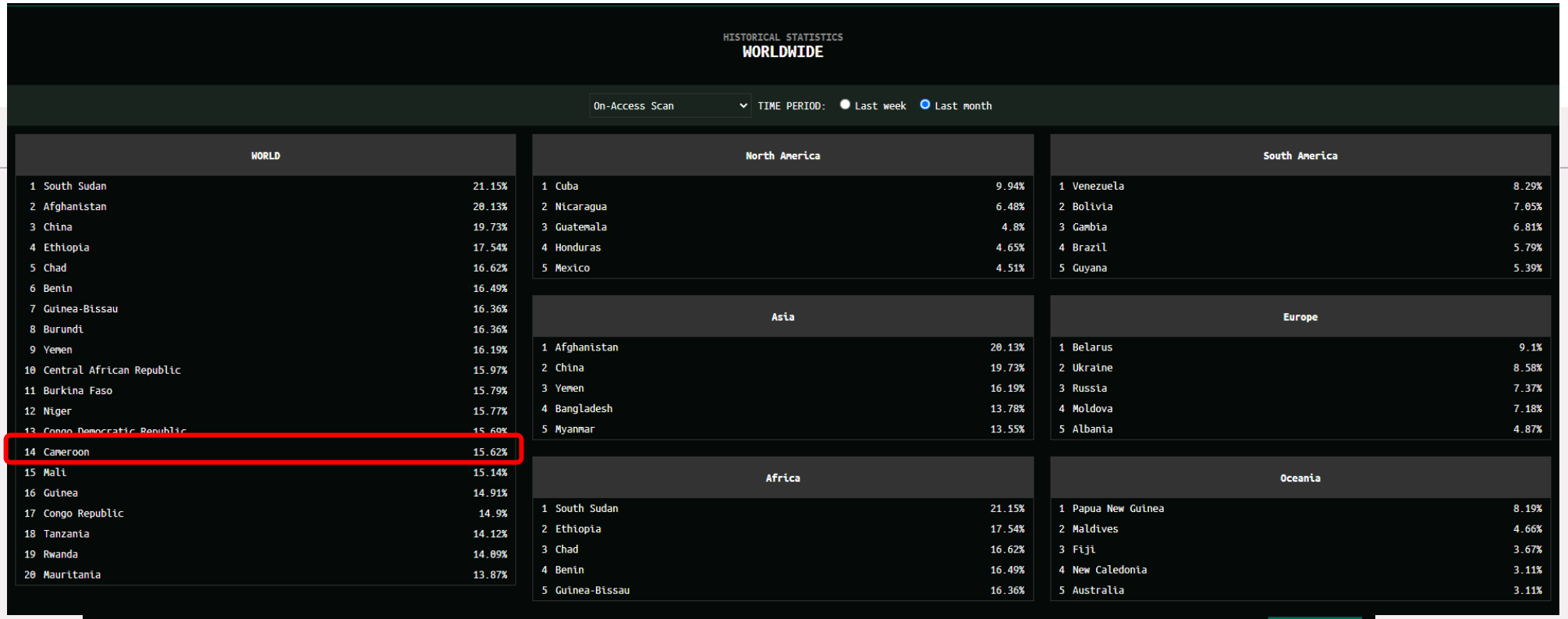
PwC - EasyOffices Business Coffee

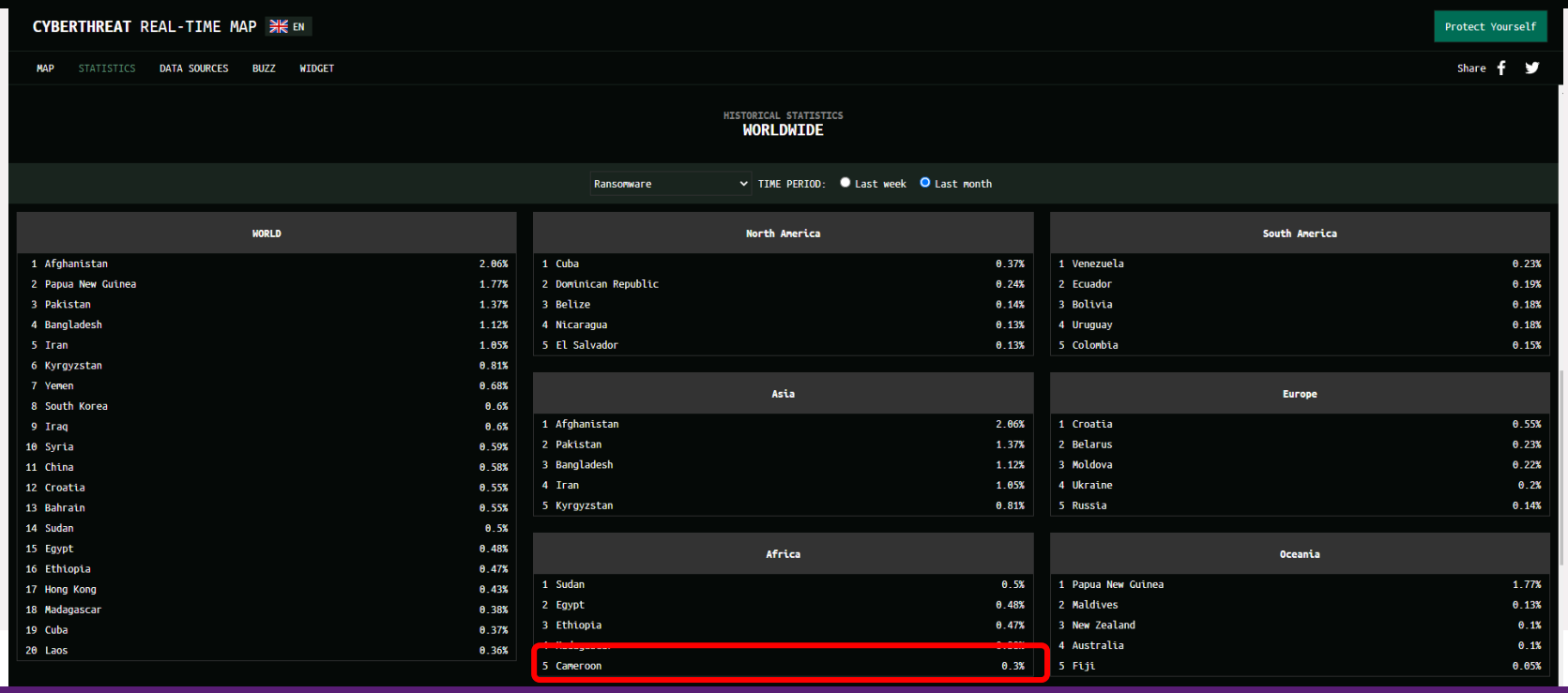
Juillet 2021

9

Checkpoint


Check Point
SOFTWARE TECHNOLOGIES LTD.
THREATCLOUD
LIVE CYBER THREAT MAP
10 325 507 ATTACKS ON THIS DAY
DON'T WAIT TO BE ATTACKED
PREVENTION STARTS NOW>
RECENT DAILY ATTACKS
400 000 000
350 000 000
300 000 000
250 000 000
200 000 000
150 000 000
100 000 000
50 000 000
0
Jun. 4th
Jun. 13th
Jun. 22nd
Jul. 1st
Jul. 10th
Jul. 19th
Jul. 28th
Aug. 6th
Aug. 15th
Aug. 24th
ATTACKS
Current rate
4
Trojan.WIN32.XMRig.A
10:21:33 Germany → Bolivia
Trojan.WIN32.XMRig.A
10:21:33 Germany → Bolivia
Trojan.WIN32.XMRig.A
10:21:33 Germany → Bolivia
Trojan.WIN32.XMRig.A
10:21:33 Germany → Bolivia
Trojan.WIN32.XMRig.A
10:21:32 Germany → Bolivia
infecting website.TC.plem
10:21:32 VA, United States → Japan
Memcached Web-Servers Network Fl...
10:21:32 India → India
Cameroon
ATTACK TREND
Last 30 days
MALWARE TYPE TRENDS
% of affected organizations
Banking Trojans 0.6%
Botnet 3.6%
Cryptominer 10.0%
Mobile 7.5%
Ransomware 0.1%
Germany
VA, United Sta
Japan
India
India
Boli
Malware
Phishing
Exploit
TOP TARGETED COUNTRIES
Highest rate of attacks per organization in the last day.
Mongolia
Nepal
Indonesia
Bolivia
Nigeria
TOP TARGETED INDUSTRIES
Highest rate of attacks per organization in the last day.
Education
Government
ISP/MSP
TOP MALWARE TYPES
Malware types with the highest global impact in the last day.
Botnet
Phishing
Worm


