DATAPROTECT
Security is our commitment

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

Livre Blanc

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

La fraude bancaire en Afrique subsaharienne - 2019

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

SIGLES ET ACRONYMES

ADD	Agence de Développement du Digital
ANRT	Agence Nationale de Réglementation des Télécommunications
API	Application Programming Interface
ASIS	American Society for Industrial Security
BSA	Business Software Alliance
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
CSP	Customer Security Programme (norme de SWIFT)
DSI	Directeur des systèmes d'information
GAFA	Google, Amazon, Facebook, Apple (on ajoute parfois Microsoft, ce qui donne GAFAM)
ISO	International Organization for Standardization
ISP	Information Systems Professional
ITCP	Information Technology Certified Professional
NIST-CSF	National Institute of Standards and Technology-Cybersecurity Framework
PKI	Public Key Infrastructure
PME	Petites et moyennes entreprises
PMP	Project Management Professional
R-D	Recherche et développement
RFID	Radio Frequency Identification
RGPD	Règlement général sur la protection des données
RSSI	Responsable de la sécurité des systèmes d'information
RVP	Réseau virtuel privé
SIEM	Security information and event management
SOC	Security Operations Center
SSCP	Systems Security Certified Practitioner
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCAC	Taux de Croissance Annuel Composé
TIC	Technologies de l'information et communications
TSCP	Transglobal Secure Collaboration Program
UEMOA	Union économique et monétaire ouest-africaine
UIT	Union internationale des télécommunications

AVANT– PROPOS

AVANT-PROPOS

Par **Ali El Azzouzi**,
Fondateur-Directeur Général, Dataprotect

Les experts DATAPROTECT ont noté avec inquiétude une recrudescence des attaques cybernétiques visant le secteur bancaire en Afrique subsaharienne depuis plusieurs mois. Chaque fois, le mode opératoire est identique. Un réseau de hackers bien organisé tire profit de l'absence de contrôles élémentaires en matière de cybersécurité de certaines institutions financières. Il s'ensuit le développement par les malfaiteurs d'un corpus des connaissances qui est mis en ligne sur le dark web moyennant rétribution.

De la fraude via les cartes prépayées jusqu'aux retraits frauduleux via le réseau Swift en passant par le Core Banking et les réseaux de transfert d'argent, rien n'est épargné. Tout ce qui est monnayable au niveau de la banque est dans le viseur des cybercriminels. Souvent, le processus commence par une simple infection d'un poste de travail au niveau d'une agence à travers une pièce jointe attachée dans un e-mail reçu. Aussi banal que cela puisse paraitre, l'histoire se termine par une prise de contrôle totale quelques semaines plus tard d'un serveur critique de l'institution financière. La même histoire se répète d'une banque à l'autre, seul le nom de l'institution change et la date du méfait.

Tout ce qui est monnayable est à risque

Cette étude est l'occasion de faire le point sur l'expérience en cybersécurité accumulée par les banques en Afrique subsaharienne au cours des dernières années. Le sondage a été très révélateur. Nous ne voulons pas garder ces données pour nous uniquement et avons décidé de les partager avec la communauté bancaire, pour la sensibiliser, pour lui démontrer que ce type de mésaventure n'arrive pas qu'aux autres, tout le monde est concerné, mais que ce n'est pas une fatalité, car, aujourd'hui, il y a moyen de se prémunir contre ce type de risque.

DATAPROTECT est présente dans l'écosystème bancaire de la cybersécurité depuis une dizaine d'années et a donc accumulé une base de « use cases » et de « runbooks ». Cette base de connaissance des modes opératoires frauduleux est maintenant très riche. Il s'agit d'un véritable trésor de guerre que nous pouvons partager avec la communauté bancaire.

La transformation digitale

Le grand enjeu du système bancaire est la transformation digitale : mise en ligne du système d'information, banque à domicile, banque en ligne, services mobiles, etc. La banque est en train de s'ouvrir sur son écosystème. Or, cette ouverture

n'est pas sans risque. Trop souvent, on privilégie les modalités fonctionnelles immédiates de la transformation digitale, tandis que la dimension sécuritaire est reléguée au deuxième plan. On y pense après coup. Il y a une raison pratique à cela : la transformation digitale est souvent confiées aux métiers qui doivent, sous la pression de la concurrence, mettre en production vite des solutions qui ne respectent pas les exigences de la cybersécurité. Or, passé un certain seuil de complexité, l'existence d'une ou plusieurs vulnérabilités devient inéluctable. Tout fonctionne tant bien que mal, jusqu'à ce qu'un lundi matin, les employés arrivent au bureau et constatent qu'une attaque a eu lieu pendant le week-end sans que personne n'ait été alerté…

La situation

De par leur nature, toutes les banques sont à risque. Les malfaiteurs examinent en permanence les moyens pour intercepter une partie de l'argent qui transite par les institutions financières. Ils préméditent leurs attaques et se concertent les uns les autres. Dans le temps, ces préparatifs avaient pour objet le braquage d'une succursale physique; aujourd'hui, ils visent le système d'information. À partir du moment où il y a flux financier, il y a menace potentielle. Par contre, ce qui diffère d'une banque à l'autre est le niveau de vulnérabilité. Une banque qui n'a pas de programme de cybersécurité, pas de centre d'opérations et de sécurité ou SOC, pas de plan de sensibilisation, court un grand danger.

Par ailleurs, force est de constater que nombre de banques n'ont pas su gérer la transition entre un système propriétaire fermé et un système ouvert interopérable. Les banques continuent à raisonner en termes de sécurité traditionnelle. Elles transposent sur le plan informatique des notions comme la défense du périmètre en multipliant les pare-feux alors que c'est inadapté ou à tout le moins insuffisant. Or, la menace actuelle se joue des mesures statiques : elle contourne les mesures de protection, ou encore, elle provient de l'intérieur même de l'institution. Les banques traversent une période de changement qui nécessite de remettre en question tous les paramètres de la sécurité : pour cela, il faut innover et investir de manière judicieuse dans une sécurité de type nouveau – la cybersécurité.

Les attaques

L'explosion spectaculaire du nombre de cyberattaques dans le secteur financier africain s'explique en grande partie par l'apparition du phénomène de « crime comme service ». Aujourd'hui, on peut acheter sur le web invisible des outils pour briser les mots de passe, monter une attaque par déni de service ou prendre le contrôle d'un ordinateur à distance, sans compter que l'on peut acheter des informations sensibles en masse (numéros de passeport et de cartes de crédit, données bancaires, etc.) Désormais, tout criminel peut avoir accès à des outils malveillants sans pour autant avoir besoin de compétences techniques. L'underground s'est agrandi pour englober des acteurs sans rapport avec l'informatique, mais qui appartiennent plutôt au crime organisé.

Le Cybercrime est maintenant vendu comme un service

Dans un premier temps, ces pirates professionnels ont profité de la désorganisation des banques en Afrique subsaharienne pour commettre leurs méfaits. Quand les banques ont commencé à adopter les règles de base de l'hygiène sécuritaire, les malfaiteurs ont très vite monté d'un cran en termes d'outils utilisés et de mode opératoire. N'oublions que ce sont des criminels professionnels. Désormais, ils utilisent des vulnérabilités de type «zero-day» qui comptent parmi les outils les plus pernicieux et dangereux. La faille subsiste jusqu'à ce qu'une solution soit mise en place par l'éditeur de logiciel ou qu'il distribue un correctif aux usagers. Pendant cette période, il suffit qu'un pirate particulièrement doué découvre l'existence de l'une ou l'autre vulnérabilité «zero-day» pour qu'il s'empresse de la vendre sur le web invisible.

La plupart des logiciels

Prévenir le crime avant qu'il ne survienne

commerciaux comportent des vulnérabilités qui sont corrigées par leurs développeurs eux-mêmes (Microsoft, Adobe, Oracle, etc.) Pour tous les usagers, cela signifie que la première mesure de cybersécurité consiste à mettre à jour les logiciels sur une base régulière. Cependant, toutes les vulnérabilités ne sont pas identifiées par les éditeurs. Il convient donc de consulter des centres de veille de vulnérabilités qui émettent des alertes de façon systématique pour chaque type de systèmes d'information – citons à titre d'exemple, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CRERT-FR), l'United State Computer Emergency Readiness Team (CERT-US) ou le Zero Day Initiative (ZDI).

Intelligence artificielle

Les institutions n'ont pas le choix et doivent suivre et même anticiper la course technologique avec le crime organisé. L'arme de choix de cette concurrence est l'intelligence artificielle (IA). Il est impératif de recourir à des solutions de cybersécurité qui intègrent des moteurs d'IA et de détection avancée qui permettent d'effectuer de l'analyse comportementale. C'est particulièrement important quand on sait que la majorité des cyberattaques ont une origine interne : qu'il s'agisse d'un employé malhonnête ou simplement négligent. Dans les deux cas, il ne suffit plus de protéger le système d'information, mais de se concentrer sur les utilisateurs : étudier leurs comportements et détecter une anomalie dès qu'elle survient.

Les moteurs d'IA s'appuient sur des modèles d'analyse qui ne sont pas forcément nouveaux, mais tirent profit du « Big Data » pour les appliquer à des volumes de données considérables et jusqu'ici largement inexploitées, à commencer par les logs des systèmes connectés à l'infrastructure informatique. Plus le nombre de données est important plus les résultats seront optimaux. Il est ainsi possible de produire en très peu de temps des algorithmes qui correspondent à des modes opératoires frauduleux. Au moment où le marché de la sécurité vit une pénurie de talents, ce recours à l'IA est indispensable pour renforcer la cybersécurité du secteur financier tout en minimisant les coûts.

SOC

Quand une institution financière introduit un SOC dans sa stratégie de cybersécurité, cela ne se limite pas à une démarche technologique, il faut aussi mettre en place un protocole de communications entre le fournisseur et le client, un protocole de gestion des incidents, un protocole de gestion de crise, c'est-à-dire toute une série de processus qui relèvent du volet organisationnel. Qui plus est, il existe aussi un volet humain qui consiste à former et à sensibiliser en permanence des analystes SOC.

Le SOC a pour fonction d'exercer une surveillance efficace sur un périmètre informatique déterminé et un suivi des incidents de bout en bout. Il transforme les données brutes qui sont générées par l'équipement informatique en incidents et, s'il y a lieu, en alertes. Le SOC notifie alors le danger en cours au client. Mais le rôle du SOC n'est pas seulement réactif. Il exerce aussi une activité de veille technologique basée sur deux sources. Il y a, en premier, le suivi des alertes. Chaque alerte fait l'objet d'une fiche de retour d'expériences qui est enregistrée dans un système d'archivage. Il est ainsi possible de procéder à des investigations (forensics) et de réutiliser les solutions trouvées en cas de récidive d'incident similaire. Il y a ensuite la veille technologique qui peut faire appel à des sources externes (type CERT).

Le SOC permet ainsi de traiter les petits signaux annonciateurs de la fraude avant qu'ils ne grandissent et ne se transforment en crise institutionnelle. Un client de DATAPROTECT posait la question de la pertinence de son recours à un SOC externe : « Il y a neuf mois que je suis abonné au service et je n'ai pas vu passer d'alertes. » Heureusement! C'était la preuve que la plateforme du SOC offrait un bon niveau de détection et de grandes capacités de corrélation des événements de sécurité. Grâce à l'usage massif de l'IA, son retour d'expérience et ses abonnements

aux systèmes internationaux de veille, le SOC de DATAPROTECT avait été capable de localiser très vite les systèmes infectés et neutraliser les menaces, sans avoir eu à inquiéter le client.

Gestion de crise

Avoir une stratégie avancée de cybersécurité ne dispense pas de prévoir le pire – une attaque réussie. Or, que se passe-t-il quand la crise frappe? La première réaction de la banque est de fermer le service attaqué pour stopper l'hémorragie et, sitôt l'opération effectuée, l'enjeu qui s'impose est : quand allons-nous pouvoir rouvrir? En effet, la dimension « business » impose tout de suite sa loi d'airain. Tout le monde téléphone : les clients, les partenaires, les pouvoirs publics afin de protester, exposer son cas particulier, exiger une solution rapide, parfois même menacer. Le chaos s'installe et plus le temps passe, plus la crise enfle et devient majeure. La banque est prise dans un dilemme : arrêter les activités attaquées, reprendre le plus tôt possible ces mêmes activités.

Toute crise est aggravée par de mauvaises communications avec les publics internes et externes. Il arrive souvent que les clients de la banque attaquée apprennent la nouvelle par les journaux. Une telle situation est inadmissible. Une cyberattaque pour une banque est comme un vol retardé ou annulé pour une compagnie aérienne : les intérêts du client doivent venir en tête des préoccupations. Quand une institution financière suspend le service de paiement par carte bancaire, il est indispensable que les utilisateurs soient mis au courant (1) de l'interruption et (2) du la date prévue pour la reprise du service. Si elle omet de le faire, elle brise le climat de confiance entre la banque et le client – cela laisse des traces.

Le protocole de communication est particulièrement important, car si un incident survient à trois heures du matin, il faut savoir qui appeler sans avoir besoin de faire des recherches chronophages et, si la personne ne répond pas, il faut avoir un numéro de relève immédiatement disponible et même un troisième pour parer à toute éventualité. Tout un processus d'escalade doit être prévu dans les moindres détails qui peut aller jusqu'au président de la banque. Il faut pouvoir l'appeler un dimanche matin si l'ampleur de la crise le justifie.

Dans certaines circonstances, il est impossible d'utiliser la messagerie, car elle peut également se trouver attaquée. Il arrive souvent que l'agresseur cherche à intercepter les communications entre l'organisation et son fournisseur de sécurité. En tout état de cause, il faut prévoir un système de communication parallèle à la messagerie habituelle pour garantir la confidentialité des opérations de gestion de crise.

Ces situations d'urgences doivent être consignées dans un Plan de réponse aux incidents. Il s'agit d'un document où on indique comment on va endiguer l'attaque, minimiser les dégâts et les impacts, communiquer avec les publics internes et externes, etc. Rien ne doit être improvisé dans l'urgence du moment. Tout doit être planifié en fonction des règles de l'art et des cas comparables.
Malheureusement, la plupart des banques en Afrique ne disposent pas d'un tel plan.

La formation et la sensibilisation

La formation et la sensibilisation en cybersécurité font le plus souvent l'objet d'actions éparpillées et ponctuelles qui visent essentiellement les équipes de TI, plutôt que l'ensemble des employés. Ces efforts ne mènent à rien et constituent un gaspillage de fonds. En effet, une stratégie d'éducation vise à modifier le comportement et les pratiques des publics cibles : employés, cadres, direction, etc. Sa composante de sensibilisation doit obligatoirement toucher tous les employés de la banque afin de les rendre réceptifs à des thèmes souvent connus, mais qu'ils ont tendance à penser qu'ils ne les concernent pas. Comme les activités de sensibilisation sont brèves, elles doivent être marquantes et répétées en continu. La composante de formation est plus formelle et plus longue, mais elle va plus en profondeur, inculque des notions nouvelles et vise des groupes spécifiques d'employés.

Les ressources humaines sont au centre de la Cybersécurité

Inculquer une culture de Cybersécurité à tous les employés

Certaines entreprises, vont même plus loin : elles formalisent leurs exigences en matière de vigilance et de protection et les inscrivent dans le contrat de travail de chaque employé. La cybersécurité fait partie de sa description de tâches avec les conséquences que cela implique : elle devient en facteur de promotion et d'augmentation salariale au même titre que ses autres responsabilités, son ancienneté, ses résultats annuels, etc. Il va de soi qu'une telle approche a un effet mobilisateur sur l'employé qui gagne l'assurance que la nouvelle charge de travail introduite par la cybersécurité est reconnue à sa juste valeur.

Le défi de toutes les institutions financières est de créer les conditions propices à l'adoption d'une culture de sécurité par tous ses employés et non seulement les spécialistes de TI. Il ne s'agit pas de freiner le développement de nouveaux métiers, de nouveaux produits et services, mais il faut y intégrer la dimension sécuritaire. Une banque est protégée dès lors que ses employés raisonnent en termes de sécurité dans chacune de leurs actions et surtout quand ils lancent de nouveaux projets. La sécurité cesse alors d'être une option pour devenir un réflexe systématique. La sécurité doit devenir la seconde nature des employés dans leur activité quotidienne.

Les assurances

Il y a des assurances qui couvrent le cybercrime, mais il s'agit d'un marché encore naissant en Afrique. Ce que l'on peut appeler la cyberassurance a besoin de tout un écosystème pour se développer. En effet, pour lancer un produit cyber, une compagnie d'assurance a besoin de déterminer le montant de la prime en fonction des conditions d'exploitation du système d'information de la banque à assurer. Pour cela, il convient d'évaluer les trois composantes de la cybersécurité de la banque : nature des applications techniques de cybersécurité déployées, évaluation des mesures de gouvernance mises en place et, enfin, existence d'un plan de sensibilisation/formation à destination des employés.

Comme les assurances n'ont généralement pas l'expertise technologique et professionnelle pour procéder à cette évaluation, elles ont besoin de s'adosser à l'expertise existante, soit en embauchant du personnel qualifié, ce qui est long et coûteux, soit en nouant des alliances avec des firmes de conseil en cybersécurité. Mais les besoins en expertise de cybersécurité des assureurs ne se limitent pas à la détermination de la prime. Ils doivent ensuite estimer les coûts probables de la remise en service des systèmes attaqués. Or, il n'existe pas suffisamment de données historiques pour évaluer les coûts de réparation, sans compter les indemnités négociables à verser aux clients et aux fournisseurs ou encore les pénalités non négociables qui peuvent être infligées par les diverses autorités de réglementation.

Dans une première phase, la cyberassurance s'inspire des méthodes d'estimation du risque opérationnel (dont elle fait d'ailleurs partie). Par la suite, au rythme de l'accroissement des données disponibles, les assureurs pourront utiliser des modèles plus quantitatifs issus de la théorie des risques extrêmes. Le marché de la cyberassurance est très limité en Afrique, mais il est appelé à se développer. L'enseigne sud-africaine de grande distribution Foschini Group et la compagnie Mycybercare ont annoncé au début 2018 le lancement d'une assurance contre les cyber-fraudes, qui permettra aux acheteurs de téléphones mobiles d'être couverts contre les pertes financières causée par la cybercriminalité. Il est probable que c'est dans le secteur financier fortement arrimé à la conjoncture internationale que les produits de cyberassurance se répandront en premier.

Que faire?

Aujourd'hui, pour ainsi dire toutes les banques sont sensibilisées au cybercrime interne et externe. Les principes d'une hygiène de base sont connus et demandent seulement à être mis en place. Les stratégies pour rallier et responsabiliser les employés sont également connues. Le grand

problème pour les institutions financières, grandes ou petites, est de dégager les budgets nécessaires à la sécurisation de leurs activités en voie de numérisation rapide. Les ressources internes en TI de l'organisation ne suffisent pas à la tâche car la cybersécurité est rapidement devenue une discipline qui dépasse largement le cadre des TI, comme nous l'avons vu ci-dessus, pour englober la gouvernance, la formation continue et les communications.

Comment se concentrer sur son activité centrale tout en demeurant à la fine pointe de cette cybersécurité en pleine ébullition ? L'analyse des résultats de l'étude « La fraude bancaire en Afrique subsaharienne » nous apprend que plus de la moitié des institutions financières (très exactement 55%) ont recours à une firme spécialisée. Typiquement, une banque ne confie pas la totalité de sa cybersécurité à un sous-traitant, elle lui délègue les tâches hautement techniques et conserve à l'interne les tâches reliées de près aux ressources humaines. La sous-traitance ou infogérance permet de contrôler les coûts et de les planifier. L'autre grand avantage de l'infogérance est qu'elle permet de mutualiser l'acquisition et la maintenance de systèmes complexes comme le SOC sont qui onéreux et nécessitent un personnel à la fois nombreux et qualifié. Peut-être plus important encore est la mutualisation du retour d'expérience. Si un groupe de criminels attaque une banque avec ou sans succès, il va immanquablement réitérer l'attaque aux dépens d'une autre banque. Le mode opératoire restera le même, seules les circonstances de l'attaque sont appelées à varier. Il va de soi que le prestataire de services de cybersécurité qui a déjà eu affaire avec ce mode opératoire part avec une longueur d'avance quand il s'agira de le mettre en échec.

L'infogérance doit nécessairement faire partie de la stratégie de cybersécurité de la banque du XXIe siècle. Reste à choisir un bon prestataire de services pour veiller à la sécurité du capital financier et informationnel de la banque ainsi qu'à sa réputation. Le prestataire doit obligatoirement fournir des outils et des processus qui soient conformes avec les exigences de sécurité de la Banque des règlements internationaux (Bâle I, Bâle II et Bâle III), de SWIFT et, bien sûr, de la Banque Centrale des États de l'Afrique de l'Ouest (BCEAO). L'un des moyens les plus sûrs pour discriminer parmi les prestataires est l'examen de sa liste de clients afin de déterminer quel est son bassin d'expérience.