HISTORICAL STATISTICS
WORLDWIDE
On-Access Scan
TIME PERIOD: Last week Last month
WORLD
1 South Sudan 21.15%
2 Afghanistan 20.13%
3 China 19.73%
4 Ethiopia 17.54%
5 Chad 16.62%
6 Benin 16.49%
7 Guinea-Bissau 16.36%
8 Burundi 16.36%
9 Yemen 16.19%
10 Central African Republic 15.97%
11 Burkina Faso 15.79%
12 Niger 15.77%
14 Cameroon 15.62%
15 Mali 15.14%
16 Guinea 14.91%
17 Congo Republic 14.9%
18 Tanzania 14.12%
19 Rwanda 14.09%
20 Mauritania 13.87%
North America
1 Cuba 9.94%
2 Nicaragua 6.48%
3 Guatemala 4.8%
4 Honduras 4.65%
5 Mexico 4.51%
South America
1 Venezuela 8.29%
2 Bolivia 7.05%
3 Gambia 6.81%
4 Brazil 5.79%
5 Guyana 5.39%
Asia
1 Afghanistan 20.13%
2 China 19.73%
3 Yemen 16.19%
4 Bangladesh 13.78%
5 Myanmar 13.55%
Europe
1 Belarus 9.1%
2 Ukraine 8.58%
3 Russia 7.37%
4 Moldova 7.18%
5 Albania 4.87%
Africa
1 South Sudan 21.15%
2 Ethiopia 17.54%
3 Chad 16.62%
4 Benin 16.49%
5 Guinea-Bissau 16.36%
Oceania
1 Papua New Guinea 8.19%
2 Maldives 4.66%
3 Fiji 3.67%
4 New Caledonia 3.11%
5 Australia 3.11%


CYBERTHREAT REAL-TIME MAP EN
Protect Yourself
MAP STATISTICS DATA SOURCES BUZZ WIDGET
Share
HISTORICAL STATISTICS
WORLDWIDE
Ransomware
TIME PERIOD: Last week Last month
WORLD
1 Afghanistan 2.06%
2 Papua New Guinea 1.77%
3 Pakistan 1.37%
4 Bangladesh 1.12%
5 Iran 1.05%
6 Kyrgyzstan 0.81%
7 Yemen 0.68%
8 South Korea 0.6%
9 Iraq 0.6%
10 Syria 0.59%
11 China 0.58%
12 Croatia 0.55%
13 Bahrain 0.55%
14 Sudan 0.5%
15 Egypt 0.48%
16 Ethiopia 0.47%
17 Hong Kong 0.43%
18 Madagascar 0.38%
19 Cuba 0.37%
20 Laos 0.36%
North America
1 Cuba 0.37%
2 Dominican Republic 0.24%
3 Belize 0.14%
4 Nicaragua 0.13%
5 El Salvador 0.13%
South America
1 Venezuela 0.23%
2 Ecuador 0.19%
3 Bolivia 0.18%
4 Uruguay 0.18%
5 Colombia 0.15%
Asia
1 Afghanistan 2.06%
2 Pakistan 1.37%
3 Bangladesh 1.12%
4 Iran 1.05%
5 Kyrgyzstan 0.81%
Europe
1 Croatia 0.55%
2 Belarus 0.23%
3 Moldova 0.22%
4 Ukraine 0.2%
5 Russia 0.14%
Africa
1 Sudan 0.5%
2 Egypt 0.48%
3 Ethiopia 0.47%
5 Cameroon 0.3%
Oceania
1 Papua New Guinea 1.77%
2 Maldives 0.13%
3 New Zealand 0.1%
4 Australia 0.1%
5 Fiji 0.05%

BOLLORÉ
TRANSPORT & LOGISTICS

Demande de rançon:
Vol des données confidentielles.

Source: lemondeinformatique.fr

2011

Source: Internet - L'éléphant déchaîné

2011

Ecobank
The Pan African Bank

Accès frauduleux:
Piratage de 43 comptes (3 Milliards FCFA)

Source: CRTV - Web

2012

CCA Bank
La Finance au Cœur des Traditions Africaines

Accès frauduleux:
Piratages de 13 Comptes
(Environ 1 Milliard)
Source: site web ecomatin

2016

A retenir…

« le risque cyber constitue toujours pour le système financier une menace systémique, donc l'acuité c'est renforcée depuis la crise…. »

Les défis de l’heure

Le télétravail

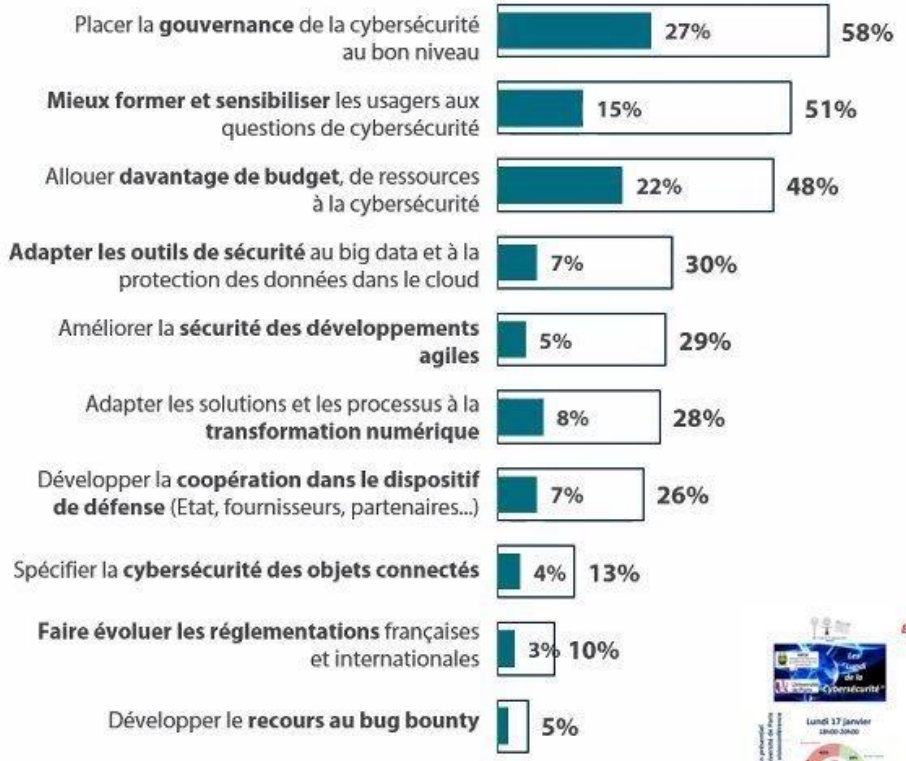
La réglementation

La Digitalisation

Les enjeux humains et budgétaires restent les priorités de demain

282 personnes

Q27. Parmi les enjeux suivants, quels sont selon vous les trois enjeux de demain pour l'avenir de la cybersécurité des entreprises ?
Base ensemble