FAITS SAILLANTS

01 TENDANCES ACTUELLES

Le secteur financier est entré dans une période de transformations profondes sur la terre entière. Tout a commencé avec la multiplication des néobanques qui misent sur le numérique et la téléphonie mobile pour réinventer les services financiers. Peu après est apparue une nouvelle industrie : les fintechs qui simplifient l'utilisation des comptes bancaires à bas coûts. Bousculées, les banques ont inventé le concept d'*Open Banking* qui consiste à ouvrir leurs systèmes d'information à des tiers et à partager avec les fintechs une partie de leurs données clients.

La bancarisation de l'Afrique a enfin décollé : le nombre de nouveaux comptes augmente d'environ 3% par an. Il ne faut donc pas s'étonner si le secteur bancaire africain est un des plus dynamique au monde : le deuxième en termes de croissance et de profitabilité. L'autre phénomène qui contribue à dynamiser le secteur financier africain est le téléphone mobile qui a été rapidement détourné de sa fonction initiale pour devenir un outil financier. Ce développement rapide du secteur financier a sa contrepartie qui est l'explosion concomitante de la cyberfraude. Or, les banques sont des cibles privilégiées des cybercriminels grâce aux programmes malveillants conçus spécialement en fonction du système financier.

La cybercriminalité se répand d'autant plus vite que le cadre législatif et réglementaire de la plupart des pays d'Afrique est inadapté et, quand il existe, mal appliqué. Au sein de cet environnement incertain, les banques constituent un cas à part. En effet, elles doivent respecter la réglementation internationale (accords de Bâle) et régionale (Banque Centrale des États de l'Afrique de l'Ouest). Pour satisfaire à leurs obligations, les banques sont donc incitées à investir en cybersécurité. Elles y ont même intérêt.

01 TENDANCES ACTUELLES

1.1 – Transformation digitale du secteur bancaire

Partout dans le monde, le secteur bancaire connaît une mutation radicale. Les banques se livrent une course effrénée pour offrir leurs services en ligne – pas quelques services : tous les produits financiers sont concernés. L'épicentre de cette révolution est l'Asie et d'abord la Chine où le dynamisme technologique trouve à s'exprimer dans un marché suffisamment vaste pour absorber toutes les innovations. L'Afrique a sauté dans le train en marche et, pour des raisons qui lui sont propres, a misé avant tout sur les paiements mobiles.

La tendance est irréversible car la technologie le permet et que le client l'exige : il ne veut pas se déplacer, parfois loin de chez lui, pour faire la queue. Il veut avoir une vue globale de ses actifs financiers instantanément, où qu'il se trouve et, surtout, faire des transactions en ligne.

Cela signifie pour la banque : numériser ses processus d'affaires. Tout a commencé avec l'automatisation des tâches du système bancaire de base (*core banking*). Il s'agit principalement de la tenue de comptes, de la gestion de l'épargne, des crédits et des paiements. Avec la montée en puissance des technologies de l'information, les banques ont eu tendance à confier leur gestion à des départements spécialisés, qui excellaient en informatique pure, mais souvent isolés des activités proprement financières de l'établissement.

Depuis les années 2000, pour répondre à de nouveaux besoins nés de la technologie et à une concurrence de plus en plus présente et diversifiée, les banques se sont engagées dans la dématérialisation de l'interface client. Cela ne va pas sans peine car la plupart des banques sont tributaires des anciens *core banking*. L'amélioration de l'interface-client se limite bien souvent à permettre aux clients de consulter leurs comptes, d'effectuer des paiements en ligne et de virer des fonds d'un compte à l'autre.

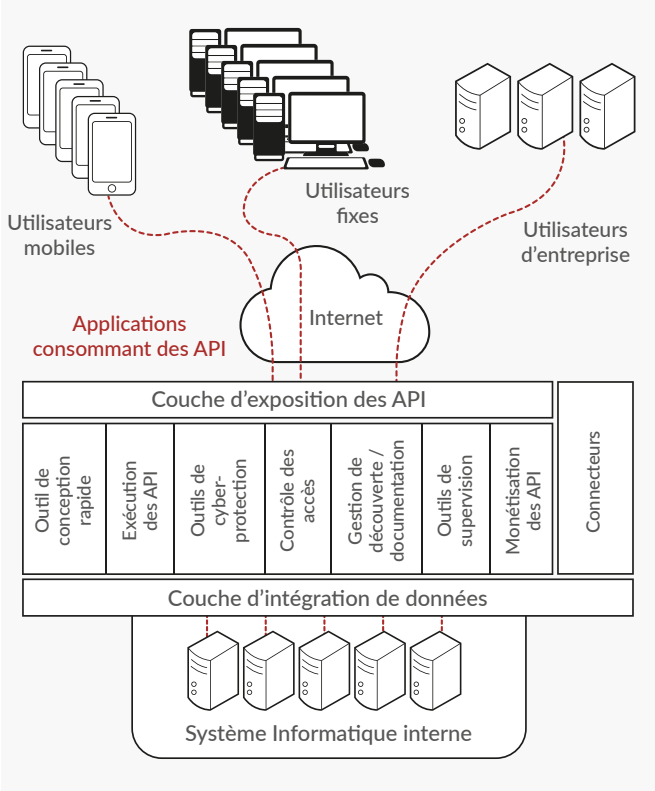
Au même moment, surviennent les néobanques qui misent sur le numérique et la téléphonie mobile pour réinventer les services financiers, faciliter la vie des clients via une offre simplifiée, tout en réduisant drastiquement les frais bancaires en renonçant à exploiter un réseau d'agences classique. Il n'y a pas de modèle unique de néobanque. Certaines sont des établissements 100% numérique, d'autres sont des filiales de banques étrangères, d'autres encore sont des extensions d'un réseau de télécommunications. Il faut enfin compter avec les GAFA qui touchent désormais tous les domaines d'activités y compris les services financiers.

À partir du bouillon de culture de l'innovation financière, une nouvelle industrie apparaît dans les années 2010 : les fintechs – contraction de « finance » et de « technologie »[1]. Comme les néobanques dont elles sont souvent les pourvoyeuses, les fintechs exploitent des canaux non traditionnels et offrent une grande simplicité de gestion des comptes bancaires, une utilisation plus conviviale et des tarifs plus attrayants. Leur modèle d'affaire est celui de la *start-up* avec ce que cela implique en termes de vitesse d'innovation, mais aussi de risque : leur capitalisation est improvisée au rythme des rondes de financement.

Bousculées, les banques ont dû se remettre en question et elles ont inventé le concept d'*Open Banking*. Celui-ci consiste à ouvrir les systèmes d'information des banques à des tiers et à partager avec les fintechs une partie de leurs données clients. La clé de cette coopération a pris la forme des *Application Programming* Interface (API). Grâce à ces interfaces de programmation, les fintechs peuvent mettre au point très vite des services personnalisés mettant généralement à profit des *robo-advisors* très sophistiqués.

1 Fintech : innovation financière fondée sur la technologie, susceptible de donner lieu à de nouveaux modèles stratégiques, applications, processus ou produits ayant un impact important sur les marchés et établissements financiers ainsi que sur la prestation de services financiers. Définition du Conseil de stabilité financière du G20 (en anglais : Financial Stability Forum).

FIGURE 1 - COMMENT FONCTIONNENT LES API



Source : « API : des plateformes de gestion agiles », in Solutions numériques, 15 juin 2017 (adaptation Sciencetech/DataProtect).

La vitrine technologique de ce nouveau monde financier est sans conteste la Chine qui abrite le plus vaste marché du paiement numérique avec près de la moitié des transactions mondiales. La combinaison d'une faible bancarisation avec un taux d'équipement en smartphones élevé, a suscité le développement de fintechs de toutes sortes dont la plus célèbre est *WeChat Payment*. Un portefeuille mobile a été intégré dans l'application de messagerie instantanée *WeChat*, rendant le transfert d'argent aussi simple et rapide que l'envoi d'un courriel. C'est un écosystème complet qui héberge, sur sa plate-forme, une grande variété de fonctionnalités, dont neuf relevant des services financiers. Il est ainsi possible de réaliser des transferts d'argent, d'accéder à des produits d'assurance et de gestion du patrimoine, et même à du microfinancement, directement depuis l'application mobile. Le service *WeChat* compte un milliard d'utilisateurs.

Son concurrent immédiat Alipay en compte 900 millions. C'est le service de paiement d'Alibaba, l'équivalent chinois d'Amazon. Alipay a évolué de portefeuille numérique à facilitateur de style de vie. Les utilisateurs peuvent commander un taxi, réserver un hôtel, acheter des tickets de cinéma, payer des factures d'électricité, prendre des rendez-vous médicaux ou acheter des produits de gestion de fortune directement dans l'appli. En plus du paiement en ligne, Alipay s'étend dans les paiements directs en magasin à la fois en Chine et au-dehors. Des dizaines de millions de commerçants en dur acceptent désormais Alipay en Chine et son service en magasin couvre plus de 36 pays et régions du monde[2]. L'objectif de ces fintechs géants est de multiplier les services intégrés pour proposer un écosystème complet aux utilisateurs sans les faire sortir de la plateforme.

En Afrique subsaharienne, les fintechs rayonnent à partir de trois pays : Afrique du Sud, Kenya et Nigeria. Le cabinet conseil EY estime que le secteur des fintechs en Afrique subsaharienne comprend 260 entreprises en majorité à capitaux africains et a connu une croissance annuelle d'environ 24% au cours des 10 dernières années[3]. Il s'agit d'un secteur en grande partie lié aux plateformes d'argent mobile, voire dans certains cas aux entreprises de télécommunications elles-mêmes. Certaines fintechs explorent cependant des créneaux diversifiés : analytique de données, agrégation de commerce électronique, cybersécurité, etc.

1.2 - Le secteur financier africain est en plein essor

La bancarisation de l'Afrique a enfin décollé. Il y a une raison structurelle à ce nouveau boom : l'Afrique est le continent qui connaît la plus forte expansion démographique au monde. Sa population est très jeune, c'est surtout le cas en Afrique subsaharienne où 43% des habitants ont moins de 15 ans. L'éducation y croît rapidement : aujourd'hui, 70% des enfants terminent leurs études primaires, contre 45% en 1971[4].

Pour les banques, cela signifie que le nombre de nouveaux comptes augmente d'environ 3% par an. Il ne faut donc pas s'étonner si le secteur bancaire africain est l'un des plus dynamique au monde : le deuxième en termes de croissance et de profitabilité – derrière l'Amérique latine.

2 "How to flourish in an uncertain future: Open banking", Deloitte, 2017, 31 pages. - Alexia Verdier, "Ces géants de la fintech venus de Chine", Unow, 27 février 2017. - Andreea Grecu, Zineb Ahmed et Gaelle Bisson, "Le modèle chinois d'open banking, futur modèle européen ?", Revue Banque, 14 juin 2018. - Juliette Raynal, "L'Open Banking pousse les banques vers des services extra-financiers", La Tribune, 14 janvier 2019.
3 "FinTechs in Sub-Saharan Africa", Ernst and Young (EY), 2019, 21 pages. Cf. p. 4.
4 "The geography of education in Africa", The Economist, 21 février 2019.

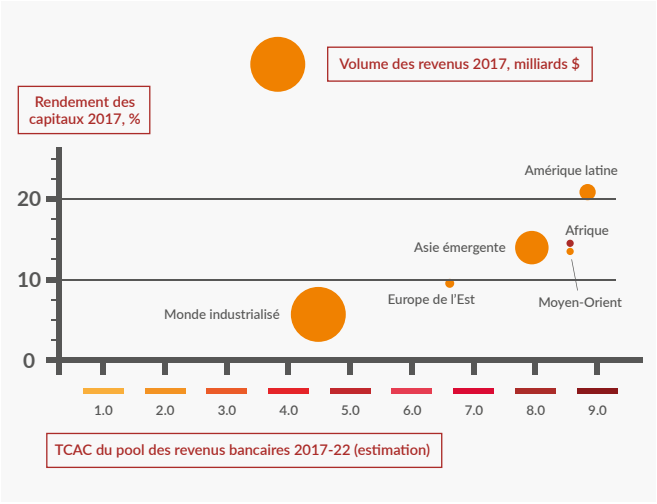
01 TENDANCES ACTUELLES

Le secteur bancaire est marqué par le développement rapide des investissements internationaux[5]. L'autre phénomène qui contribue à dynamiser le secteur financier africain est technologique. L'adoption massive du téléphone mobile est en passe de faire de l'Afrique le continent numérique du XXIe siècle.

Or, le téléphone est devenu un outil financier. Il y a eu un « miracle » africain. À la faveur d'un phénomène d'appropriation technologique, une population largement rurale et sans accès au système financier, a détourné le téléphone mobile de sa fonction initiale et en a fait un moyen de paiement de personne à personne. Il suffit d'utiliser une partie des montants versés pour la recharge de la carte SIM. La simplicité du système est telle que son succès a été immédiat.

Aujourd'hui, l'offre en argent mobile tend à se diversifier au-delà du seul paiement pour englober les transferts internationaux, les frais de scolarité, le versement d'argent vers un compte bancaire et même, dans certains pays, le prélèvement de l'impôt! Il ne s'agit pas de véritables comptes bancaires : les opérateurs de télécommunications ne peuvent pas consentir de crédit à leurs clients. Même celles qui ont obtenu une licence d'émetteur de monnaie électronique demeurent limitées par la réglementation en vigueur.

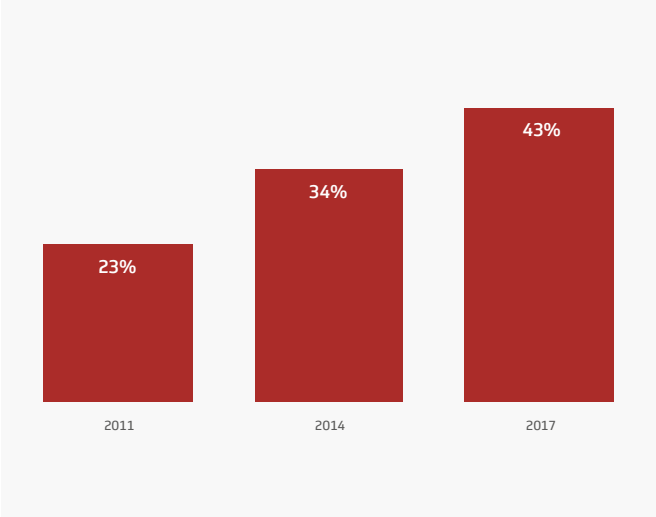
FIGURE 2 - DYNAMISME DU SECTEUR BANCAIRE AFRICAIN



Source : McKinsey Global Banking Pools, 2017

Ces services sont offerts par les opérateurs ou par des *start-ups* spécialisées en développement des technologies financières – les fintechs. Au total, des milliers d'applications pour téléphones intelligents sont nées qui réinventent la nature du secteur financier pour coller à la réalité africaine.

FIGURE 3 - EXPLOSION DU TAUX D'INCLUSION FINANCIÈRE EN AFRIQUE SUBSAHARIENNE



Source : Global Findex Database, World Bank, 2018.

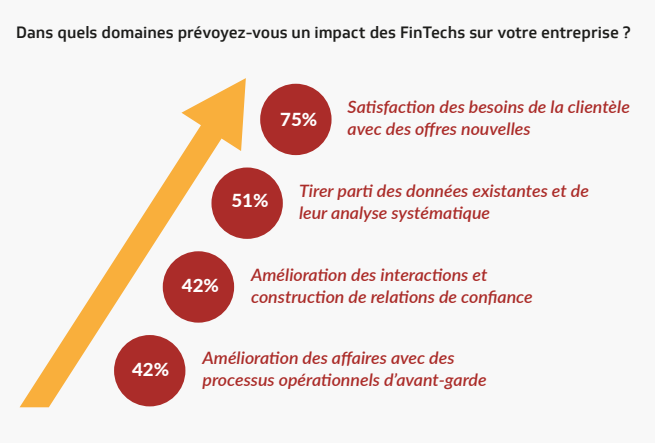
Pourtant, l'argent mobile a exposé des millions de personnes à la fluidité des services financiers. Dans bien des cas, les détenteurs d'un compte d'argent mobile ont été incités à ouvrir un véritable compte bancaire. De leur côté, les banques passent souvent des accords avec les compagnies de téléphone pour desservir les régions rurales où elles n'ont pas de succursales. Les deux industries sont tour à tour concurrentes et partenaires.

5 "Africa Payments: Insights into African transaction flows", SWIFT, 2018, 40 pages. Cf. p. 3. Nicholas Megaw and Heba Saleh, "Morocco banks expand to west Africa for greater if riskier returns", Financial Times, 23 janvier 2019. Paul Derremaux, "Banques françaises en Afrique subsaharienne: vers un nouveau repli", L'Opinion, 14 octobre 2018.

La téléphonie mobile sert d'ailleurs de plateforme privilégiée pour le développement des technologies financières ou fintechs. Les fintechs ont permis à l'argent mobile de sortir du cadre restrictif du paiement pour s'étendre aux prêts et aux assurances, mais il s'agit bien souvent de services très ciblés comme le *crowdfunding*, le microcrédit et le prêt interpersonnel. Dans le monde l'assurance, les fintechs vont mettre au point des offres très concrètes, en prise directe avec les préoccupations de leurs clientèles comme une couverture sur la récolte ou sur les frais funéraires[6].

Un autre champ d'application aux activités des fintechs est la gestion du risque. En effet, les banques africaines ont un des plus hauts taux de risque au monde. L'emblématique fintech sud-africaine JUMO a mis au point un système d'agrégation des données au moyen d'algorithmes spécialisés qui permet à sa clientèle d'emprunter de petits montants en temps réel tout en abaissant le taux de défaut de paiement. Les banques Barclays Africa et Old Mutual travaillent désormais avec JUMO pour améliorer leurs services de prêts[7].

FIGURE 4 - POURQUOI LES BANQUES S'INTÉRESSENT-ELLES AUX FINTECHS ?



Source: PwC, "Disrupting Africa: Riding the wave of the digital revolution", 2016.

Il convient de préciser qu'en Afrique les fintechs ne menacent généralement pas les banques : elles attaquent plutôt le vaste désert financier où aucun service n'est accessible. Elles construisent une infrastructure financière à partir de zéro. Au total, il existe à présent plus de plus de 300 start-up dans la fintech en Afrique. Ce secteur a vu ses investissements exploser en quelques années à peine, même si les fonds sont très inégalement disponibles (principalement Nigeria, Afrique du Sud et Kenya)[8].

Le résultat est que près de 200 millions de personnes possèdent un compte bancaire ou mobile en Afrique subsaharienne, ce qui représente 43% de la population âgée de 15 ans ou plus. Même si une grande partie de la population est toujours exclue du système financier, celui-ci dispose désormais d'une masse critique (voir figure 3). Les récents progrès proviennent non seulement de l'arrivée des services financiers par téléphonie mobile, mais aussi de la nouvelle offre de services en ligne par les banques traditionnelles.

1.3 - La contrepartie de la bancarisation : essor parallèle de l'underground

1.3.1 - Préhistoire de la cybercriminalité en Afrique

Ce développement rapide du secteur financier a sa contrepartie qui est l'explosion concomitante de la cyberfraude. La plus connue est le scam 419, en référence au Code pénal nigérian qui les sanctionne, puisque c'est dans ce pays que ce type de fraude est né. Le procédé consiste à se faire passer pour une veuve éplorée qui souhaite faire sortir des fonds de son pays. La prétendue veuve explique à son interlocuteur qu'elle possède de l'argent et lui fait part de son besoin de le transférer rapidement sur son compte, en échange de quoi, elle lui offre un généreux pourcentage sur cette somme pour entamer la transaction, le « Client » doit déposer de l'argent sur un compte.

L'Afrique francophone n'est pas en reste qui a vu proliférer les « brouteurs » – comme le mouton qui se nourrit en broutant dans les champs sans se fatiguer. Leur spécialité est l'amour en ligne. Un Don Juan professionnel contacte des femmes sur les réseaux sociaux en Europe ou en Amérique du Nord – à moins que ce ne soit une femme fatale qui jette son dévolu sur des hommes – pour leur promettre le grand amour et fidélité éternelle. Quelle que soit l'histoire, elle débouche immanquablement sur une demande d'argent à laquelle on ne peut se soustraire sous peine de passer pour un goujat.

6 "Fintech in Sub-Saharan African Countries", Fonds monétaire international (FMI), 2019, 51 pages. Cf. pp. 10-1.
"Disrupting Africa: Riding the wave of the digital revolution", PwC, 2016, 53 pages. Cf. p. 15.
7 "Roaring to life: Growth and innovation in African retail banking", McKinsey & Company, 2018, 54 pages. Cf. p. 4
8 Yomi KazeemAugust, "Why African fintech startups are becoming even more attractive for investors", Quartz Africa, 06 août 2017..