"opinionway pour CESIN

Évolution statistiquement significative par rapport à la vague précédente

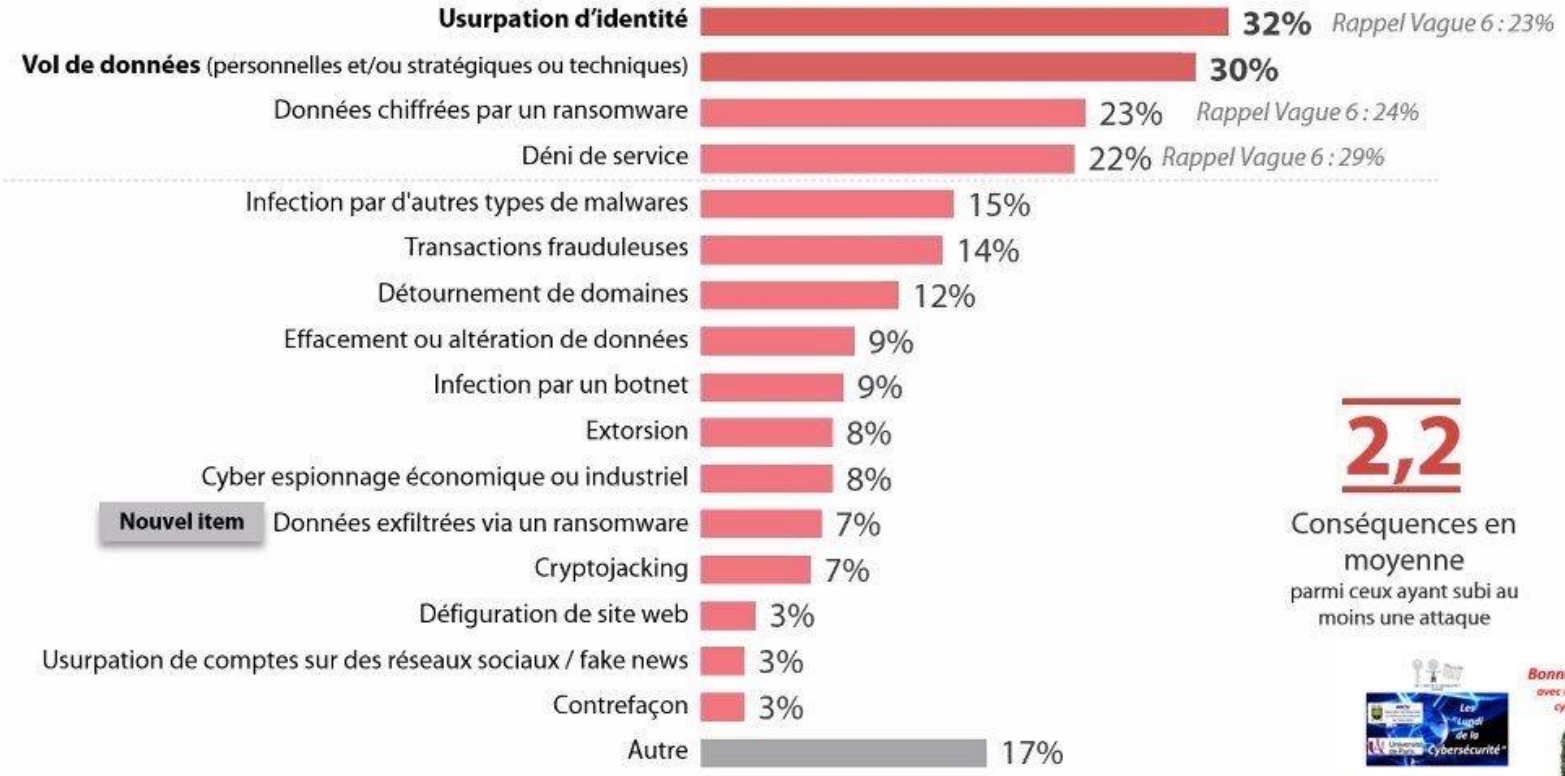
51

Principaux risques de Cybersécurités

L'usurpation d'identité est, cette année, la première conséquence des attaques. Le chiffrement des données par ransomware se stabilise

152 personnes

Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?
Base ont constaté une attaque / Plusieurs réponses possibles



2,2

Conséquences en moyenne
parmi ceux ayant subi au moins une attaque

"opinionway pour CESIN

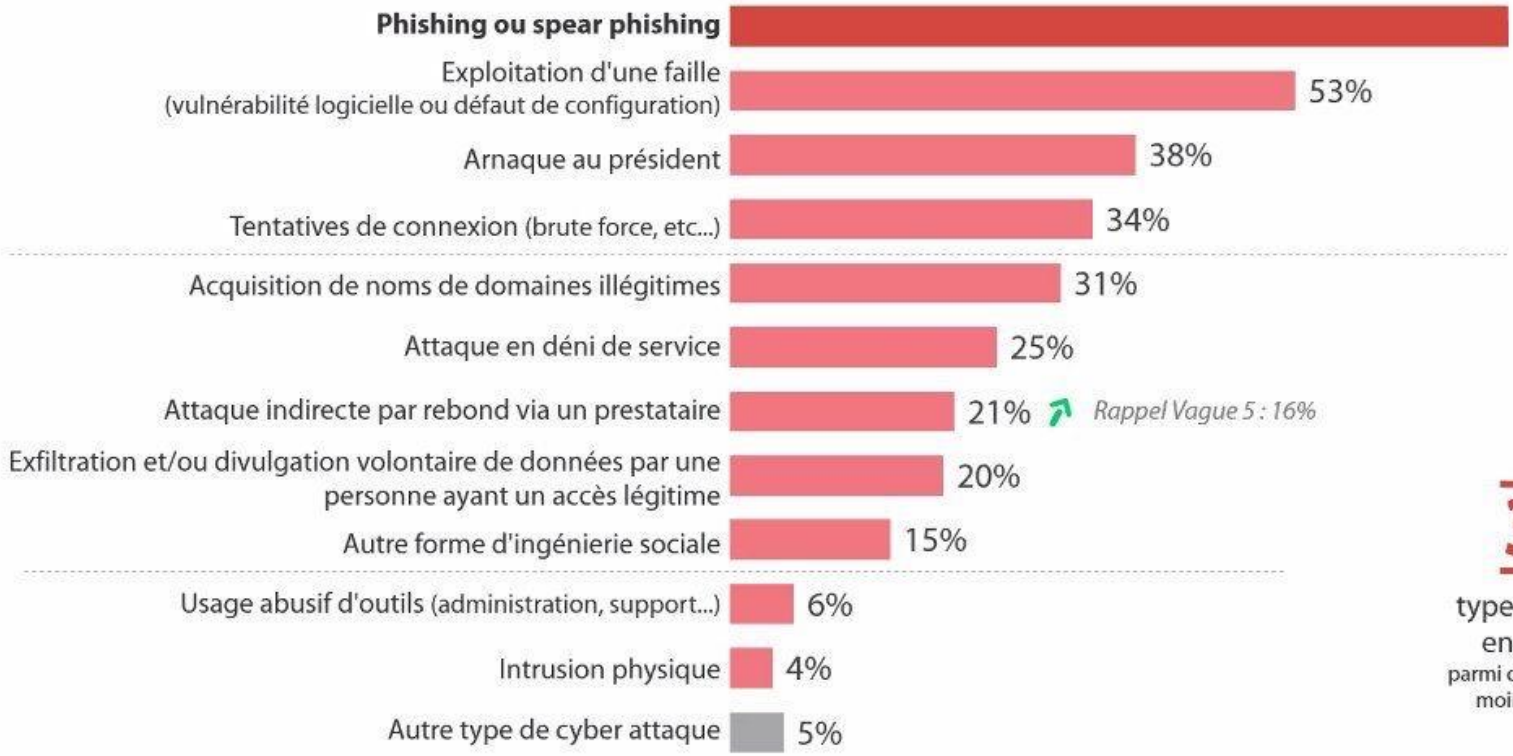
14

Quelques risques sur les services Digitaux

Le phishing, reste le premier vecteur d'attaque dans les entreprises malgré une légère baisse. A noter, l'augmentation des attaques indirectes via un prestataire

152 personnes

Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?
Base ont constaté une attaque / Plusieurs réponses possibles



3,3
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

"opinionway pour CESIN

13

La démarche

Importance reconnue mais **stratégie** souvent **inadaptée** et non productive

Responsabilité cybersécurité encore **attribuée au personnel technique**

Stratégie de **gestion des risques pas toujours adaptée** au contexte

Gestion des incidents cybersécurité **pas encore maîtrisée**

Facteur humain identifié comme **lacune importante** liée aux cyber risques

Le **cadre réglementaire et la coopération internationale pas** toujours **mis en place**

La démarche en 9 points

1. Sécurité du réseau

- Protéger le réseau des attaques
- Défendre le périmètre de réseau, bloquer tout contenu malicieux et accès non autorisés
- Contrôler et tester les contrôles de sécurités

2. Education et Sensibilisation

- Former les équipes
- Maintenir la conscience des cyber risques
- Implémenter les règles de sécurités qui couvrent l'utilisation acceptable et sécurisé des systèmes

3. Prévention des malwares

- Etablir les défenses anti-malware
- Implémenter les règles adéquates

4. Contrôle des supports Amovibles

- Mettre en place une règle permettant le contrôle des accès aux périphériques amovible
- Limiter les types de support et leur utilisation.
- Faire un scan anti-malware sur tous les médias externes avant de les importer dans le système de l'entreprise.

5. Configuration sécurisée

- Appliquer les patchs de sécurité et s'assurer que la sécurité des configurations de tous les systèmes est maintenue.
- Créer un inventaire des systèmes et définir un modèle pour tous les équipements informatiques.

La démarche en 9 points

6. **Gérer les privilèges des utilisateurs**

- Etablir des processus de gestion efficaces et limiter le nombre de comptes ayant des privilèges.
- Limiter les privilèges des utilisateurs et surveiller les activités des utilisateurs.
- Contrôler les accès aux journaux d'audit et d'activité.
- Interdire les comptes générique

7. **Gestion des incidents**

- Être capable de réagir en cas d'incident ou de récupération après une catastrophe.
- Tester vos plans de gestion d'incidents.
- Fournir des formations spécialisées.
- Informer les autorités locales des incidents criminels.

8. **Surveillance**

- Établir une politique de surveillance et mettre en place les stratégies justificatives.
- Surveiller en continu tous les systèmes et réseaux.
- Analyser les journaux pour toute activité suspecte qui pourrait indiquer une attaque.

9. **Le travail à domicile ou à l'extérieur**

- Développer une stratégie de travail nomade et former les employés pour une bonne adhésion.
- Appliquer le modèle de sécurité pour tous les périphériques.
- Protéger les données à la fois lors du transit et au repos.

#MFW4A/EIBWEBINARSERIES

Q&A

Soumettez vos questions via le "Chat" ou "Q & A"

Africa Cybersecurity Resource Centre for Financial Inclusion (ACRC)

Académie de la BEI pour la banque et la microfinance pour les PME en Afrique de l'Ouest et du Centre 2022

Les défis de la cybersécurité pour les institutions financières dans le contexte de l'expansion des services financiers numériques