01 TENDANCES ACTUELLES

1.3.2 - Cyberattaques et cyberescroquerie : les deux volets de la cybercriminalité organisée

Ces arnaques initiales peuvent prêter à sourire tant leur mode opératoire est simpliste – elles ont pourtant fait leur lot de victimes. Elles ont aujourd'hui donné naissance à une fraude autrement plus sophistiquée. Il est possible de diviser la cybercriminalité en deux : cyberattaque et cyberescroquerie. La cyberattaque correspond à une intrusion informatique (non ciblée dans le cas des virus et autres programmes malveillants ou ciblé), un sabotage (*botnet*, programme malveillant ou déni de service) ou encore un rançongiciel qui rend inutilisable l'entièreté d'un serveur en le chiffrant. De son côté, la cyber-escroquerie relève du champ de l'ingénierie sociale ou hameçonnage (*phishing*) avec des fraudes allant de la divulgation d'information à l'arnaque au président.

Sans surprise, le type de cybercriminalité qui domine en Afrique subsaharienne est la cyberescroquerie – sans doute un héritage lointain du modèle scam 419. Pourtant, il ne faut pas s'y tromper, les nouveaux cyberescrocs ont mis en place des techniques très élaborées d'hameçonnage (*phishing*), basées sur une connaissance approfondie de la compagnie visée, ainsi que sur la production de documents électroniques contrefaisant très habilement leurs modèles légitimes. Quand la fraude est personnalisée et parfois même accompagnée de procédés technologiques (installation de chevaux de Troie), on parle alors de *spear-phishing*[9].

> « Des mails fictifs sont envoyés aux utilisateurs ; ils peuvent comporter des liens permettant d'installer des logiciels malveillants qui sont des outils de prise en main à distance, mais aussi des *key loggers* pour enregistrer les frappes des claviers. Ils ciblent des gestionnaires ou toutes autres personnes hautement habilitées et ayant la possibilité de faire des opérations sur des comptes. »
>
> RSSI d'une banque au Mali

Les banques sont les cibles privilégiées des cybercriminels grâce à des programmes malveillants conçus spécialement en fonction du système financier. Un des plus ancien est Qbot qui est un cheval de Troie spécialisé dans le vol des données bancaires, notamment les identifiants, mots de passe et autres codes confidentiels (claviers virtuels ou code sms) permettant d'accéder aux comptes bancaires en ligne. Le but recherché par les pirates qui utilisent Qbot, est d'effectuer des virements bancaires frauduleux à l'aide des données dérobées. Normalement bloqué par tous les systèmes antivirus, Qbot est un programme polymorphe qui renaît chaque année sous des formes diverses, car son code source est accessible aux cybercriminels, ce qui lui permet d'être facilement copié et modifié.

Toutefois, ce type de logiciel nécessite une certaine expertise. Aujourd'hui, le principal danger provient des plateformes de cybercriminalité sur demande. Une quantité de programmes malveillants et de données personnelles (documents d'identité complets, numéros de comptes, mots de passe, etc.) se trouvent en vente libre sur le web invisible (*darkweb*). Des outils de rançongiciels ou de dénis de service (DDoS) entièrement préprogrammés sont proposés avec le mode d'emploi, ce qui permet à des malfaiteurs ignorants en informatique de monter des cyberattaques aussi dévastatrices que celles de hackers professionnels. On parle alors de « *crime as a service* » et cela a permis au crime organisé de se lancer dans les cyberattaques de façon à la fois professionnelle et massive[10].

9 Antoine Vandevoorde, "Afrique numérique : un état des lieux du cyberespace africain" (1/2), Les yeux du monde, 20 mars 2019.
10 État de la menace liée au numérique en 2018, Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), ministère de l'Intérieur, Rapport No 2, mai 2018, 112 pages. Cf. p. 46.

1.3.3 - Ampleur de la menace

À l'échelle du continent africain, le coût de la cybercriminalité est estimé à 3,5 milliards d'euros[11]. À titre de comparaison, le coût de la cybercriminalité mondiale s'élève à environ 528 milliards d'euros[12].

Cela ne signifie pas que la cybercriminalité soit moins intense en Afrique que dans le reste du monde. Au contraire, cela signifie que les cyberattaques ne sont en général ni décelées, ni signalées. Il en résulte un terrain extrêmement propice à la propagation de la cybercriminalité. On sait que partout dans le monde, la principale vulnérabilité des entreprises victimes de cyberattaques est l'absence de mise à jour des programmes informatiques. Tous les logiciels ont besoin de mises à jour pour corriger des bugs d'origine, pour intégrer de nouvelles fonctionnalités et parce que l'environnement informatique change. Une entreprise qui néglige des mises à jour régulières est à risque.

Or, l'association mondiale du logiciel BSA estime qu'en Afrique environ 80% des logiciels sont piratés ou contrefaits (installation sans licence)[13]. Cela signifie que ces logiciels ne peuvent jamais être mis à jour et constituent autant de portes ouvertes pour les cybercriminels. Faut-il s'étonner si, dans ces conditions, les experts en cybersécurité estiment que 80% des ordinateurs sur le continent africain sont infectés par des virus et d'autres logiciels malveillants[14]? De façon significative, le taux des logiciels piratés et celui des ordinateurs infectés est le même.

Des organisations de cyberdélinquants téléchargent alors des logiciels malveillants sur les ordinateurs équipés de logiciels piratés qui servent ensuite à lancer des attaques. Ces groupes criminels créent ainsi des « botnets » ou réseaux de programmes informatiques parasites, pour profiter de la puissance d'ordinateurs tiers. De la sorte, ils peuvent capitaliser sur des millions d'appareils connectés et lancer en tout anonymat des offensives de grande envergure, en particulier des attaques par déni de service (DDoS). C'est ainsi qu'on a pu dire de façon imagée que « faire entrer un logiciel piraté chez soi ou dans une entreprise revient à y inviter un délinquant.[15]»

FIGURE 5 - BILAN RÉCAPITULATIF DE LA CYBERMENACE

3,5 G$	1,33 G$	80% des logiciels	80% des PC
Représente le coût annuel des cyberattaques pour les entreprises africaines	Constitue le marché annuel de la cybersécurité en Afrique (2017)	Africains sont piratés ou contrefaits (installés sans licence)	Africains sont infectés par des virus et autres logiciels malveillants
Africa Cyber Security Report: Demystifying Africa's Cyber Security Poverty Line, Serianu, 2017	Africa Cyber Security Market by Solution, by Service, by Verticals, by Country - Global forecast to 2020", MarketsandMarkets.	Global Software Survey 2018, Business Software Alliance (BSA), 2018.	Relever les défis juridiques de la Cybersécurité en Afrique, Union africaine, Ouagadougou, 9-11 octobre 2018

11 "Africa Cyber Security Report: Demystifying Africa's Cyber Security Poverty Line", Serianu, 2017, 86 pages. Cf. p. 58.
12 "Economic Impact of Cybercrime—No Slowing Down", McAfee, février 2018, 28 pages. Cf. p. 4.
13"Global Software Survey 2018", Business Software Alliance (BSA), 2018, 20 pages. Cf. p. 11 (chiffre arrondi).
14 "Relever les défis juridiques de la cybersécurité en Afrique", Union africaine, Ouagadougou, 9-11 octobre 2018. "Relever les défis de la cybersécurité en Afrique", Nations Unies, 2014.
15 "Le piratage de logiciels atteint des sommets en Afrique : voici de bonnes raisons d'utiliser des produits authentiques", Ivoire-Presse, 28 avril 2016.

01 TENDANCES ACTUELLES

1.3.4 - État de la législation en cybercriminalité en Afrique

La cybercriminalité africaine bénéficie aussi de l'inadaptation du cadre législatif et réglementaire africain. Le questionnaire qu'a adressé l'Union africaine à ses membres, montre que la plupart des pays n'ont pas de loi sur la cybersécurité ou la protection des données personnelles, ni même de projets de loi (voir figure 6).

Or, une législation nationale est indispensable, mais nullement suffisante. D'une part, de plus en plus d'entreprises stockent leurs données dans le « Cloud ». Il est impossible de garantir la sécurité de ces données avec une législation purement nationale. D'autre part, la cybercriminalité est un phénomène international. Si on veut que les forces de l'ordre soient sur un pied d'égalité avec les organisations criminelles, il faut que la lutte contre la cybercriminalité soit aussi continentale. Dans cette optique, l'Union africaine a adopté en juin 2014 la Convention de Malabo.

FIGURE 6 - L'ÉTAT DE LA LÉGISLATION EN CYBERCRIMINALITÉ DE L'AFRIQUE SUBSAHARIENNE

Source : Union africaine, Relever les défis juridiques de la cybersécurité en Afrique, 2018

Celle-ci prévoit que « chaque État partie s'engage à adopter des mesures législatives et/ou réglementaires pour identifier les secteurs considérés comme sensibles pour sa sécurité nationale et le bien-être de l'économie ». Le texte s'attache à la régulation des transactions électroniques et à la protection des données personnelles. Malheureusement, quatre pays seulement sur les 55 que compte l'Union africaine ont ratifié cette convention (Sénégal, Guinée, Maurice et le Ghana), neuf autres l'ont signée mais pas ratifiée (Bénin, Tchad, Comores, Congo, Guinée-Bissau, Mauritanie, Sierra Leone, São Tomé-et-Príncipe et Zambie)[16].

Au niveau sous régional, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a émis une Directive relative à la lutte contre la cybercriminalité (août 2011) qui contient des dispositions sanctionnant les actes relevant de la cybercriminalité en Afrique de l'Ouest. Elle invite les États à transférer ce cadre juridique dans les législations nationales.

Il y a enfin la réglementation internationale qui présente l'avantage de prendre en compte le caractère global de la cybercriminalité. C'est ainsi que des pays africains se tournent vers la Convention sur la cybercriminalité de Budapest entrée en vigueur en juillet 2004. Bien qu'adoptée sous l'égide du Conseil de l'Europe, la Convention de Budapest est ouverte à tous les États. Au total, 63 pays ont ratifié la Convention de Budapest, dont cinq pays africains : Maurice, Sénégal, Cap Vert, Ghana et Maroc.

Il faut noter que les banques ont leurs propres organismes de réglementation. Toutes les banques sont assujetties aux accords de Bâle 2 et Bâle 3 qui définissent des règles prudentielles rigoureuses. Ces règles sont transposées dans la zone de l'Union monétaire ouest africaine (UMOA) afin de garantir l'existence d'un système bancaire solide, de niveau international, mais en tenant compte des spécificités locales. En termes de cybersécurité, le grand avantage des recommandations Bâle 2/Bâle 3 est de définir un ratio minimal de fonds propres par rapport à l'ensemble des crédits accordés. Ce ratio évolue en fonction du risque que présente l'institution financière considérée[17].

Cela signifie que les banques ont un intérêt structurel à réduire leur exposition au risque pour avoir à détenir le moins de fonds propres possibles. Ainsi, tout ce que la banque investit en cybersécurité contribue à réduire l'exposition au risque et donc à réduire les fonds propres réglementaires exigés par le Comité de Bâle. Signalons enfin que depuis 2018, le Comité de Bâle a établi un Groupe de travail sur la résilience opérationnelle (ORG) dans l'intention de contribuer, entre autres, à l'effort international sur la gestion du cyber-risque. Il faut donc prévoir un regain d'activité réglementaire dans ce domaine[18].

16 "African Forum on Cybercrime", African Union Commission, 16-18 octobre 2018.
17 Élysée Lath, "Octroi de crédit aux Pme : Pourquoi les banques sont si exigeantes", Linfodrome, 26 mars 2019.
18 Un rapport intitulé "Cyberrésilience: un éventail des pratiques" a déjà été publié en décembre 2018 à l'occasion duquel le Comité de Bâle partage des observations et quelques grandes conclusions relatives aux pratiques en matière de cyber-résilience dans plusieurs banques et organes de supervision. Cité dans "Lettre d'actualité réglementaire banque", PwC, janvier 2019.

1.3.5 - Niveau de cybersécurité

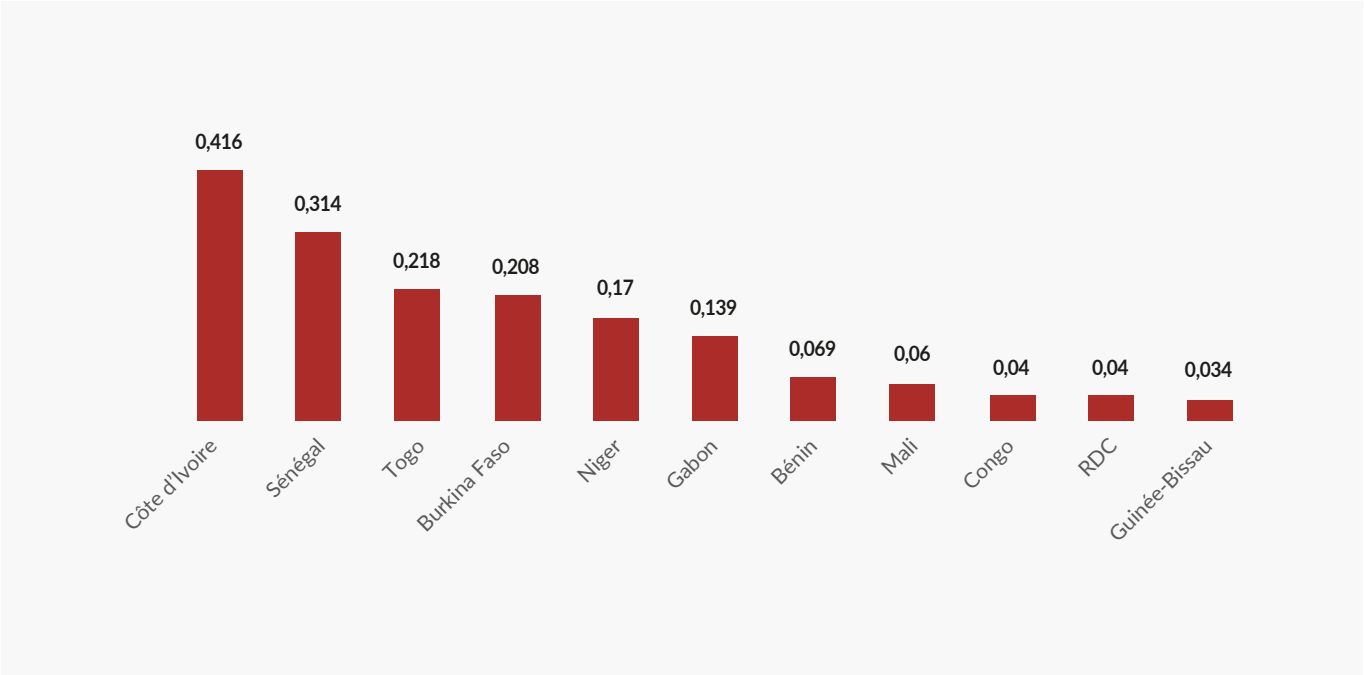
Au total, la cybersécurité est la résultante d'une combinaison de plusieurs facteurs. L'Union Internationale des Télécommunications (UIT) a regroupé ces facteurs en cinq « piliers » qui sont :

- Les mesures juridiques (législation, formation…);
- Les mesures techniques (normes, CERT…);
- Les mesures organisationnelles (stratégie nationale, indicateurs de cybersécurité…);
- Le renforcement de capacité (campagnes de sensibilisation, présence d'une industrie domestique…);
- La coopération (accords bilatéraux et multilatéraux, partenariats public-privé…).

La Côte d'Ivoire qui est le pays le plus performant du groupe considéré dans cette étude arrive au 8e rang africain et au 73e rang mondial, c'est dire le chemin qui reste à faire (voir les détails de l'enquête de l'UIT à l'annexe 1).

Notons que les trois premiers pays africains subsahariens sont Maurice (sixième à l'échelle mondiale), le Rwanda (36e) et le Kenya (45e). Dans les trois cas, l'État a servi de locomotive au développement de la cybersécurité : lancement d'un CERT adossé à un projet de dépistage des *botnets* à Maurice ; stratégie de partenariats public-privé au Rwanda ; création d'un CIRT au Kenya avec une forte coopération internationale (UIT, États-Unis et Japon). Ces pays peuvent servir de modèles pour le reste de l'Afrique.

FIGURE 7 - NIVEAU D'ENGAGEMENT MONDIAL DES ÉTATS MEMBRES DE L'UIT EN CYBERSECURITE



Source : UIT, Global Cybersecurity Index 2017,. Cf. pp. 51-52.

01 TENDANCES ACTUELLES

Certains pays subsahariens ont déjà élaboré de stratégies nationales sur la cybersécurité (Cameroun, Sénégal, Burkina Faso, Côte d'Ivoire…). Au chapitre des mesures techniques, la mesure la plus notable est l'installation graduelle d'une infrastructure de cybersécurité en Afrique subsaharienne. Il y a déjà cinq CERT en activité (Côte d'Ivoire, Maurice, Nigeria, Ouganda et Tanzanie) et 12 CIRT (Afrique du Sud, Burkina Faso, Cameroun, Éthiopie, Ghana, Kenya, Nigeria, Ouganda, Rwanda, Sénégal, Tanzanie et Zambie)[19]. Ces chiffres varient selon les sources, car les appellations CERT et CIRT sont parfois confondues[20]. Il existe en outre plusieurs projets en cours de développement (Bénin, Cap-Vert…).

Face à l'inertie des pouvoirs publics et de la coopération régionale, les responsables de cybersécurité tentent de s'organiser. C'est ainsi qu'en février 2017, à l'occasion de l'IT Forum Sénégal, une dizaine de DSI représentant sept pays (Sénégal, Côte d'Ivoire, Mali, Togo, Bénin, Maroc et Tunisie) ont élaboré un plan d'action visant à créer un réseau des Clubs DSI Africains. Une deuxième rencontre a eu lieu au Maroc en mai 2017 en présence des représentants de l'AUSIM et des présidents des Club DSI du Sénégal et de la Tunisie. En octobre 2017, à l'occasion de la 4ème édition du Forum International des DSI organisé en Tunisie, une trentaine de DSI représentant 15 pays africains ont créé le CIO Africa Network[21].

De même, de grands évènements dédiés à la question de la cybersécurité continentale voient le jour, tels que l'*Africa Cybersecurity Conference* d'Abidjan, ou encore le *Sommet Africain de l'Internet* de Dakar. C'est lors de ce dernier que la commission de l'organisation, en partenariat avec l'Internet Society – ISOC – dévoile en 2018 les *Personal Data Protection Guidelines for Africa*[22].

Enfin, il faut accorder une place spéciale à l'École de cybersécurité qui a été ouverte en novembre 2018 à Dakar. En effet, l'Afrique manque cruellement d'expertise : l'étude Serianu recense 10 000 professionnels certifiés cybersécurité sur l'ensemble du continent, alors qu'il en faudrait quatre fois plus[23]. Voilà pourquoi, cette première institution africaine consacrée à l'enseignement de la cybersécurité marque une date importante. Provisoirement installé à Dakar, au sein des locaux de l'École nationale d'administration (ENA), ce centre de formation disposera bientôt de son propre bâtiment dans la future ville numérique de Diamniadio, à une trentaine de kilomètres de la capitale.

La nouvelle institution a pour ambition de rayonner dans toute l'Afrique de l'Ouest en formant des hauts fonctionnaires, des magistrats, des policiers et des RSSI du secteur privé. L'accent y est mis sur la cybersécurité, le renseignement numérique et la cybergouvernance. L'École de cybersécurité fait partie du réseau des Écoles nationales à vocation régionale, qui sont des institutions de formation sécuritaire créées en coopération par la France et plusieurs pays africains.

La création de l'École de cybersécurité couronne la politique dynamique du Sénégal en matière de cybersécurité. C'est ainsi que ce pays a créé en 2013 une première unité spéciale de lutte contre la cybercriminalité – ses effectifs ont triplé en 2017 pour passer à 29 personnes. Celle-ci a déjà plusieurs faits d'armes à son actif. C'est ainsi qu'au cours de la dernière année, elle a réussi à arrêter 200 cybercriminels pour des infractions allant du piratage, à la collecte déloyale de données à caractère personnel[24].