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

>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

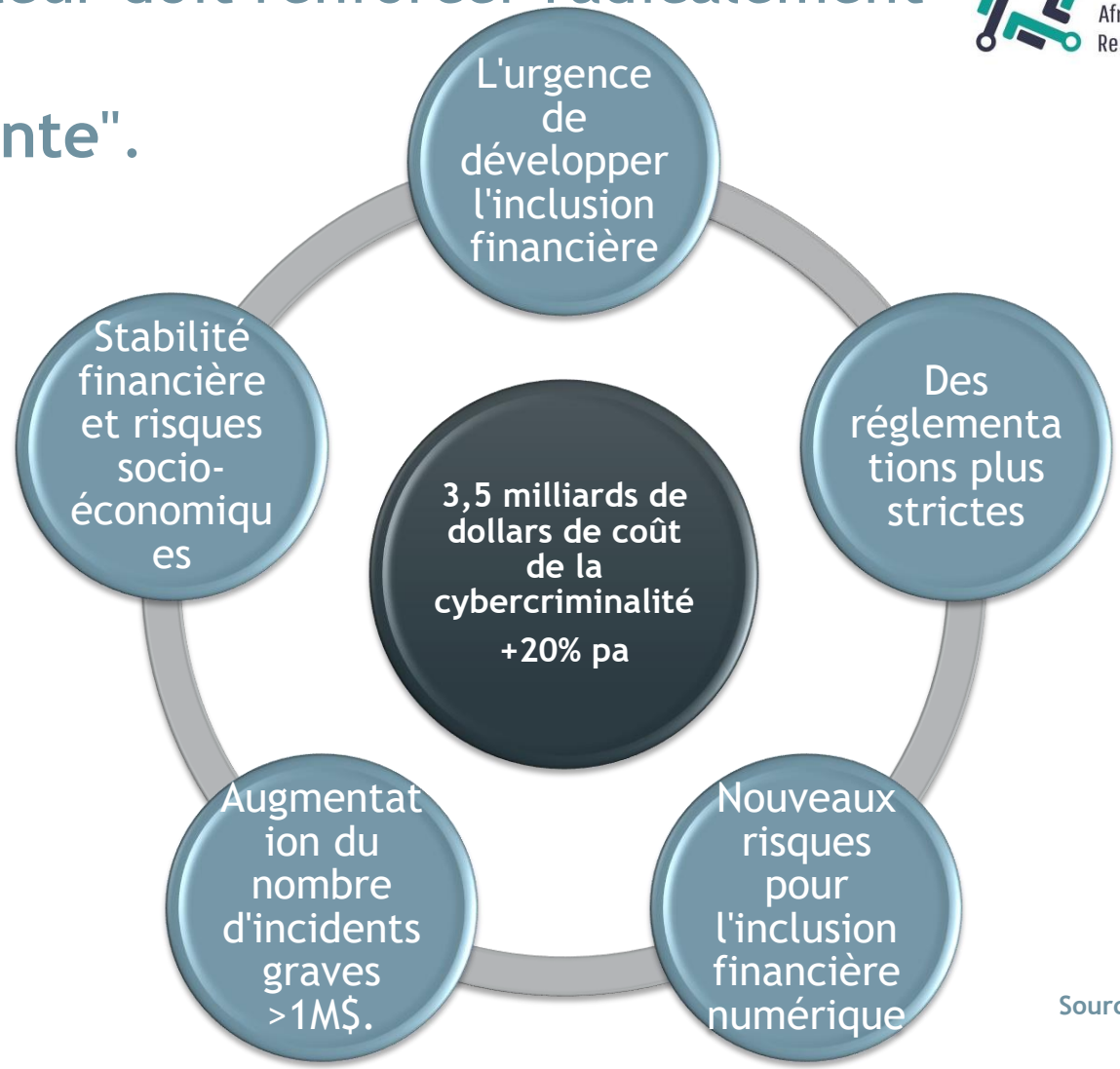
1,5 Md $ = dépenses de cybersécurité des 4 premières banques américaines

14/54 pays dotés d'agences nationales de cybersécurité

0 données et coordination embryonnaire

Sources : Verizon, IBM, Banque mondiale

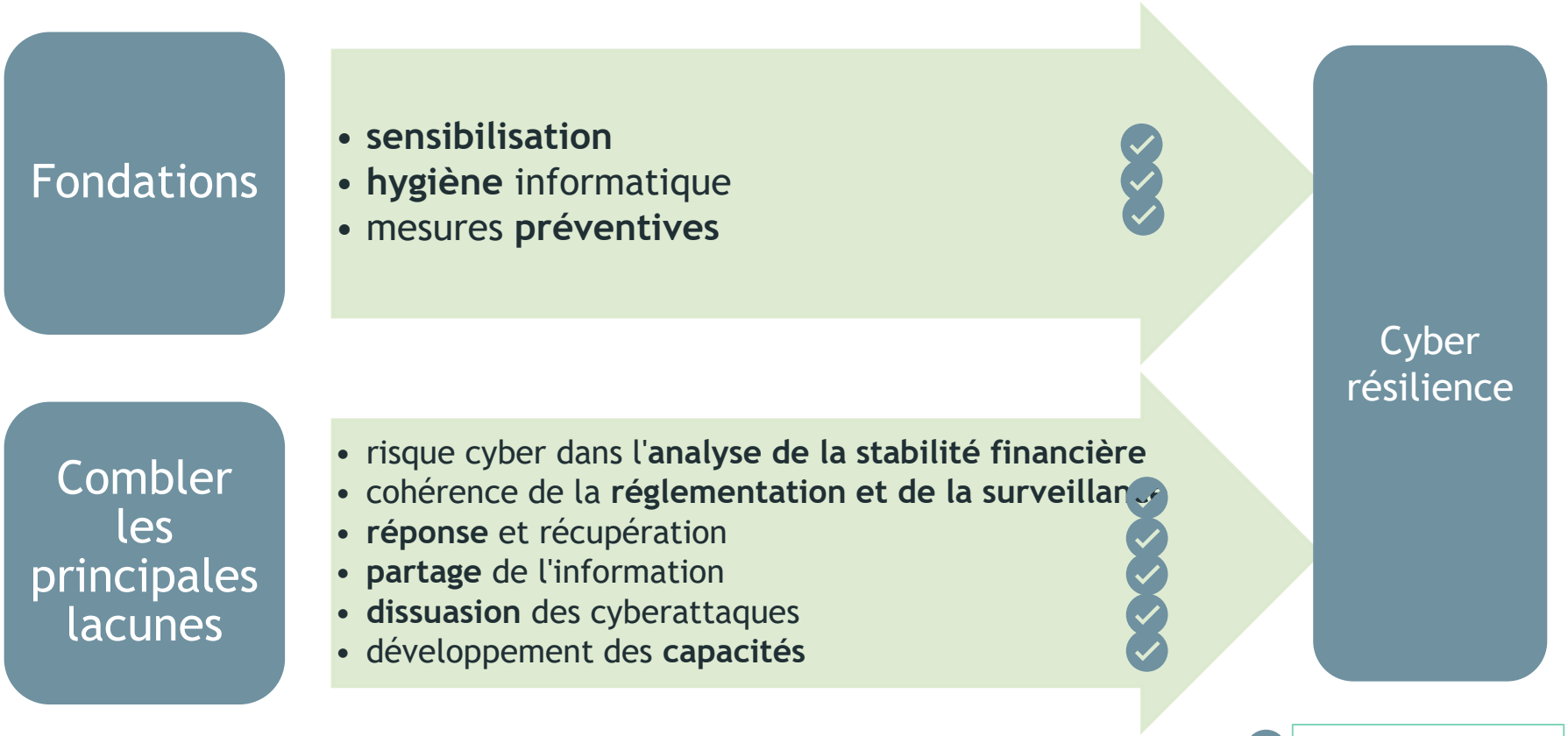
Le problème : le secteur doit renforcer radicalement la **cyber-résilience de manière "intelligente".**