19 Antoine Vandevoorde, "Afrique numérique : un état des lieux du cyberespace africain" (1/2) et "Penser le cyberespace africain, entre ambitions politiques déçues et cyber-résilience" (2/2, Les yeux du monde, 20 et 25 mars 2019. National CIRT, International Telecommunications Union (ITU). - https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx. Voir aussi : FIRST Teams - https://www.first.org/members/teams/?#.
20 Le sigle CERT est une marque de commerce de l'Université Carnegie Mellon. Pour l'utiliser, il faut en demander l'autorisation auprès des autorités de cette institution. On réserve le terme de CERT aux grandes organisations de sécurité informatique qui collaborent au sein d'une grande communauté de renseignement informatique. De son côté, le sigle CIRT est plus générique et peut recouvrir des petites organisations. Son rôle est d'intervenir en cas d'incident de sécurité informatique à titre de responsable de la réception, de la révision et du traitement des rapports d'incident. On parle parfois de CSIRT.
21 Faouzi Moussa, "Interview de Hatem Trigui Président Club DSI Tunisie", Cio Mag, 02 octobre 2018.
22 Antoine Vandevoorde, "Penser le cyberespace africain, entre ambitions politiques déçues et cyber-résilience" (2/2), Les yeux du monde, 25 mars 2019
23 "Africa Cybersecurity Report", Serianu 2017, 86 pages. Cf. p. 11. Olga Egrelle, "Sénégal : une école nationale de cybersécurité à vocation régionale", Portail de l'IE, 19 novembre 2018.
24 Matteo Maillard, "Au Sénégal, un centre pour former les Africains à la cybersécurité", Le Monde, 22 novembre 2018. Fatou Diop, « Cybercrimninalité : plus de 200 personnes arrêtées depuis septembre 2017 », Agence de presse sénégalaise (APS), 23 novembre 2018.

02

PROFIL DU SECTEUR BANCAIRE

L'enquête de DATAPROTECT a eu lieu entre février et avril 2019 auprès de 148 banques provenant de 11 pays d'Afrique de l'Ouest et centrale. Au total, 21 banques ont participé à l'enquête directement ou indirectement, ce qui fait un taux de réponse de 14%. La plupart des répondants sont des banques commerciales ou des banques de détail. La majorité sont de tailles moyennes ou petites et à capitaux africains. Pas de géant, mais une des institutions financières contactées a déjà essaimé en Afrique et une autre en France.

02 PROFIL DU SECTEUR BANCAIRE

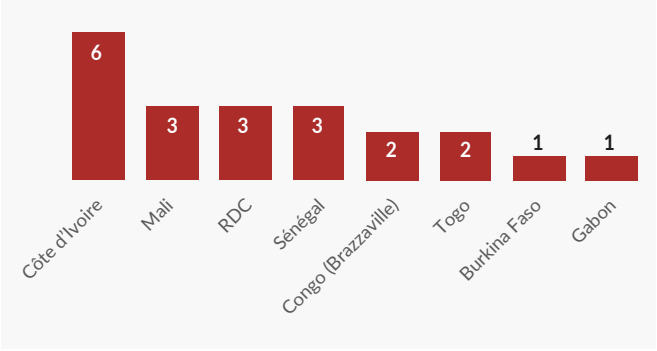
2.1 – Mise en contexte de l'échantillon

L'enquête a eu lieu entre février et août 2019 auprès d'institutions financières établies en Afrique subsaharienne. La population de base est composée par 148 banques provenant des huit pays membres de l'Union économique et monétaire ouest-africaine (UEMOA) auxquels nous avons ajouté trois pays d'Afrique centrale : Gabon, Congo et République démocratique du Congo (RDC). Au total, 21 banques ont participé à l'enquête directement ou indirectement, ce qui fait un taux de réponse de 14%.

2.2 - Nature des banques ayant participé à l'enquête

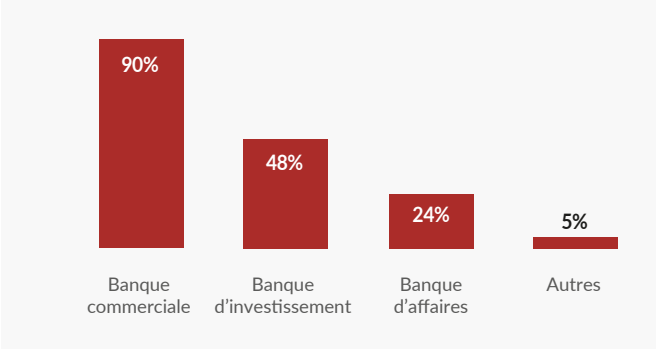
La plupart des répondants sont des banques commerciales ou des banques de détail (90% des répondants), mais la plupart d'entre elles exercent aussi d'autres activités : banques d'investissement et banques d'affaires. Une banque a également indiqué une vocation sociale – la microfinance. En cela, l'échantillon est représentatif du caractère polyvalent des institutions financières d'Afrique subsaharienne.

FIGURE 8 - EMPLACEMENTS DES BANQUES INTERROGÉES



Source : Étude Sciencetech/DataProtect, février-août 2019

FIGURE 9 - NATURE DES BANQUES

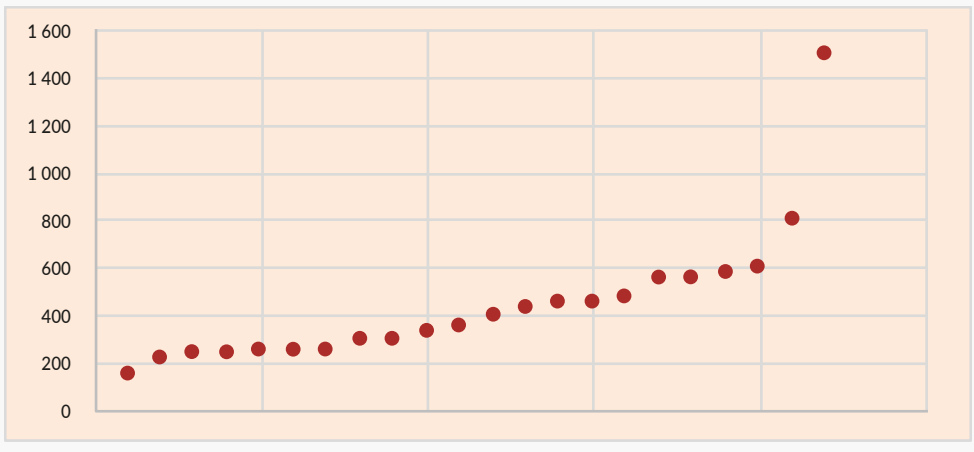


Source : Étude Sciencetech/DataProtect, février-août 2019.

2.3 - Taille des banques ayant participé à l'enquête

En termes de tailles, les institutions financières sont moyennes ou petites et à capitaux africains. La plus grande banque ayant participé à l'enquête compte 1 500 employés et la plus petite 150. La moitié de l'échantillon a entre 250 et 500 employés. Une d'entre elle a déjà essaimé en Afrique (Burkina Faso, Côte d'Ivoire, Guinée Bissau) et une autre en France – pour suivre la diaspora africaine en Europe.

FIGURE 10 - TAILLE DES RÉPONDANTS EN TERMES D'EMPLOIS



Source : Étude Sciencetech/DataProtect, février-août 2019.

03

LA GOUVERNANCE EN CYBERSECURITE DES BANQUES AFRICAINES

La grande majorité des institutions financières ont confié la responsabilité de leur cybersécurité à un responsable de la sécurité des systèmes d'information (RSSI), mais celui-ci relève du directeur des systèmes d'information (DSI). La cybersécurité n'a pas acquis le rang de discipline à part entière, elle est toujours considérée comme une composante des TI. Cela se traduit par des effectifs sous-dimensionnée : entre un employé à plein temps et trois.

Cette situation est expliquée en partie par les difficultés de recrutement de ressource qualifiée : outre le phénomène central qui est le manque de talents, les hauts salaires pratiqués et l'inadaptation de la formation sont les deux raisons les plus souvent mentionnées. Cinquante-cinq pour cent des banques ont tendance à contourner ce problème en recourant à la sous-traitance ou à l'infogérance.

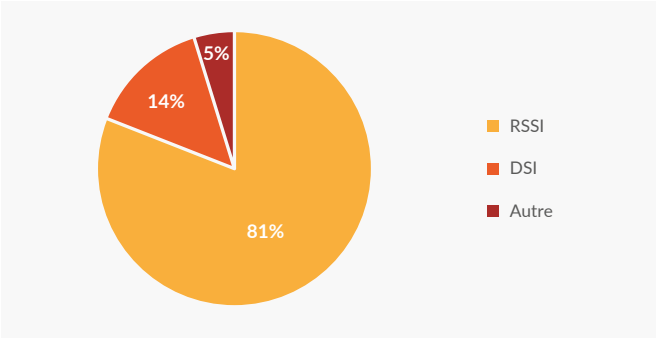
Plus de 70% des entreprises organisent des campagnes de sensibilisation et de formation. Cette forte proportion laisse cependant une minorité sans programme de sensibilisation, ni programme de formation, ce qui est inquiétant. Il s'agit d'activités peu coûteuses et relativement faciles à implanter, sans lesquelles toute stratégie de cybersécurité est vouée à l'échec. Enfin, la cyberassurance est encore absente, non qu'elle soit considérée comme inutile, mais parce qu'elle n'est pas disponible.

03 LA GOUVERNANCE EN CYBERSECURITE DES BANQUES AFRICAINES

3.1 - Gestion de la cybersécurité

Sans surprise, la grande majorité des institutions financières ont confié la responsabilité de leur cybersécurité à un responsable de la sécurité des systèmes d'information (RSSI). La seule institution bancaire à avoir répondu « autre » a confié la cybersécurité au responsable Réseaux et Télécoms.

FIGURE 11 - QUI EST RESPONSABLE DE LA CYBERSÉCURITÉ DANS L'INSTITUTION FINANCIÈRE ?



Source : Étude Sciencetech/DataProtect, février-août 2019.

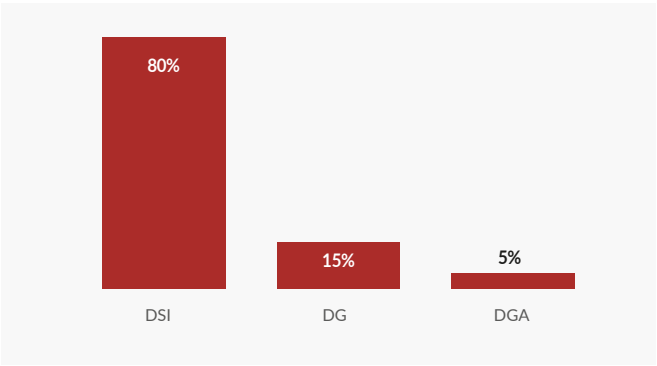
Analyse

Le rôle prééminent des RSSI un premier signe de maturité dans la mesure où cela signifie une reconnaissance de la spécialisation de la fonction. La cybersécurité ne peut pas être traitée comme un simple segment des technologies de l'information (TI). Il y a des champs d'activités non-TI dans la cybersécurité : formation et sensibilisation, gestion des accès physiques et virtuels, rapports avec les sous-traitants, etc. Nommer un RSSI est indispensable, mais ce n'est pas suffisant.

3.2 - Situation hiérarchique du RSSI dans l'institution financière

La plupart des RSSI relèvent du directeur des systèmes d'information (DSI). Seule la minorité relève du directeur général (DG) ou du directeur général adjoint (DGA).

FIGURE 12 - QUEL EST LE SUPÉRIEUR HIÉRARCHIQUE IMMÉDIAT DU RESPONSABLE DE LA SÉCURITÉ ?



Source : Étude Sciencetech/DataProtect, février-août 2019.

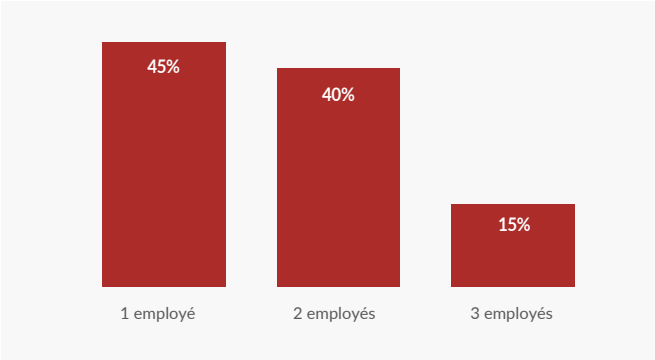
Analyse

L'intégration du RSSI dans le département des TI marque les limites de la maturité des banques africaines. On accorde bien un statut spécial à la cybersécurité, mais dans le cadre des TI. Seule la minorité d'institutions qui ont placé le RSSI sous l'autorité directe du DG, sur un pied d'égalité avec le DSI, a atteint un degré adéquat de maturité en cybersécurité.

3.3 - Taille des équipes de cybersécurité

La taille des équipes de cybersécurité est modeste : elle varie d'un employé à plein temps (le RSSI) à trois. En outre, deux institutions financières ont signalé recourir à des employés à temps partagé.

FIGURE 13 - COMBIEN D'EMPLOYÉS SONT AFFECTÉS À LA CYBERSÉCURITÉ DANS L'INSTITUTION FINANCIÈRE ?



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

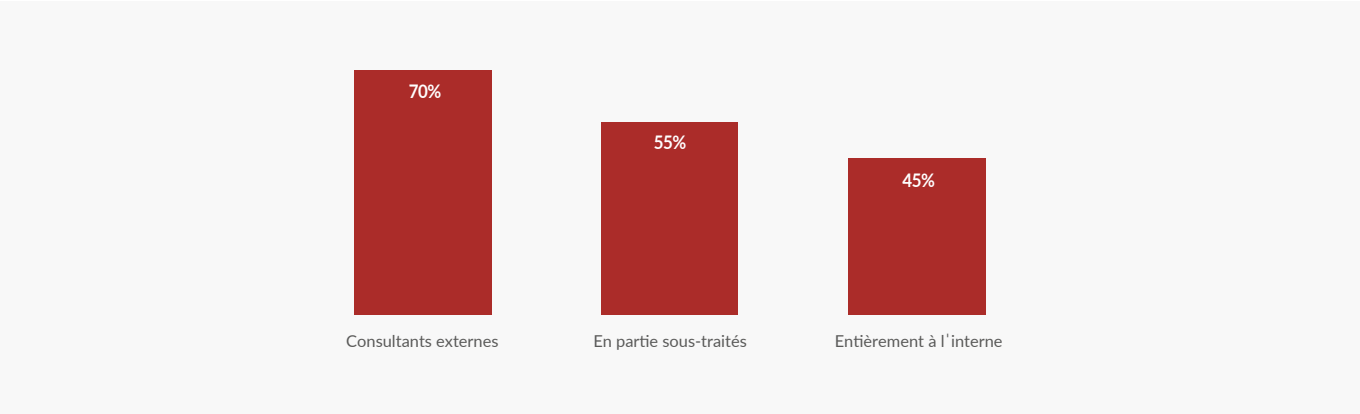
Des effectifs réduits ne signifient pas obligatoirement une faiblesse des moyens. Partout dans le monde, les institutions financières (tout comme les grandes entreprises) conservent à l'interne la décision stratégique et certaines fonctions spécifiques (par exemple, la gestion des autorisations et le contrôle d'accès logique aux ressources), mais confient l'exécution du plan stratégique à des ressources externes.

3.4 - Sous-traiter ou non la cybersécurité

Une majorité de 55% des institutions financières recourent à la sous-traitance (infogérance) pour leurs activités de cybersécurité, tandis que 45% les gèrent entièrement à l'interne. En fait, près de la moitié de ceux qui disent gérer entièrement la cybersécurité à l'interne, font quand même appel à des consultants. Seuls 20% des institutions concernées font tout à l'interne.

Rien d'étonnant à ce que l'utilisation de consultants externes soit très répandue. Il ne s'agit pas d'un recours ponctuel, mais plutôt d'une façon de gérer la cybersécurité : les banques qui font appel à des consultants utilisent en moyenne 167 employés équivalents temps plein (ETP) par an.

FIGURE 14 - FAUT-IL GÉRER LA CYBERSÉCURITÉ À L'INTERNE OU À L'EXTERNE?
(le total n'est pas égal à 100, car certaines institutions ont recours à plusieurs types de gestion de la cybersécurité)



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

La raison principale de l'infogérance est la volonté de l'entreprise de se concentrer sur son activité centrale et de ne pas éparpiller ses efforts dans des domaines où elle a peu d'expertise. Une raison additionnelle vient se surimposer depuis quelques années : la difficulté de recruter du personnel qualifié. Un spécialiste en cybersécurité répugne souvent à travailler dans une entreprise où il va être isolé professionnellement et sans possibilité de promotion dans son domaine. Comment une PME industrielle pourrait-elle offrir un emploi comparable à ceux disponibles dans une grande firme spécialisée ? En sous-traitant tout ou partie de leur cybersécurité, les banques se débarrassent de cette difficulté.

Typiquement, les institutions financières délèguent à des sous-traitants les tâches hautement techniques (SOC, audits de cybersécurité, tests de pénétration…) et conservent les tâches reliées de près aux ressources humaines (gestion de l'accès à l'information, attribution des droits d'accès et de privilèges spéciaux, retrait des codes lors du départ d'un employé…). Rares sont celles qui confient la totalité des tâches de cybersécurité à des prestataires externes. Une seule banque a déclaré confier 100% de sa cybersécurité en infogérance.

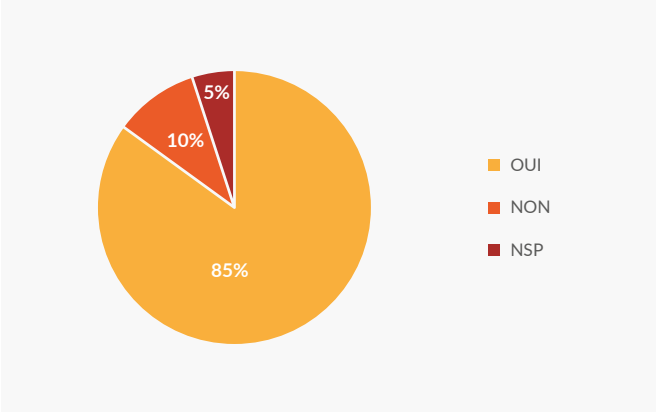
Par contre la petite minorité de 20% de banques qui disent gérer toute leur cybersécurité à l'interne sont probablement à risque. Il s'agit des plus petites institutions ayant participé à l'enquête et elles ont toutes un seul employé de cybersécurité.

03 LA GOUVERNANCE EN CYBERSECURITE DES BANQUES AFRICAINES

3.5 - Difficultés de recrutement de ressource qualifiée

La très grande majorité des intervenants évoque la question de la difficulté de recruter des talents en cybersécurité. Parmi la minorité qui déclare n'avoir pas de difficulté à recruter des spécialistes en cybersécurité, on retrouve des profils très divers : une banque qui sous-traite une partie importante de sa cybersécurité, une autre qui au contraire fait tout à l'interne, mais semble valoriser la fonction de RSSI qui est placé sous l'autorité directe du DG.

FIGURE 15 - DIFFICULTÉS À RECRUTER DES EMPLOYÉS SPÉCIALISÉS EN CYBERSÉCURITÉ



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

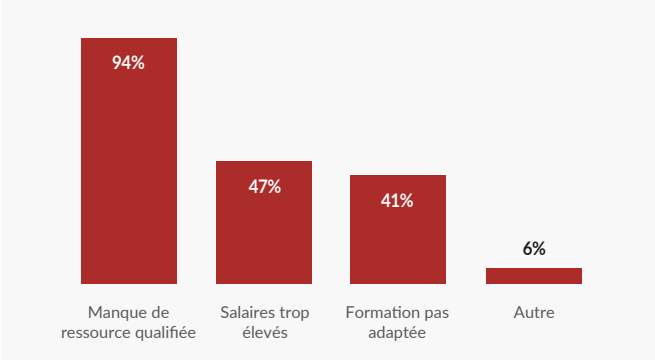
Cette difficulté est bien sûr créée par l'immense appel d'air de la cybercriminalité en hausse constante. Le développement rapide du secteur financier a sa contrepartie qui est l'explosion concomitante de la cyberfraude. Le résultat est une demande soudaine pour des talents en cybersécurité que le marché peine à fournir.

Une piste de solution passe par l'établissement ou le renforcement de liens avec les universités. Les institutions financières ont tout à gagner à travailler avec des universités dont la mission de faire de la recherche dans les domaines de pointe : intelligence cyber-statistique, techniques de traçage, chaînes de blocs, etc. Il y a là un bouillon de culture qui donne naissance aux idées nouvelles et parfois même à des « spin-offs ». Donner un contrat de recherche à une université permet bien entendu de résoudre des problèmes immédiats, mais c'est aussi une manière d'identifier les talents prometteurs qui pourront devenir les cadres de demain.

3.6 - Raisons invoquées pour les difficultés de recrutement

Sans surprise, la quasi-totalité des institutions financières invoquent le manque de ressource qualifiée. Les salaires pratiqués dans le secteur de la cybersécurité et l'inadaptation de la formation sont les deux autres raisons le plus souvent mentionnées.

FIGURE 16 - PRINCIPALES RAISONS INVOQUÉES
(le total n'est pas égal à 100, car les institutions ont invoqué plusieurs raisons)



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Le phénomène de la cybercriminalité a longtemps été négligé ou sous-estimé. Mais les amateurs du scam 419 ont depuis de nombreuses années cédé la place au crime organisé et au terrorisme étatique. Face à cette explosion de la cybercriminalité, les universités et les collèges ont été longs à réagir et, aujourd'hui encore, forment peu de diplômés. Comme on l'a vu ci-dessus, la première École de cybercriminalité d'Afrique subsaharienne vient seulement de recevoir ses premiers étudiants à Dakar en janvier 2019.

La conséquence de cette lenteur à réagir est une pénurie d'experts en cybersécurité. Il y a pis : les minuscules cohortes qui sortent des universités sont souvent enclines à parachever leur formation en Europe ou en Amérique du Nord, ce qui réduit encore plus leurs rangs.

Enfin, les programmes universitaires ont du mal à suivre les cadences tumultueuses de l'univers de la cybercriminalité. Les programmes sont souvent dépassés avant même d'avoir été mis en œuvre. Un des moyens de lutter contre cette inadéquation entre les contenus enseignés et les besoins du marché, serait de multiplier les stages en entreprise.

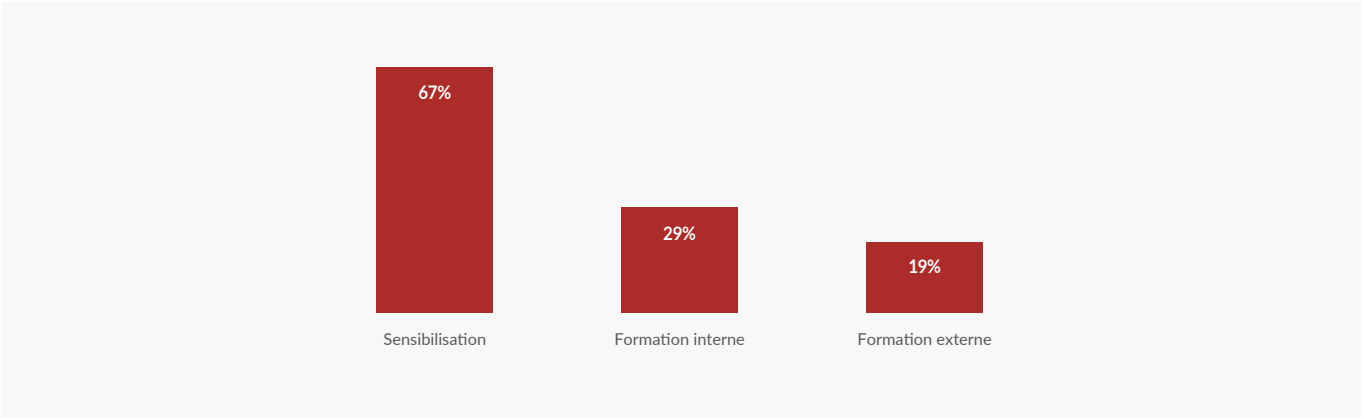
3.7 - Formation et sensibilisation à la cybersécurité

Plus de 70% des entreprises organisent des campagnes de formation et de sensibilisation[25]. Il y a une différence significative entre formation et sensibilisation. La formation consiste à enseigner de façon formelle des notions ou des procédés, tandis que la sensibilisation relève plus de la communication et vise à créer une prise de conscience chez l'employé.

La sensibilisation vient en tête avec 67% des banques qui ont lancé un ou plusieurs programmes de sensibilisation de leurs employés non TI. La sensibilisation peut aller de la simple séance d'information à l'organisation d'une campagne complète mobilisant l'intranet, des courriels personnalisés, des bulletins en ligne, les écrans de veille des ordinateurs, les affiches dans les lieux de travail et une plateforme vidéo interactive. Il est à noter que la moitié des intervenants qui ont mis en place une campagne de sensibilisation, ont déclaré recourir à une plateforme vidéo interactive qui constitue le haut de gamme des activités de sensibilisation.

Quand il s'agit de formation, les programmes internes (29%) sont plus populaires que les programmes externes (conférence, cours, etc.). Ceci est explicable par la faible disponibilité de ces programmes de formation. Mais il faut aussi compter avec la spécificité du secteur bancaire. Qui connaît mieux les risques qui lui sont propres qu'une institution financière ?

FIGURE 17 - FORMATION ET SENSIBILISATION



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Il est injustifiable qu'un petit groupe d'institutions bancaires n'ait ni programme de sensibilisation, ni programme de formation car ce n'est pas une activité qui exige des moyens onéreux, ni qui mobilise des ressources humaines nombreuses. S'il est un champ de la cybersécurité où une action vigoureuse est indispensable, c'est bien celui de la sensibilisation/formation en cybersécurité dans le secteur bancaire. L'objectif doit être d'atteindre au plus tôt l'objectif de 100% de pénétration de la sensibilisation/formation sur une base continue.

C'est d'autant plus indispensable que la majorité des cybercrimes provient de l'intérieur, que ce soit un employé qui laisse traîner un mot de passe, un employé leurré par hameçonnage ou encore un employé malhonnête. Toute stratégie de cybersécurité commence par la formation et la sensibilisation des employés.

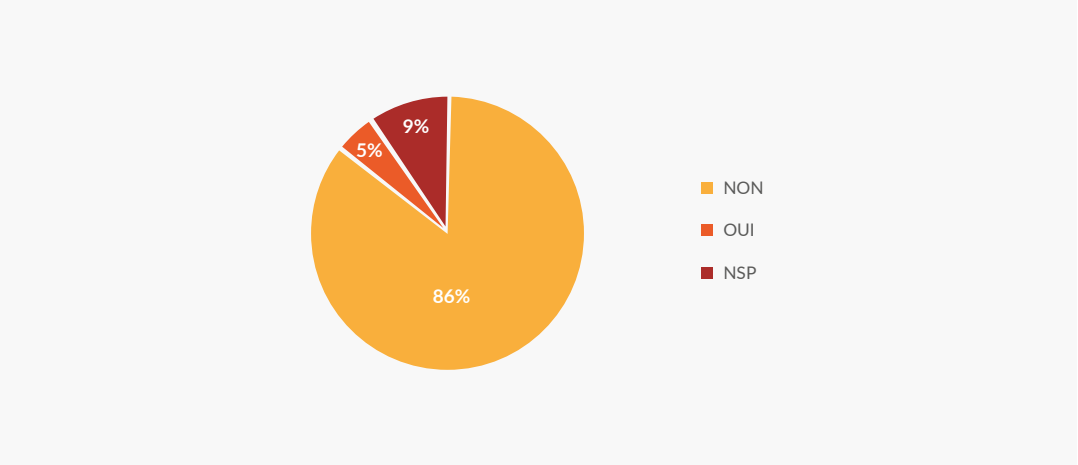
25 Même si toutes les institutions ayant des programmes de formation ont aussi un programme de sensibilisation, certaines institutions ont un programme de formation et pas de programme de sensibilisation..

03 LA GOUVERNANCE EN CYBERSECURITE DES BANQUES AFRICAINES

3.8 - La cyber-assurance tarde à prendre son envol

Quand on aborde le thème de l'assurance en cybersécurité, le phénomène marquant est la grande proportion de répondants qui n'ont pas d'assurance. À peine 5% des institutions financières sont assurées. Parmi les banques qui n'ont pas d'assurance, trois ont expliqué qu'une telle protection n'était pas disponible dans leur région.

FIGURE 18 - ENTREPRISES QUI ONT UNE ASSURANCE POUR COUVRIR LE RISQUE CYBER



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Cette situation n'est pas spécifique à l'Afrique. Dans le monde entier, les entreprises ont mis d'autant plus de temps à assurer leurs actifs informationnels que l'offre était incertaine et souvent peu adaptée aux besoins du marché ou trop chère. La cyberassurance est née à la fin des années 1990 avec la peur du « bug » de l'an 2000 et elle a mis du temps à s'adapter à l'environnement Internet. Il faut reconnaître que la nature protéiforme des cybermenaces rend difficile la définition d'une offre standardisée. Hormis en Grande-Bretagne et aux États-Unis, l'offre est encore changeante et immature.

Il convient d'accorder une grande importance au développement de l'assurance cybersécurité. En effet, il ne s'agit pas seulement d'une protection financière, mais d'un processus complet de gestion du risque. Dans les pays où elle est bien implantée, l'assurance oblige les clients à se doter des mesures d'hygiène de base en matière de cybersécurité comme condition d'admissibilité. Une fois la police d'assurance émise, la compagnie accompagne les clients pour les mettre à jour sur la cybermenace et les aider à y faire face de manière préventive.

04 LE CADRE SECURITAIRE

Près des deux-tiers des institutions financières sont dotées d'un programme écrit de cybersécurité, mais ce résultat diminue quand on vérifie la présence effective de plusieurs des composantes d'un tel programme, à savoir les tests d'intrusion (62%), un plan de relève (52%), une analyse de risque (52%), un audit des systèmes d'information (52%) et l'obligation d'inclure une clause de cybersécurité dans les accords de sous-traitance (14%).

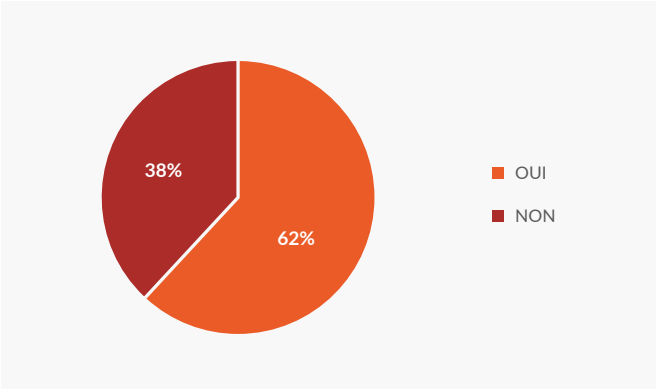
Un peu plus de la moitié des institutions financières déclarent disposer d'un SOC et, dans la presque totalité des cas, il s'agit d'un SOC externe. Cette tendance à l'externalisation du SOC correspond aux meilleures pratiques en vigueur. En effet, un SOC doit fonctionner 24/7 pour être efficace et nécessite du personnel qualifié en conséquence, toutes choses qu'il est difficile de réaliser à l'interne.

04 LE CADRE SECURITAIRE

4.1 - La majorité des banques dispose d'un programme formel de cybersécurité

Près des deux-tiers des institutions financières sont dotées d'un programme formalisé de cybersécurité. Parmi les entreprises qui ont répondu NON, trois expliquent cette carence par le manque de moyens financiers, une par l'instabilité structurelle (fusion de deux banques) et une affirme être en train de mettre au point son programme.

FIGURE 19 - L'INSTITUTION FINANCIÈRE DISPOSE-T-ELLE D'UN PROGRAMME ÉCRIT DE CYBERSÉCURITÉ ?



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

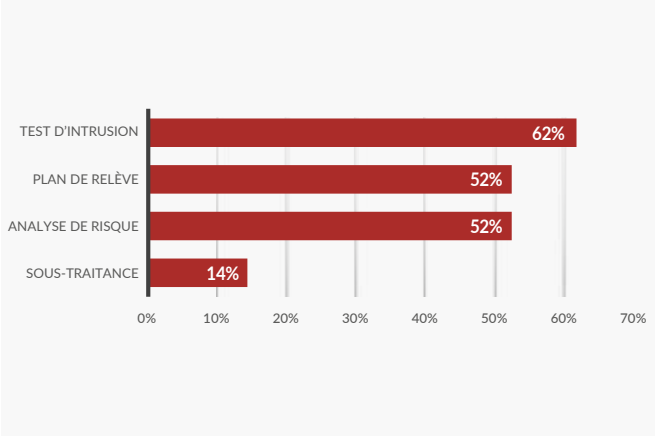
Toute entreprise appelée à gérer des actifs informationnels devrait disposer d'un programme formel de cybersécurité et c'est encore plus impératif dans le cas d'une institution financière. Rappelons que le risque informatique est reconnu comme un risque opérationnel par le Comité de Bâle sur le contrôle bancaire (CBCB) depuis 2003 et, à ce titre, requiert un programme de contrôle très strict. En outre, un encadrement renforcé est exigé quand la banque fait appel à des fintechs ou tout autre type de sous-traitance financière[26].

4.2 - Meilleures pratiques de cybersécurité

Tout programme de cybersécurité est généralement basé sur un audit et prévoit certaines bonnes pratiques comme les tests d'intrusion, une analyse de risque, une politique d'accès aux systèmes, l'obligation d'inclure une clause de cybersécurité dans les accords de sous-traitance, un plan de gestion des incidents et de relève, etc. La liste n'est pas exhaustive. Nous avons effectué un choix au profit de certaines pratiques seulement, en fonction de leur caractère structurant.

La moitié environ des institutions financières effectuent des audits de leurs systèmes d'information. Sans surprise, il s'agit dans tous les cas de banques qui ont un programme écrit de cybersécurité. Ce sont d'ailleurs les mêmes banques qui se sont dotées d'un plan de relève. Manifestement, il s'agit des « bons élèves » de la cybersécurité. Dans ce groupe, trois banques seulement indiquent procéder régulièrement à un audit de cybersécurité, tandis que trois autres sont en passe de faire de même dans le courant de l'année. Cela signifie que les autres banques doivent se fier à des données désuètes ou incomplètes pour protéger leur parc informatique.

FIGURE 20 - DÉPLOIEMENT DE QUELQUES PROCESSUS DE BASE



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Parmi les processus de cybersécurité mis en place dans les institutions financières, le plus populaire est sans conteste le test d'intrusion – une mesure technique – et le moins populaire, l'obligation d'inclure une clause de cybersécurité dans les accords de sous-traitance – une mesure de gestion. Ce contraste est significatif de la gouvernance de la cybersécurité : il renvoie à la nature TI des postes de RSSI dans les institutions financières africaines. La cybersécurité est encore considérée dans une perspective purement informatique et non pas dans une perspective stratégique et opérationnelle élargie.

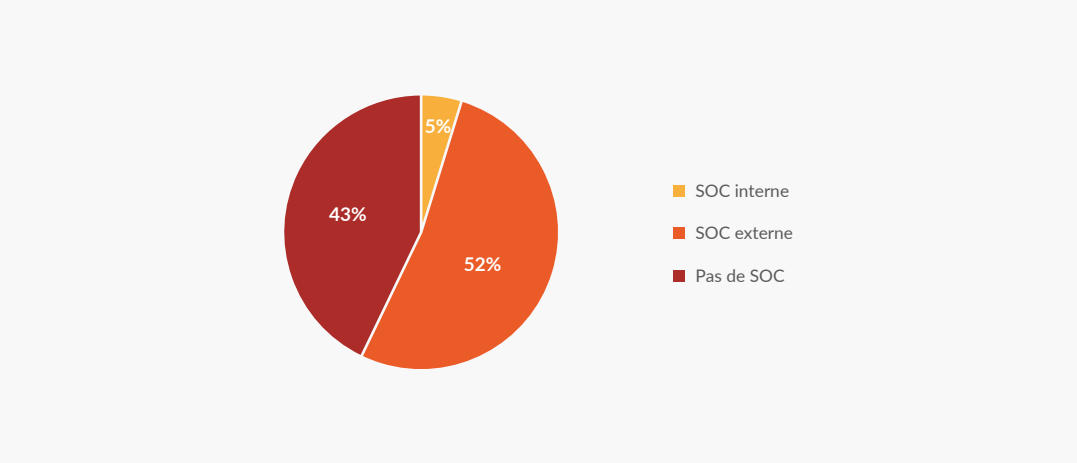
26 Comité de Bâle sur le contrôle bancaire, "Saines pratiques: Implications des évolutions de la technologie financière pour les banques et les autorités de contrôle bancaire", Banque des Règlements Internationaux, février 2018, 52 pages.

4.3 - Accès à une plateforme de surveillance permanente des événements

Que l'on dispose de serveurs locaux ou que l'on recourt à la solution du « cloud », il est indispensable de surveiller les flux de données entrantes et sortantes. Il est important d'identifier les comportements anormaux avant même le déclenchement de l'incident en formalisant le traitement des signaux avant-coureurs depuis leur détection jusqu'à leur traitement et centraliser les processus de façon à avoir une visibilité globale de la situation en temps réel. L'outil capable de satisfaire à ce double objectif est le centre d'opérations et de sécurité ou SOC selon son acronyme anglais (*Security Operations Center*).

Un peu plus de la moitié des institutions financières déclarent disposer d'un SOC et dans la presque totalité des cas, il s'agit d'un SOC externe. La principale raison invoquée par celles qui en sont dépourvues est l'absence de moyens financiers, une institution invoque des circonstances conjoncturelles et une autre le manque d'offre locale; enfin, une banque affirme être en voie de se doter d'un SOC.

FIGURE 21 - SURVEILLANCE DES SYSTÈMES D'INFORMATION



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Déclarer avoir un SOC est une chose. La qualité du SOC déployé en est une autre. Dans le cadre de cette enquête, une seule institution a soutenu avoir un SOC en interne et elle a expliqué qu'elle prévoyait externaliser la gestion de cette plateforme. C'est une décision qui correspond aux meilleures pratiques en vigueur parmi les responsables de sécurité. En effet, un SOC exige une configuration précise et difficile à mettre en place. Pour fonctionner 24/7, un SOC doit employer au minimum cinq spécialistes de haut niveau à temps plein.

Il est encourageant de noter que la quasi-totalité des institutions financières qui utilisent un SOC, a recours à un prestataire externe. Grâce à la mutualisation de l'expérience acquise auprès de différents clients, une organisation spécialisée est à même de suivre l'évolution de l'environnement cybercriminel. Elle peut aussi suivre l'actualité technologique en temps réel et disposer toujours des dernières mises à jour logicielles. Enfin, le regard critique d'un tiers neutre sur les activités informationnelles de l'institution financière est un atout pour les responsables TI de la banque.

05

LES CYBERATTAQUES ET LEURS IMPACTS

Au moins 85% des institutions financières consultées déclare avoir déjà été victime d'une ou plusieurs cyberattaques ayant occasionné des dommages - dans certains cas, il s'agit même d'attaques à répétition. Globalement, ce sont les fraudes sur les cartes bancaires (*carding* et *skimming*) ainsi que l'hameçonnage (*phishing*) qui sont les types de cyberattaques les plus fréquentes, suivies des atteintes au *core banking*, les infections virales et les intrusions dans les systèmes d'information critiques.

La moitié des incidents signalés dans l'enquête de DATAPROTECT ont mis trois mois et plus pour être découverts. Cela laisse toute latitude aux assaillants pour commettre leurs méfaits. La longueur du temps de détection renvoie à la carence d'outils et de ressources nécessaires à l'identification des anomalies. À preuve, seulement 6% des incidents sont découverts par les employés de cybersécurité des institutions financières, la majorité ayant été découverts par des employés des banques ou par des intervenants extérieurs.

Le principal impact des cyberattaques est la perte d'argent, suivi de la suspension des services en ligne et de l'indisponibilité d'un ou plusieurs postes de travail - la fermeture d'une succursale entière ou des guichets automatiques demeurant peu fréquentes. Pour répondre aux cyberattaques, les institutions financières misent avant tout sur des prestataires externes, ce qui est prévisible en raison de leurs ressources humaines et techniques très limitées. La police est très rarement mentionnée et les organismes nationaux spécialisés pour ainsi dire jamais.

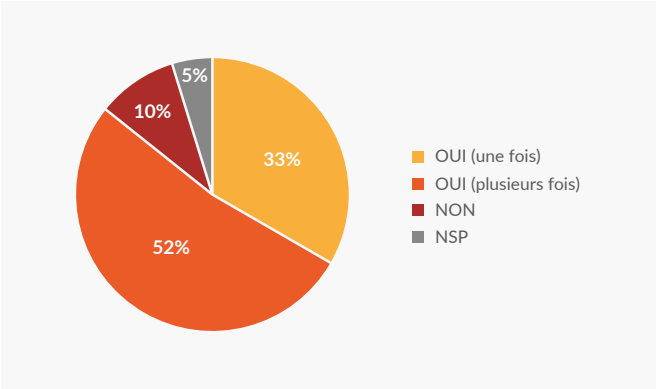
L'impact financier des cyberattaques est en moyenne de 770 000 euros, mais bien des répondants ont refusé de répondre à la question. Parmi ceux qui n'ont pas voulu donner de chiffres, on notera des réponses parlant d'une simple question de quelques heures de travail perdues.

05 LES CYBERATTAQUES ET LEURS IMPACTS

5.1 - Entreprises ayant subi des cyberattaques

Une grande majorité d'au moins 85% des institutions financières consultées déclare avoir déjà été victime d'une ou plusieurs cyberattaques – dans certains cas, il s'agit même d'attaques à répétition. Il faut souligner que la question porte uniquement sur les cyberattaques ayant entraîné des dommages. Sinon, toutes les entreprises affrontent des cyberattaques en mode continu, a fortiori les banques.