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

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 combler le fossé entre les sexes, R&D

ACRC un projet et une organisation africaine

ACRC
Africa Cybersecurity Resource Centre

Consortium en partenariat public-privé à but non lucratif

>350 experts de l'agence de sécurité du Luxembourg SECURITYMADEIN.LU, SnT/Université du Luxembourg, Groupe Excellium et Suricate Solutions

Premier financement Banque Africaine de Développement

ADFI Africa Digital Financial Inclusion Facility

Un écosystème ouvert et cohérent au service de la communauté financière (microfinance, banques, fintech, régulateurs et superviseurs) avec Echange d'information, renforcement de capacité, R&D & Innovation, conseil règlementaire

- "Services de base" bien public
- Partenariats associations professionnelles, universités, organisations multilatérales, autorités, donateurs, prestataires
- Un réseau de proximité de partenaires commerciaux de référence dans les sous-régions pour Réponse aux incidents (CSIRT), Supervision de sécurité (SOC), autres services commerciaux

Déploiement sous-régional progressif

- Sénégal puis Afrique Est et Afrique de l'Ouest anglophone
- 33 experts à 3 ans, +100 à 5 ans

Conférence annuelle sur le partage d'information, la recherche et l'education

Rwanda, 20-22 octobre 2021 pendant la SAM 21

Une gamme complète de 50 services pour tous les segments

2 offres d'accompagnement cybersécurité PME/ microfinances et Fintech, en collaboration avec Assoc. Professionnelles et investisseurs

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
Liberté
Égalité
Fraternité

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

Merci.

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

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

ACRC
Africa Cybersecurity
Resource Centre

Annexes : les services

1x Centre régional de l'ACRC

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

Centre de partage et d'analyse des informations	• Fonctionnement de la plateforme de partage d'informations sur les logiciels malveillants (MISP) • Interconnexion avec les ISAC internationaux (FS-ISAC, BCE, Interpol, ...) et les CERT. • Analyser et partager les informations sur les menaces, les vulnérabilités et les meilleures 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
Capacité Bâtiment	•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'information).
Conseil stratégique et réglementaire	•Services de conseil aux banques centrales •Soutenir la mise en place et la mise en œuvre de la réglementation intelligente par les PSF •Initiatives à l'échelle du pays ou du secteur (par exemple, sensibilisation)

3x Centres sous-régionaux

Réseau de partenaires privés pour la proximité

Equipe de réponse aux incidents informatiques (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

#MFW4A/EIBWEBINARSERIES

Q&A

Soumettez vos questions via le "Chat" ou "Q & A"

Conclusion : messages clés

#MFW4A/EIBWEBINARSERIES

www.msmefinanceta.eu

Contacts

Programme d'Assistance Technique
eibtawestafrica@ipcgmbh.com

MFW4A
secretariat@mfw4a.org
+225.20.26.39.53
CCIA, Rue Jean Paul II
Abidjan, Côte d'Ivoire
mfw4a.org