FIGURE 22 - VOTRE ENTREPRISE A-T-ELLE DÉJÀ SUBI UNE CYBERATTAQUE AVEC DOMMAGES ?



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

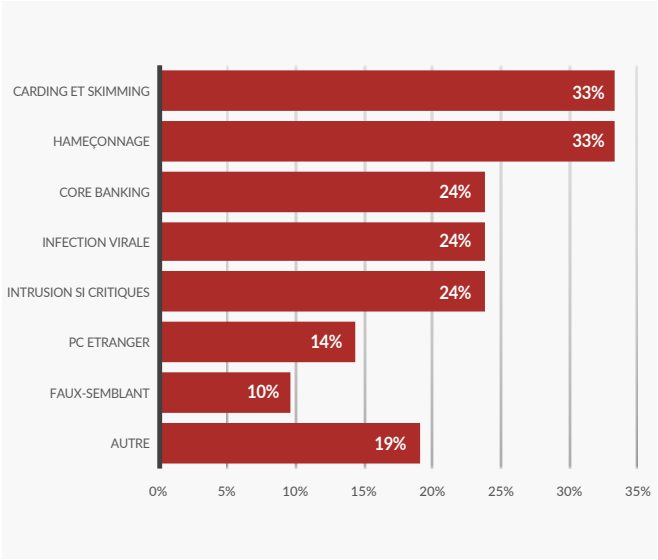
La très grande majorité des institutions a subi des cyberattaques « réussies » qui parviennent à prendre le contrôle d'un système d'information, à dérober ses données ou à paralyser son fonctionnement. Ces cyberattaques occasionnent des coûts moyens de 9 000 euros pour chaque ordinateur infecté par un programme malveillant (*malware*)[27]. Pour peu que l'attaque ne soit pas contenue, le montant global des dommages peut rapidement devenir catastrophique – sans parler des atteintes portées à l'image de marque de l'institution financière.

C'est sans compter les sommes qui peuvent être dérobées dans les comptes bancaires au moyen de versements frauduleux. Au début de l'année 2019, une série de cyberattaques de banques ont porté sur des vols allant de quelques dizaines de milliers d'euros à plusieurs centaines de milliers d'euros. Selon les médias, la plus importante cyberescroquerie a même provoqué des pertes cumulées de l'ordre de deux millions d'euros[28]. Comme on le constate, les montants ainsi dérobés peuvent atteindre des montants dévastateurs pour la banque.

5.2 - Nature des cyberattaques

Globalement, ce sont les fraudes sur les cartes bancaires (*carding* et *skimming*) ainsi que l'hameçonnage (*phishing*) qui sont les types de cyberattaques les plus fréquents (33% chaque) suivies des atteintes au *core banking*, les infections virales et les intrusions dans les systèmes d'information critiques (24% chaque). Les attaques par branchement d'un poste de travail étranger et les infections par faux-semblant (*pretexting*) sont mentionnées marginalement. Dans la catégorie « autre », on retrouve pêle-mêle la fuite d'information, l'usurpation d'identité, les fraudes par transfert d'argent ou retrait sur des faux chèques, etc.

FIGURE 23 - TYPES DE CYBERATTAQUES
(le total n'est pas égal à 100, car la plupart des institutions ont subi plusieurs types d'attaques)



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Une autre façon de classifier les cyberattaques consiste à distinguer le vandalisme (infections virales, destruction gratuite, piratage de site web) des fraudes motivées par le gain. À l'exception des infections virales, toutes les cyberattaques relevées dans le cadre de l'enquête sont motivées par le gain. Manifestement, les banques africaines ont affaire à des criminels professionnels.

27 "Global Software Survey", (Software Management: Security Imperative, Business Opportunity), BSA, 2018, 20 pages. Cf. p. 2.
28 Stéphanie Wenger, « Piratage : quand l'Afrique prend sa sécurité en main », Jeune Afrique, 27 mars 2019.

05 LES CYBERATTAQUES ET LEURS IMPACTS

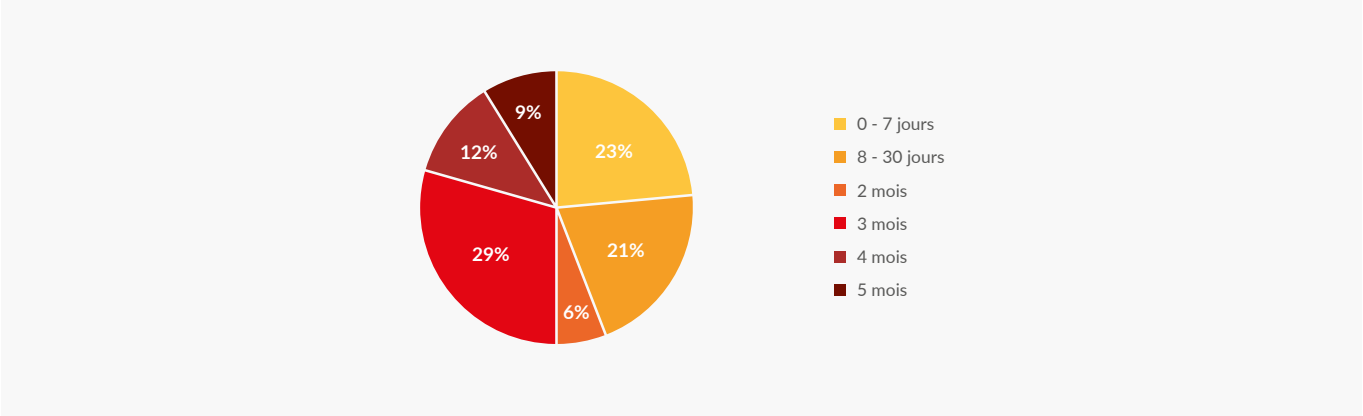
5.3 - Temps de latence

Les cyberattaques ne sont pas spectaculaires. Ce n'est pas comme un vol à main armée qui a lieu dans le bruit et la fureur avec trop souvent son cortège de victimes. Au contraire, une intrusion informatique se déroule dans le silence électronique. La plupart du temps, elle passe inaperçue et, plus le cybercriminel est habile, moins l'institution financière a de chance de savoir qu'il y a une brèche furtive dans son périmètre informatique. Pourtant, c'est la phase la plus importante de la cyberattaque : la préparation du crime.

Il faut savoir que le but du cybercriminel est de se maintenir dans le système d'information aussi longtemps que possible. Son but est de recenser toutes les défenses mises en place par la banque, puis de les contourner soigneusement afin de parvenir au but fixé qui est toujours de voler de l'information. Or, la brèche a d'autant moins de chance d'être découverte qu'elle représente un événement seulement au milieu des millions d'événements qui surviennent chaque jour dans un réseau.

Au total, la moitié des incidents signalés dans l'enquête de DATAPROTECT ont mis trois mois et plus pour être découverts. Cela laisse toute latitude aux assaillants pour commettre leurs méfaits. Parfois, une anomalie est décelée dans un poste de travail isolé, alors que l'attaque principale se déroule à l'échelle du système d'information dans son ensemble. Moins du quart des incidents est identifié en moins d'une semaine.

FIGURE 24 - TEMPS ÉCOULÉ ENTRE LA CYBERATTAQUE ET LA DÉCOUVERTE DE L'INCIDENT



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

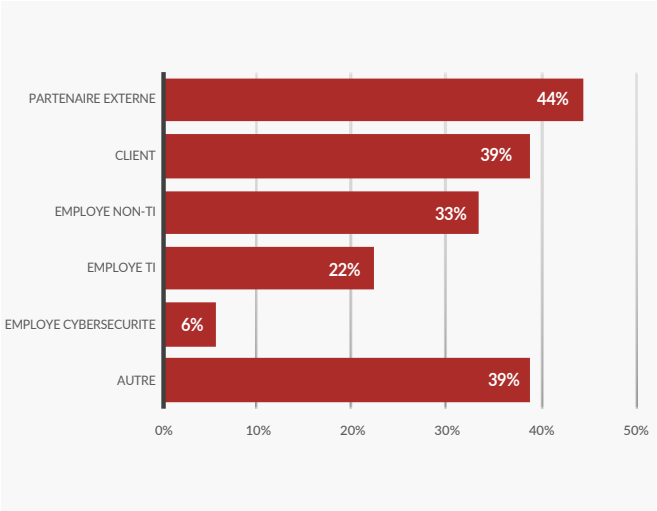
La longueur du temps de détection renvoie à la carence d'outils et de ressources nécessaires à l'identification des anomalies. Surveiller le réseau informatique et le pare-feu est une tâche qui requiert des moyens considérables et qui est inefficace une fois que la brèche a eu lieu et que l'ennemi est installé dans le système central. En outre, la plupart des événements identifiés par les solutions standardisées de surveillance se révèlent après analyse être des faux-positifs. Un système bien ordonné de cybersécurité consiste à repérer les signaux faibles suscités par l'intrusion avant le passage à l'acte criminel proprement dit.

Voilà pourquoi, il est pratique de recourir à un SOC. Le SOC recourt à l'intelligence artificielle pour analyser les logs de manière centralisée et établir des liens entre les différents événements. À titre d'exemple, si un individu exécute 10 000 ou plus essais d'intrusion sur un serveur, l'ensemble sera traité comme un seul événement. De cette façon, il devient possible de traiter des millions d'événements par jour et de filtrer les faux-positifs pour ne conserver que les incidents réels.

5.4 - Qui a découvert l'incident ?

Seulement 6% des incidents sont découverts par les employés de cybersécurité des institutions financières. Au total, 61% des incidents ont été découverts par des employés des banques et 83% par des intervenants extérieurs – certains ont pu l'être à la fois à l'interne et à l'externe. Les réponses « autres » recouvrent toute une gamme de situations : l'incident a été signalé lors d'une demande de rançon, grâce à la détection de mouvements bancaires suspects, à l'occasion du rapprochement et des arrêtés de fin de journée, par une alerte du dispositif de contrôle interne ou même dans les médias.

FIGURE 25 - L'INCIDENT A ÉTÉ DÉCOUVERT PAR UN…
(le total n'est pas égal à 100, car les incidents ont pu être décelés par plusieurs catégories d'intervenants)



Source : Étude Sciencetech/DataProtect, février-août 2019.

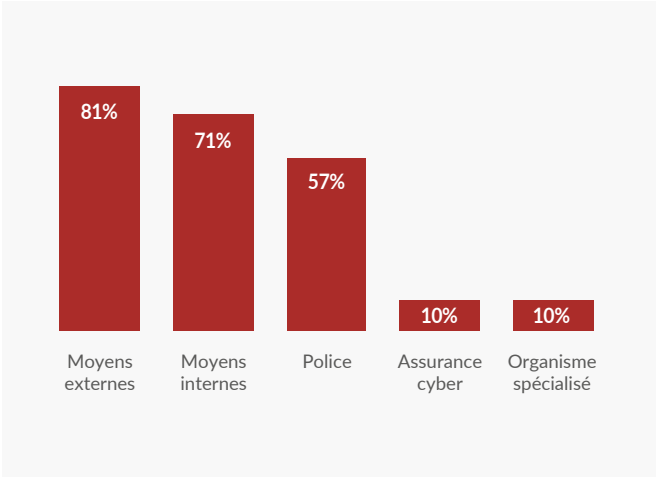
Analyse

L'environnement extérieur de la banque joue un rôle essentiel dans le repérage des incidents. Voilà pourquoi, il est indispensable de mettre au point des forums de partage d'information avec les fournisseurs et les partenaires ainsi que des processus pour faire remonter l'information depuis les clients individuels. La cybersécurité ne peut être assurée par une organisation isolée. De même que les cybercriminels collaborent entre eux, les institutions financières doivent tisser des réseaux de solidarité pour protéger leurs actifs informationnels. Toute stratégie de cybersécurité est obligatoirement collective.

5.5 - Réaction aux cyberattaques

Pour répondre aux cyberattaques, les institutions financières misent avant tout sur des prestataires externes (81%) et c'est prévisible puisque leurs ressources humaines et techniques sont très limitées. Les moyens internes sont aussi mobilisés mais ils sont mentionnés en second (71%). Si la police est souvent appelée en renfort, les compagnies d'assurance et les organismes nationaux spécialisés en cybersécurité sont cités à titre marginal seulement.

FIGURE 26 - À QUI L'ENTREPRISE A-T-ELLE FAIT APPEL EN RÉACTION AUX CYBERATTAQUES ?
(le total n'est pas égal à 100, car la plupart des institutions ont fait appel à plusieurs catégories d'intervenants)



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

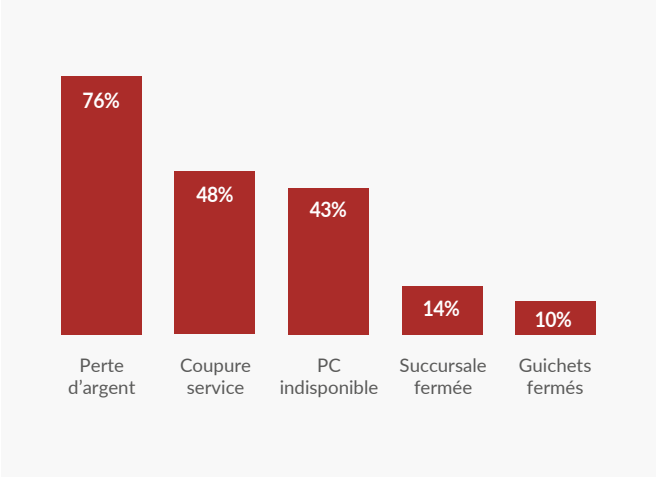
L'absence des gouvernements quand survient une cyberattaque est le fait notoire de cette enquête – les seules exceptions proviennent de Côte d'Ivoire. Cela provient de l'absence d'organisme national spécialisé en cybersécurité dans la plupart des pays. Les banques sont laissées à elles-mêmes, ce qui renforce l'incitation à recourir au partage d'information avec d'autres organisations.

05 LES CYBERATTAQUES ET LEURS IMPACTS

5.6 - Impact des incidents

La perte d'argent est le principal impact des cyberattaques (76%) suivie de la suspension des services en ligne (48%) et de l'indisponibilité d'un ou plusieurs postes de travail (43%) – la fermeture d'une succursale entière ou des guichets automatiques, est peu fréquente.

FIGURE 27 - QUEL A ÉTÉ L'IMPACT DE L'INCIDENT ?
(le total n'est pas égal à 100, car les institutions ont subi plusieurs types d'impacts)



Source : Étude Sciencetech/DataProtect, février-août 2019.

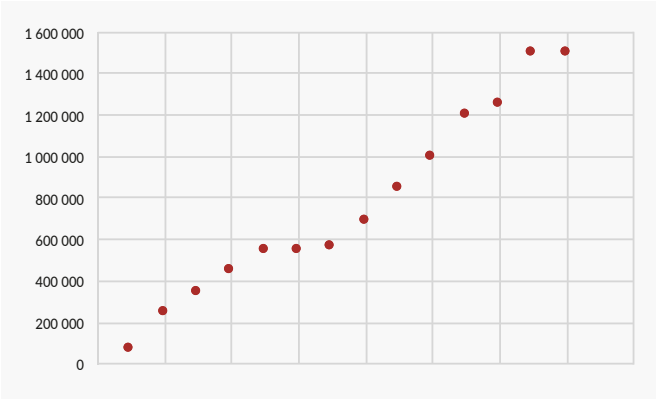
Analyse

La perte d'argent a trois sources : la mutation de la cybercriminalité vers l'extorsion, les dommages logiciels encourus et le manque à gagner dus à l'interruption des activités. Tous les types de cyberattaques se traduisent par un impact financier direct ou indirect – même les atteintes à la réputation de la banque ont un coût. Si les données personnelles des clients sont dérobées suite à une cyberattaque, ces derniers peuvent fermer leurs comptes et, peut-être plus grave, de nouveaux clients se détourner de l'institution.

5.7 - Coût des incidents

L'impact financier des cyberattaques est difficile à évaluer, car, comme on l'a vu, les entreprises répugnent à avouer qu'elles ont subi des dommages et encore plus à donner un chiffre. Parmi les entreprises qui ont accepté d'évoquer leurs coûts, la perte moyenne est de 770 000 euros, encore s'agit-il de pertes cumulatives s'échelonnant sur plusieurs années. Parmi ceux qui n'ont pas voulu donner de chiffres, on notera des réponses parlant d'une simple question de quelques heures de travail perdues.

FIGURE 28 - MONTANT DES DOMMAGES EN EUROS
(y compris le temps des employés, le recrutement de consultants en informatique, les applications de cybersécurité et de matériel connexe, le remboursement des clients, les amendes imposées par les autorités, etc.)



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

La plupart des cyberattaques échouent ou sont bloquées avant d'avoir fait des dégâts significatifs. Cette insignifiance de la menace cyber n'est qu'apparente. Trop souvent, les gens confondent attaques génériques et attaques ciblées. Les attaques génériques fonctionnent comme un bruit de fond sur Internet. Virus, rançongiciels et ingénierie sociale cognent à toutes les portes en permanence. Leur nuisance affecte surtout les organisations mal préparées, sans programme de cybersécurité et sans véritable équipe de cybersécurité pour veiller au grain. On a vu que ces organisations sont encore très nombreuses dans le secteur financier africain[29].

Entièrement différentes sont les attaques ciblées. On quitte le domaine des amateurs et des vandales pour entrer dans celui du crime organisé - encore que des loups solitaires puissent commettre des dommages considérables. Par définition, une banque a toujours une information de valeur ou une situation stratégique.

Le caractère spectaculaire des attaques ciblées et leur relative rareté ont fait croire qu'elles étaient réservées à de grandes organisations (Adobe, Sony, Target, Equifax, Marriott, Yahoo, etc.). C'était peut-être vrai dans le passé. Ce n'est plus le cas aujourd'hui. Avec la « démocratisation » de la cybercriminalité, toutes les organisations sont dans la mire des malfaiteurs.

29 On a vu que 38% des répondants à cette enquête n'ont pas de programme formel de cybersécurité, près de la moitié n'ont pas procédé à un audit des systèmes d'information ou à une analyse de risque, près de la moitié encore n'ont pas de plan de relève. Or, ne l'oublions pas, les organisations interrogées dans le cadre de cette enquête sont des banques, donc des organisations plus avancées sur le plan technologique que la moyenne africaine.

06

CADRE LEGAL ET REGLEMENTAIRE

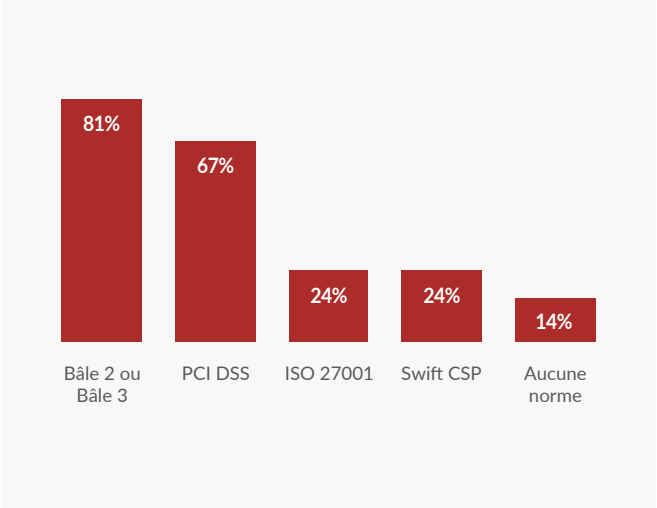
La plupart des banques africaines déclarent souscrire aux accords de Bâle 2 ou Bâle 3 et une bonne majorité de banques a aussi adopté la norme PCI DSS relative à l'utilisation des cartes de crédit. Ce qui est anormal est que 14% d'entre elles aient déclaré n'avoir adopté aucune norme de cybersécurité. À l'inverse, le respect des normes internationales par les banques explique le succès croissant du secteur financier en Afrique. À bien des égards, on peut dire que le secteur financier joue un rôle de modèle structurant pour le reste de l'économie africaine.

06 CADRE LEGAL ET REGLEMENTAIRE

6.1 - Normes ou règlements en vigueur

La plupart des banques déclarent souscrire aux accords de Bâle 2 ou Bâle 3 qui, comme on l'a signalé, émettent des recommandations importantes en matière de résilience opérationnelle. Une grande majorité de banques a aussi adopté la norme PCI DSS qui veille à la sécurité des données tout au long de la chaîne d'utilisation des cartes de crédit. Les normes ISO 27001 et Swift CSP suivent loin derrière, ce qui n'est pas étonnant dans le cas de la première qui est purement volontaire, moins dans le cas de la seconde qui est indispensable pour les transactions internationales.

FIGURE 29 - NORMES DE SÉCURITÉ EN VIGUEUR DANS LES BANQUES
(le total n'est pas égal à 100, car les institutions ont généralement adoptés plusieurs normes)



Source : Étude Sciencetech/DataProtect, février-août 2019.

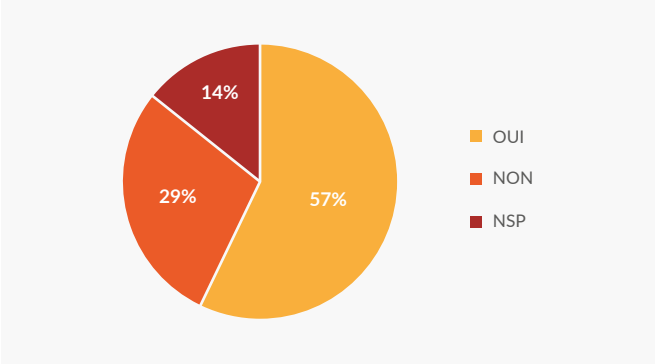
Analyse

Le fait saillant de la situation des banques africaines est que 14% d'entre elles aient déclaré n'avoir adopté aucune norme de cybersécurité. Il est paradoxal qu'une institution financière puisse fonctionner sans se référer aux accords de Bâle et à Swift. Précisons qu'il s'agit de petites institutions (moins de 300 employés) situées hors de la zone UEMOA. La grande majorité des banques africaines (86%) suivent les grandes normes de cybersécurité internationale. Cette stratégie explique d'ailleurs le succès croissant du secteur financier en Afrique. Cette garantie de bonne gouvernance inspire confiance aux consommateurs et, encore plus, aux entreprises. La banque joue un rôle de modèle structurant pour le reste de l'économie.

6.2 - Vérification de la conformité aux normes

Une majorité de 57% des institutions financières vérifie périodiquement la conformité des normes de cybersécurité – les autres ne le font pas ou ne le savent pas, ce qui signifie probablement qu'elles ne le font pas non plus. La norme qui est le plus souvent citée est PCI DSS (42%), suivie des accords de Bâle 2 (33%) et de Swift CSP (25%).

FIGURE 30 - VÉRIFICATION DE CONFORMITÉ



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Adopter une norme est un premier pas nécessaire, mais qui ne garantit pas la cybersécurité. En matière de norme, la vérification périodique des bonnes pratiques en fonction d'un référentiel de mise en œuvre et d'une liste de pointage (*check list*), est tout aussi important que l'adoption initiale. Pour cela, il convient que les données de l'ensemble des systèmes et applications soient en permanence collectées et archivées en un point unique. Dès lors, les informations peuvent être analysées et compilées en rapports réguliers. Faute de quoi, la certification tombe et tout le travail consacré à la mise en place du programme, est perdu.

À titre d'exemple, la certification ISO 27001 est valable trois ans à condition qu'un audit de contrôle soit effectué tous les ans. La banque qui adopte une norme doit obligatoirement déployer un programme de gestion de la cybersécurité qui exige de réorganiser son environnement de travail et d'intégrer une série précise de mesures à suivre dans la gestion quotidienne. Cet engagement de tous les instants est précisément l'effet souhaité par les organismes qui instituent les normes. Or, 57% seulement des banques africaines satisfont à ces exigences.

07

INVESTISSEMENTS EN CYBERSECURITE

L'investissement en cybersécurité des banques africaines demeure très modeste. Quatre-vingt-cinq pour cent des banques investissent moins de 500 000 € par an en cybersécurité alors qu'elles reconnaissent avoir déjà essuyé des pertes moyennes nettement supérieures (770 000 euros, voir plus haut). Il apparaît clairement que la cybersécurité coûte cher, mais que l'absence de cybersécurité coûte encore plus cher, surtout dans le secteur financier où le risque est maximal.

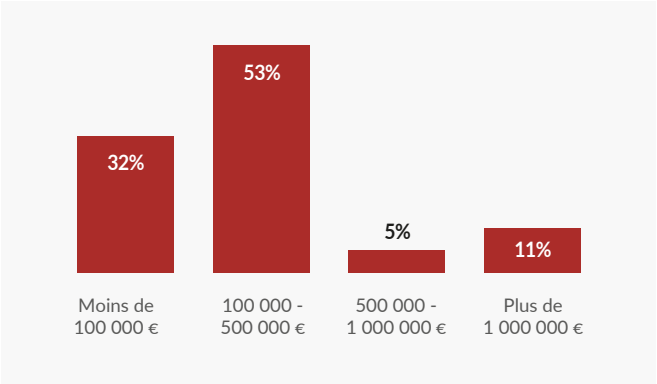
Près des trois-quarts des investissements en cybersécurité sont à la hausse : il s'agit sans conteste d'un premier élément de réponse à la modestie des budgets. Les institutions financières qui prévoient des coupes budgétaires sont rares. Au total, près des deux-tiers des personnes interrogées ne jugent pas satisfaisant l'outillage de cybersécurité déployé dans leur banque.

07 INVESTISSEMENTS EN CYBERSECURITE

7.1 - Montant investi sur une base annuelle

Un tiers des institutions financières ont investi moins de 100 000 € en cybersécurité en 2018. Sans surprise, ce sont les petites banques qui constituent la totalité de cette catégorie. Environ la moitié des banques investit entre 100 000 et 500 000 € annuellement. D'une façon générale, la courbe des investissements épouse assez exactement la taille de la banque.

FIGURE 31 - MONTANT ANNUEL INVESTI EN CYBERSÉCURITÉ (2018)



Source : Étude Sciencetech/DataProtect, février-août 2019.

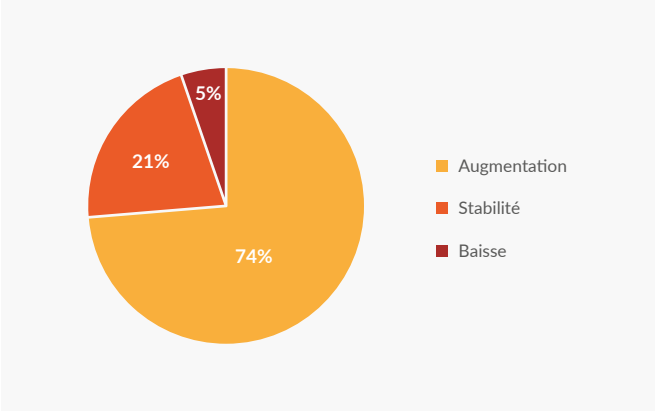
Analyse

L'investissement en cybersécurité des banques africaines demeure très modeste. Quatre-vingt-cinq pour cent des banques investissent moins de 500 000 € par an en cybersécurité alors qu'elles reconnaissent avoir déjà essuyé des pertes moyennes de 770 000 € à ce seul chapitre (voir section 5.7 - Coût des incidents). Il apparaît clairement que la cybersécurité coûte cher, mais que l'absence de cybersécurité coûte encore plus cher. Pourtant, les institutions financières continuent à investir peu, voire très peu, en cybersécurité. S'il est une règle d'or en cybersécurité, c'est bien que « les investissements doivent être proportionnels au risque informationnel encouru par l'entreprise.[30]» Or, c'est dans le secteur financier que le risque est maximal.

7.2 - Prévisions d'investissement pour 2019

Près des trois-quarts des investissements en cybersécurité sont à la hausse : il s'agit sans conteste d'un premier élément de réponse à la modestie des budgets. Curieusement, la minorité qui prévoit des investissements stables a des budgets supérieurs à 100 000 €, c'est-à-dire qu'il s'agit de banques où on peut supposer une certaine conscience du risque. Les institutions financières qui prévoient des coupes budgétaires sont rares.

FIGURE 32 - ÉVOLUTION PRÉVUE DE L'INVESTISSEMENT



Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

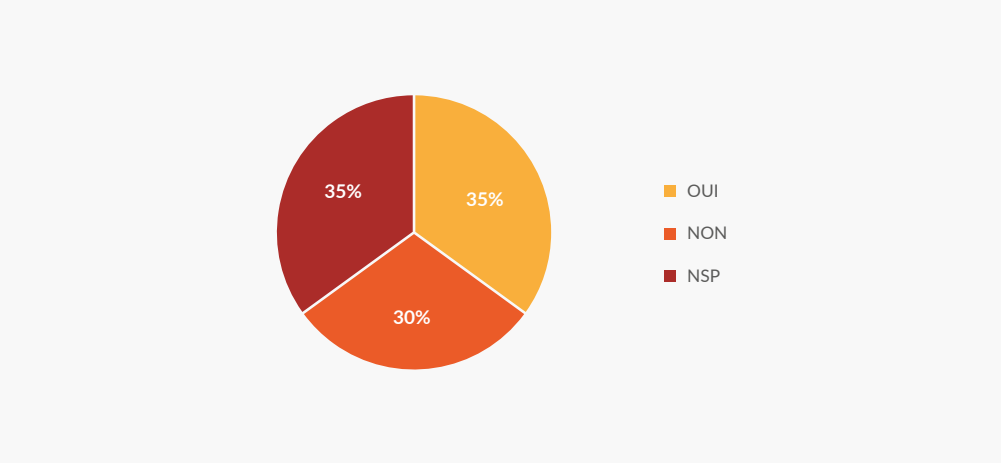
L'augmentation des investissements en cybersécurité atteste de la volonté des institutions financières de combler ses carences. Cette tendance haussière corrobore l'estimation d'Orange Cyberdefense qui prévoit que le marché de la cybersécurité en Afrique passe de 1,5 milliard d'euros en 2017 à plus de 2,2 milliards d'euros en 2020[31]. Comme les banques sont en pointe de la lutte contre la cybercriminalité, il est normal que la hausse se fasse sentir en priorité dans leurs budgets.

30 Solange Ghernaouti, "Cybersécurité: Sécurité informatique et réseaux", éditions Dunod, 2016, 384 pages. Cf. p. 69.
31 "L'investissement de l'Afrique dans la cybersécurité", Africa News, 25 octobre 2018.

7.3 - Bilan général de la cybersécurité : niveau de satisfaction

Près du tiers des personnes interrogées n'hésitent pas à considérer l'état de préparation de leur institution financière comme insatisfaisant. Si on y ajoute la masse de celles qui refusent de trancher (35%), on obtient une grande majorité de responsables qui ne jugent pas satisfaisant l'outillage de cybersécurité déployé dans leur banque (65%).

FIGURE 33 - LA BANQUE EST-ELLE BIEN OUTILLÉE EN MATIÈRE DE CYBERSÉCURITÉ ?

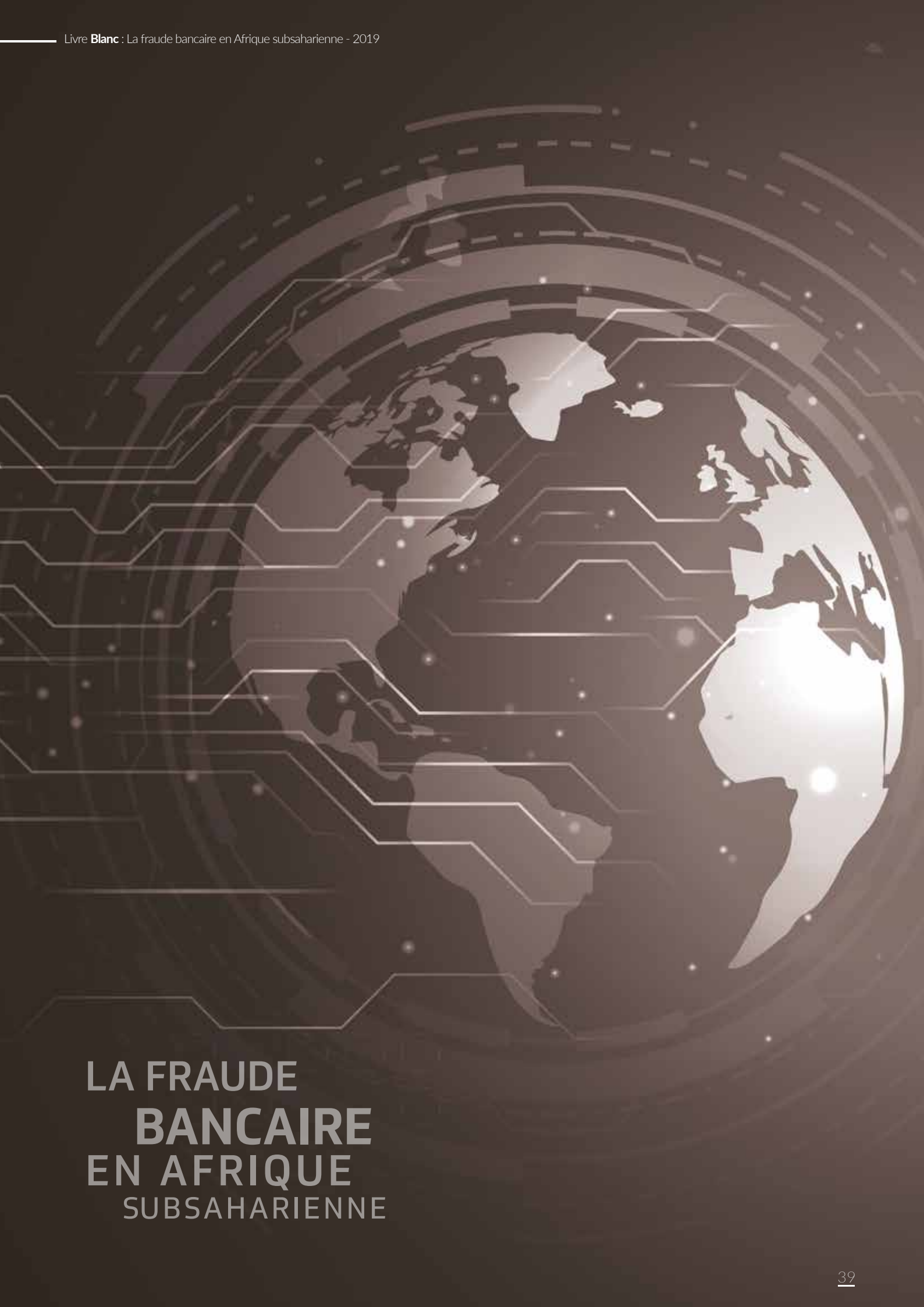


Source : Étude Sciencetech/DataProtect, février-août 2019.

Analyse

Encore faut-il souligner que ces données relèvent de la perception. Dans les faits, la situation est quelque peu différente. Certaines banques, dont les responsables jugent l'outillage satisfaisant, n'ont pas de programme formel de cybersécurité (5%), d'autres ne suivent pas la réglementation des accords de Bâle (5%) et d'autres encore n'effectuent pas de surveillance permanentes des évènements de sécurité (15%).

Ce sont ces quelques banques aux dirigeants et responsables TI satisfaits, alors que les assises fondamentales de la cybersécurité sont absentes, qui sont les plus à risque. Heureusement, elles sont très minoritaires. Reste que ce tableau d'ensemble renvoie une fois de plus au manque de maturité de la cybersécurité dans le secteur financier.



LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

08 CONCLUSION ET ENJEUX

Environ 20% des banques africaines ayant participé à l'enquête affichent un taux de cybersécurité relativement satisfaisant (institutions financières qui satisfont à huit facteurs essentiels : nomination d'un RSSI, adoption des recommandations des accords de Bâle 2, présence d'un plan de formation ou de sensibilisation, etc.) A contrario, 80% des banques africaines sont vulnérables aux cyberattaques.

Les grands enjeux de la cybersécurité sont le partage d'information, le partenariat avec les fintechs et la mutualisation des ressources (abonnement à un SOC externe).

08 INVESTISSEMENTS EN CYBERSECURITE

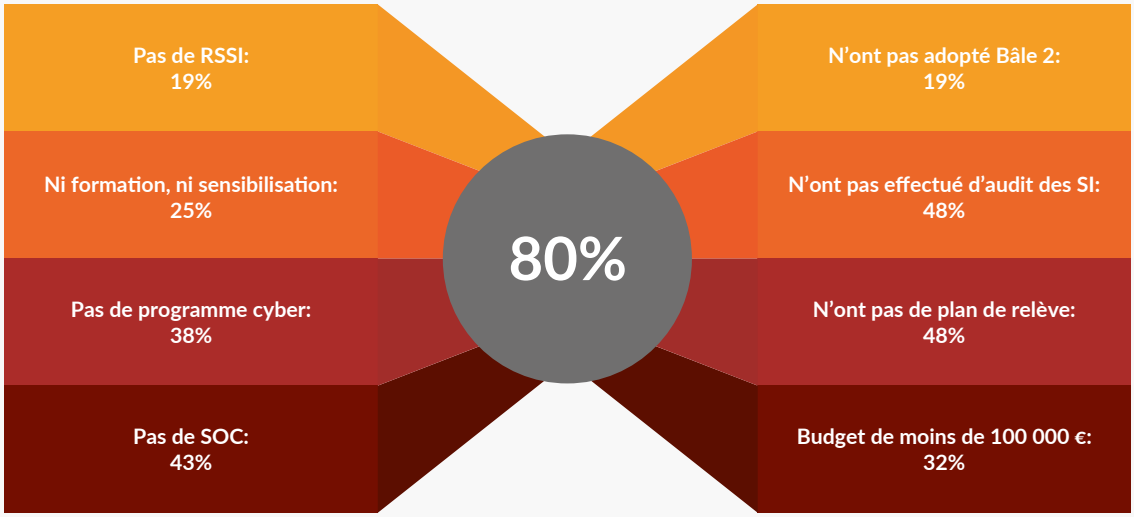
8.1 - Conclusion d'ensemble

Environ 20% des banques africaines ayant participé à l'enquête affichent un taux de cybersécurité relativement satisfaisant, ce qui ne veut pas dire qu'elles sont immunisées contre la cybercriminalité, mais qu'elles réussiront à prévenir la majeure partie des intrusions, circonscrire les dommages et remédier aux attaques.

Cela signifie que ces institutions financières satisfont à huit facteurs essentiels : nomination d'un RSSI, adoption des recommandations des accords de Bâle 2, présence d'un plan de formation ou de sensibilisation, réalisation d'un audit des systèmes d'information (SI), élaboration d'un programme de cybersécurité et d'un plan de relève, recours à un SOC et budget annuel supérieur à 100 000 €. Il ne suffit pas de répondre à quelques-uns de ces critères pour être sécuritaire : il faut répondre à tous.

Par contre, cela signifie que 80% des banques africaines sont vulnérables aux cyberattaques. Incapables de parer aux attaques, elles opèrent les yeux fermés dans une zone à haut risque et, une fois frappées, elles subiront des dommages maximums.

FIGURE 34 - PROPORTION DES BANQUES À RISQUE



Source : Étude Sciencetech/DataProtect, février-août 2019.

8.2 - Enjeux

Toute stratégie de cybersécurité est basée sur le partage d'information. Ce partage d'information ne relève pas du simple réseautage, il s'apparente plutôt à un outil pour prévenir les incidents de cybersécurité – peut-être même s'agit-il du meilleur outil de cybersécurité. En effet, celle-ci ne peut pas être assurée par une équipe isolée, aussi talentueuse soit-elle, mais par la création d'échanges constants des meilleures pratiques entre toute la communauté des experts.

Enjeu No 1 - Partage d'information

Dans le domaine de la cybersécurité, le partage d'information ne relève pas du simple « networking », il s'apparente plutôt à un outil pour prévenir les incidents de cybersécurité - peut-être même s'agit-il du meilleur outil de cybersécurité. La cybersécurité ne peut pas être assurée par une équipe de deux ou trois personnes, aussi talentueuse soit-elle, mais par la création d'échanges constants et systématiques des meilleures pratiques entre toute la communauté financière.

L'information partagée porte aussi bien sur l'existence de la menace elle-même, les indicateurs techniques (caractéristiques de la menace) et les données opérationnelles (nature de l'attaque et nature de la cible, contre-mesures déployées, etc.). C'est cet ensemble de processus qu'il convient de formaliser de manière détaillée. À cette fin, il est indispensable de créer un cadre de concertation.

Ce partage est généralement volontaire, mais encore faut-il créer le cadre législatif, réglementaire et financier propice. Quand Israël a voulu inciter ses institutions financières à partager l'information, il a placé son CERT à leur disposition et a adopté un règlement exemptant les activités de partage de poursuites antitrust[32].

Le partage peut aussi être obligatoire. L'Union européenne (UE) a émis en 2016 la « directive NIS » qui vise à faciliter le partage d'informations techniques sur les risques et vulnérabilités entre les opérateurs d'infrastructures essentielles. Pour cela, les États membres de l'UE ont dû se doter d'équipes nationales de réponse aux incidents informatiques (CSIRT) dans un délai de deux ans. Tout incident ayant un impact significatif doit être notifié à l'autorité nationale ou au CSIRT qui détermine alors si l'information doit être transmise aux autres États membres ou non.

Il y a là un rôle clé à jouer pour la Banque Centrale des États de l'Afrique de l'Ouest (BCEAO). Sa position transnationale en fait un acteur clé du partage de l'information. La BCAO pourrait envisager de créer un groupe de travail destiné à étudier les différentes modalités destinées à encourager le partage d'information parmi les institutions financières sur une base volontaire ou obligatoire.

Enjeu No 2 - Partenariat avec les fintechs

L'Afrique bénéficie d'une industrie des fintechs en plein essor qui attire déjà l'attention des investisseurs internationaux. Pour les banques, ces fintechs ne sont pas des adversaires et doivent être considérées comme des partenaires, surtout dans le sous-secteur de la cybersécurité. Alors que le déploiement d'une architecture du système bancaire de base (*core banking*) prend deux ou trois ans, une application fintech a un horizon temporel de quelques semaines. Cela signifie que les processus du système bancaire de base sont désuets dès leur inauguration et que pour les sécuriser, il faudra ajouter des couches et des couches de logiciel[33].

À titre d'exemple, la plateforme de système bancaire de base TagPay permet de mettre en place une banque opérationnelle digitale en trois mois, avec l'ensemble des fonctionnalités nécessaires à la gestion d'un compte bancaire. Autrement dit une solution clé en main pour les acteurs bancaires agréés permettant de lancer et de gérer des services digitaux[34]. Concrètement, TagPay permet à ses clients de proposer des services financiers de tous genres par le simple biais d'un téléphone portable, indépendamment des opérateurs de télécommunications et sans besoin de se déplacer dans une agence bancaire classique.

32 Deborah Housen_Couriel, "Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing two Nascent Models", Part 2, European Cybersecurity Journal, vol. 5, issue 1, Cracovie (Pologne), 2019.
33 Yves Eonnet et Hervé Manceron, "Fintech : les banques contre-attaquent", éditions Dunod, 2018, 176 pages. Cf. P. 29.
34 Aude Chardenon, "TagPay, la fintech qui veut aider les banques à affronter... les néobanques", L'usine digitale, 20 février 2019.

08 INVESTISSEMENTS EN CYBERSECURITE

Enjeu No 3 - Mutualiser les ressources

Le déploiement d'un SOC est la plupart du temps hors de portée pour les institutions financières de taille modeste – parfois même les plus grandes d'entre elles éprouvent des difficultés à gérer un outil aussi spécialisé et aussi éloigné de leur activité centrale. En effet, un SOC complet doit pouvoir fonctionner 24 heures sur 24 et sept jours sur sept. Cela nécessite au minimum cinq employés à plein temps pour assurer la présence d'un analyste sur toute la période de surveillance. Ces employés doivent avoir une solide formation en applications réseaux et parfois même en rétro-ingénierie (*reverse engineering*).

La valeur ajoutée de l'externalisation d'un SOC permet non seulement de réduire les coûts de mise en œuvre et d'exploitation mais également de bénéficier de l'expertise et des compétences que seule peut réunir une entreprise spécialisée en cybersécurité. Cette diminution des coûts peut s'avérer considérable. En effet, pour un SOC interne, il faut prévoir entre 1 060 000 € et 1 870 000 € pour les seuls coûts du développement et du maintien de la plateforme mais sans les coûts d'acquisition des équipements. Tandis pour un SOC géré par un prestataire externe, il faut compter un budget entre 90 000 € et 250 000 €[35].

Enfin, autre avantage appréciable, l'institution financière qui fait appel à un prestataire spécialisé bénéficie de l'expérience acquise par ce dernier auprès des autres clients. Le SOC devient un outil mutualisé du type « *security as a service* » qui peut mettre à profit les toutes dernières technologies pour adopter une posture à la fois proactive (identification des signaux faibles) et réactive (protection immédiate du système d'information).

35 Hassan Meddah, "Pourquoi privilégier l'externalisation de son centre d'opérations de cybersécurité", L'usine nouvelle, 02 septembre 2017.

Annexe 01

INDICE MONDIAL DE CYBERSECURITE (GCI)

Extrait de l'Indice mondial de cybersécurité (GCI) concernant les pays qui font l'objet de l'étude DATAPROTECT. L'enquête de l'UIT mesure au moyen d'un « tableau de bord régional » l'engagement des États membres vis-à-vis de chaque pilier et sous-piliers : vert pour un niveau élevé, jaune pour moyen et rouge pour faible.

Annexe 01 INDICE MONDIAL DE CYBERSECURITE (GCI)

Extrait de l'Indice mondial de cybersécurité (GCI) concernant les pays qui font l'objet de l'étude DATAPROTECT. L'enquête de l'UIT mesure au moyen d'un « tableau de bord régional » l'engagement des États membres vis-à-vis de chaque pilier et sous-piliers : vert pour un niveau élevé, jaune pour moyen et rouge pour faible.

	Bénin	Burkina Faso	Côte d'ivoire	Guinée Bissau	Mali	Niger	Sénégal	Togo	Congo (Brazza)	Gabon	RDC
Législation de la cybercriminalité											
Législation de la cybersécurité											
Formation en cybersécurité											
MESURES JURIDIQUES											
CERT/CIRT/national											
CERT/CIRT/gouvernemental											
CERT/CIRT/sectoriel											
Normes pour les organisations											
Normes pour les professionnels											
Protection en ligne pour les enfants											
MESURES TECHNIQUES											
Stratégie											
Responsabilité organisationnelle											
Indicateurs de cybersécurité											
MESURES ORGANISATIONNELLES											
Organisations de normes											
Bonnes pratiques en cybersécurité											
Programme de R-D											
Campagnes de sensibilisation publiques											
Cours de formation professionnelle											
Programmes éducatifs											
Mécanismes d'incitation											
Industrie domestique											
RENFORCEMENT DE CAPACITÉ											
Accords bilatéraux											
Accords multilatéraux											
Engagement international											
Partenariats public-privés											
Partenariats inter-organisationnels											
COOPÉRATION											
INDEX GLOBAL GCI											

Source: UIT, Global Cybersecurity Index 2017, cf. p. 27.

Il s'agit de la deuxième édition de l'Indice mondial de cybersécurité 2017, publié par l'Union Internationale des Télécommunications (UIT), agence des Nations Unies, afin de mesurer l'engagement des 193 États membres de l'UIT en matière de cybersécurité et de mettre en lumière un certain nombre de pratiques illustratives du monde entier.

Le GCI s'articule autour du Programme mondial de cybersécurité de l'UIT (GCA) et de ses cinq piliers : juridique, technique, organisationnel, renforcement des capacités et coopération.

ANNEXE 02
QUESTIONNAIRE

DATAPROTECT
Security is our commitment

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

Cette initiative vise à promouvoir la cybersécurité dans l'industrie et dans le secteur des services financiers en Afrique. En dressant le panorama des mesures prises par les institutions financières en matière de cybersécurité, Dataprotect vise deux buts : évaluer le degré de maturité du marché de la cybersécurité et promouvoir les meilleures pratiques dans ce domaine.

La cybersécurité est devenue un atout stratégique dans le développement du secteur financier. Or, celui-ci est spectaculaire en Afrique subsaharienne. D'après McKinsey & Company, le nombre d'Africains bancarisés est passé de 170 millions en 2012 à 300 millions en 2017. Ce chiffre devrait atteindre 450 millions en 2022. Cette croissance se fait dans un contexte de très grande rentabilité : le ROI du secteur bancaire atteint 14,9% en Afrique – contre une moyenne mondiale de 8,6%.

L'effervescence du secteur bancaire africain ne doit pas masquer les deux grands défis qu'il doit affronter. D'une part, comme partout dans le monde, les banques sont en pleine transition vers la numérisation de leurs processus : banque en ligne, applications mobiles, toutes les transactions sont en passe d'être dématérialisées. D'autre part, le continent africain a vu la montée d'une concurrence sans pareille au monde de la part de l'argent mobile. Bien sûr, les banques occidentales doivent elles aussi se mesurer aux néo-banques et aux fintechs. Mais c'est en Afrique que le phénomène a pris le plus d'ampleur avec de plus en plus le concours actif des opérateurs de télécommunications comme Safaricom et Orange Money. Un peu partout, des start-ups de technologies financières se multiplient qui proposent des services à valeur ajoutée.

Dans ce contexte hautement volatile, les banques font face à un paradoxe : elles doivent ouvrir leurs structures traditionnellement fermées, tout en maintenant une sécurité au moins égale à celle qui prévalait dans un milieu clos. Les institutions financières font face à ce paradoxe ouvert/fermé de manière imaginative, mais en ordre dispersé. Trop souvent, leurs réalisations ponctuelles sont méconnues. Grâce à cette étude, nous serons à même de dresser un état de la situation et de bénéficier d'un avantage stratégique sur nos concurrents.

Nous comptons sur votre participation !

Ali El-Azzouzi
Président

Annexe 02 QUESTIONNAIRE

IDENTIFICATION DE L'INSTITUTION FINANCIERE

Q.01

Répondant		Organisme bancaire	
Responsable	.....	Institution	.....
Téléphone	.....	Ville	.....
Courriel	.....	Pays	.....

Confidentialité. Les réponses aux questions suivantes seront traitées de façon confidentielle. Elles n'apparaîtront pas dans la base de données et seront utilisées sous forme agrégée à des fins uniquement statistiques. Elles ne sont ni rétrocédées à des tiers ni utilisées à d'autres fins que celle requises à l'analyse des résultats de cette enquête.

CADRE ORGANISATIONNEL

Q.02

Qui est responsable de la cybersécurité dans l'institution financière ?

Responsable de la sécurité des systèmes d'information (RSSI) ..... ☐
Directeur des systèmes d'information (DSI) ..... ☐
Autre ..... ☐

Si vous avez répondu « Autre », veuillez préciser la fonction, SVP :
.....

Q.03

Quel est le supérieur hiérarchique immédiat du responsable de la sécurité ?
.....

Q.04

Combien d'employés sont affectés à la cybersécurité dans l'institution financière :

Nombre d'employés à plein temps ___
Nombre d'employés à temps partiel ___

Q.05

Les systèmes de cybersécurité de l'institution financière.....

..... sont gérés entièrement à l'interne ..... ☐
..... font appel à des consultants externes ..... ☐
..... sont gérés en partie chez un ou des sous-traitants (prestataire) ..... ☐
..... sont gérés entièrement chez un ou des sous-traitants (prestataire) ..... ☐

Si vous avez répondu que l'institution faisait « appel à des consultants externes», veuillez préciser le nombre d'équivalents temps plein (ETP) par an :
.....

Si vous avez répondu « en partie) ou « entièrement chez un ou des sous-traitants », veuillez préciser le nombre des sous-traitants, quelles tâches sont sous-traitées et enfin quel pourcentage est sous-traité :
.....
.....
.....

À votre connaissance, l'institution financière éprouve-t-elle des difficultés à recruter des employés spécialisés en cybersécurité ?

Oui ☐ Non ☐ NSP ☐

Annexe 02 QUESTIONNAIRE

Q.06

[Pour ceux qui ont répondu OUI à la question précédente]

Quelles sont les principales difficultés rencontrées ?

Manque de main d'œuvre qualifiée ..... ☐
Les salaires exigés sont trop élevés ..... ☐
La formation universitaire des candidats n'est pas adaptée aux besoins ..... ☐
Autre ..... ☐

Si vous avez répondu « Autre », veuillez préciser la difficulté, SVP :

.....

Q.07

Dans l'institution financière considérée, en matière de cybersécurité, existe-t-il…

… un programme de formation à l'externe (université, école spécialisée, etc) ..... ☐
… un programme de formation à l'interne (conférences, cours, etc) ..... ☐
… un ou des programmes de sensibilisation* ..... ☐

Pouvez-vous définir en quelques mots en quoi consiste ce ou ces programmes de formation et/ou sensibilisation, SVP :

.....

.....

.....

** Il peut s'agir par exemple, de messages sur l'intranet, courriels personnalisés, bulletins en ligne, écrans de veille des ordinateurs, affiches, ou de capsules vidéo.*

Q.08

L'institution considérée a-t-elle contracté une assurance pour couvrir le risque en matière de cybersécurité ?

Oui ☐ Non ☐ NSP ☐

Si vous avez répondu « Non », veuillez préciser pourquoi :

(par exemple : pas d'assurance disponible, prix trop élevé, etc.) :

.....

CADRE SECURITAIRE

Q.09

L'Institution financière dispose-t-elle d'un programme écrit de cybersécurité (mesures à prendre pour prévenir et remédier aux incidents relatifs à la sécurité de l'information) ?

Oui ☐ Non ☐

Si la réponse est « Non », savez-vous quelles sont les raisons de cette omission :

.....

Q.10

Ce programme comprend-il : *[Plusieurs réponses possibles.]*

Un audit complet des systèmes d'information ..... ☐
Un test d'intrusion des systèmes d'information ..... ☐
Une analyse de risque des systèmes d'information ..... ☐
L'obligation d'inclure une clause de cybersécurité dans les accords de sous-traitance
..... ☐
Un plan de relève en cas d'incident ..... ☐

Q.11

L'institution financière effectue-t-elle de la surveillance permanentes des évènements de sécurité ?

Oui (dans le cadre d'un SOC interne) ..... ☐
Oui (dans le cadre d'un SOC externe) ..... ☐
Non ..... ☐

Si la réponse est « Oui dans le cadre d'un SOC interne », veuillez décrire le SOC, son fonctionnement, le nombre de personnes qui y est affecté, leurs qualifications etc.

.....

Si la réponse est « NON », savez-vous pourquoi ?

.....

Q.12

L'institution financière a-t-elle déjà fait l'objet d'une cyberattaque (incident ayant occasionné de dommages) ?

Oui ☐ Non ☐ NSP ☐

Si « Oui », veuillez préciser à combien de reprises :

.....

Annexe 02 QUESTIONNAIRE

Q.13

[Pour ceux qui ont répondu OUI à la question précédente.]

Pouvez-vous définir de quel type de cyberattaques il s'est agi

Infection par hameçonnage (phishing) ☐
Infection par faux-semblant (pretexting) ☐
Infection par branchement d'un poste de travail étranger ☐
Carding et skimming ou fraude sur les cartes bancaires ☐
DDoS avec demande de rançon ☐
Autre ☐

Si vous avez répondu « Autre », veuillez expliquer la nature de l'incident :

.....

Si l'institution financière a subi plusieurs attaques de nature différentes, veuillez expliquer ci-dessous la nature des incidents 2, 3 etc.

Incident 2 : .....
Incident 3 : .....
Incident 4 : .....
Incident n : .....

Q.14

[Pour ceux qui ont répondu aux deux questions précédentes.]

Comment l'institution financière a-t-elle découvert l'incident

[Plusieurs réponses possibles.]

Par un audit de cybersécurité ☐
Par un employé de la cybersécurité de la banque ☐
Par un employé des services informatique de la banque ☐
Par un employé d'un service non-informatique ☐
Par un client de la banque ☐
Autre ☐

Si vous avez répondu « Autre », veuillez préciser, SVP :

.....

Si l'institution financière a subi plusieurs attaques de nature différentes, veuillez expliquer ci-dessous les circonstances de la découverte des incidents 2, 3 etc.

Incident 2 : .....
Incident 3 : .....
Incident 4 : .....
Incident n : .....

Q.15

[Pour ceux qui ont répondu aux trois questions précédentes.]

Veuillez estimer le temps qui s'est écoulé entre la date probable de l'infection initiale et celle de la découverte de l'incident ?

Moins d'une semaine ..... ☐
Moins d'un mois ..... ☐
Plus d'un mois ..... ☐

Si vous avez répondu « Plus d'un mois », veuillez préciser le nombre de mois (approximativement) :

.....

Si l'institution financière a subi plusieurs attaques, veuillez indiquer le temps de latence avant la découverte des incidents 2, 3 etc.

Incident 2 : .....
Incident 3 : .....
Incident 4 : .....
Incident n : .....

Q.16

[Pour ceux qui ont répondu aux quatre questions précédentes.]

Comment l'institution financière a-t-elle réagi à la cyberattaque ?

[Plusieurs réponses possibles.]

Par des moyens techniques et organisationnels internes ..... ☐
En faisant appel à des experts externes ..... ☐
En contactant l'assurance spécialisée en cybersécurité ..... ☐
En portant plainte aux forces de police ..... ☐
En contactant l'organisme national spécialisé en cybersécurité ..... ☐
Autre ..... ☐

Si vous avez répondu « Autre », veuillez préciser, SVP :

.....

Annexe 02 QUESTIONNAIRE

Q.17

Quel a été l'impact de l'incident :

Perte d'argent ..... ☐
Suspension des services en ligne ..... ☐
Fermeture des guichets automatiques ..... ☐
Fermeture d'une succursale ..... ☐
Fermeture de la banque entière ..... ☐

Veuillez préciser l'ampleur des dommages, la nature des activités interrompues, le nombre de succursales fermes, le temps de la fermeture, etc. Tous détails permettant de qualifier l'incident est bienvenu :

.....

Si l'institution financière a subi plusieurs attaques, veuillez indiquer la nature et l'ampleur des dommages des incidents 2, 3 etc.

Incident 2 : .....
Incident 3 : .....
Incident 4 : .....
Incident n : .....

Q.18

À combien évaluez-vous le coût des dommages (approximativement) :

[Veuillez tenir compte du temps des employés, du recrutement de consultants en informatique, des applications de cybersécurité et du matériel connexe, du remboursement des clients, des amendes imposées par les autorités, etc.]

.....

CADRE LEGAL ET REGLEMENTAIRE

Q.19

L'institution financière considérée a-t-elle adopté une ou plusieurs des normes de sécurité :

Accords de Bâle 2 ou Bâle 3 ..... ☐
ISO 27001 (management de la sécurité des informations) ..... ☐
PCI DSS (Payment Card Industry Data Security Standard) ..... ☐
Autre ..... ☐

Si vous avez répondu « Autre », veuillez préciser la ou les normes, SVP :

.....

Q.20

L'institution financière vérifie-t-elle périodiquement sa conformité aux normes sectorielles et à la réglementation ?

Oui ☐ Non ☐

Si vous avez répondu « Oui », veuillez préciser de quelles normes et règles il s'agit :

.....

INVESTISSEMENTS EN CYBERSECURITE

Q.21

Quel est le montant approximatif que l'institution financière investit en cybersécurité sur une base annuelle (montant pour 2018) :

Moins de 100 000 € ..... ☐
Entre 100 000 et 500 000 € ..... ☐
Entre 500 000 et 1 000 000 € ..... ☐
Plus de 1 000 000 € ..... ☐

Si vous avez répondu « Plus de 1 000 000 € », veuillez préciser le montant approximatif, SVP :

.....

Q.22

Au cours de 2019, selon les informations que vous avez, prévoyez-vous que ce montant sera amené à…

..... augmenter ..... ☐
..... baisser ..... ☐
..... demeurer stable ..... ☐

Annexe 02 QUESTIONNAIRE

Q.23

D'une façon générale, estimez-vous que l'institution financière considérée est bien outillée en matière de cybersécurité ?

Oui ☐ Non ☐

Si vous avez répondu « Non », veuillez préciser ce qui devrait être fait, selon vous, pour améliorer la sécurité :

.....

INFORMATION GENERALE

Q.24

Quelle est la nature de l'Institution financière considérée :

Banque d'affaires ..... ☐
Crédit aux particuliers ..... ☐
Autres services financiers ..... ☐

Si vous avez répondu « Autres services financiers », veuillez préciser, SVP :

.....

Q.25

Combien d'employés travaillent dans l'institution financière ?

[Veuillez indiquer le nombre approximatif d'employés à temps plein.]

Dans le pays d'origine ....._____
À l'étranger (s'il y a lieu) ....._____

Si vous avez répondu « À l'étranger », veuillez préciser dans quel(s) pays :

.....

PRIERE DE RENVOYER LE QUESTIONNAIRE

Par courriel **aelazzouzi@dataprotect.ma**
Par télécopie **(+212) 522 218 396**

MERCI !

ANNEXE 03
BIBLIOGRAPHIE

TITRE	ORGANISME	Pays	Date	Pages
FinTechs in Sub-Saharan Africa	EY	Grande-Bretagne	2019	21
The impact of mobile money on monetary and financial stability in Sub-Saharan Africa	GSMA	Grande-Bretagne	2019	28
Fintech in Sub-Saharan African Countries	Fonds monétaire international (FMI)	USA	2019	51
Cybersécurité au Sénégal	SAYTU	Sénégal	2019	61
Digital Access: The Future of Financial Inclusion in Africa	International Finance Corporation (IFC)	Afrique du Sud	2018	89
Roaring to life: Growth and innovation in African retail banking	McKinsey & Company	Afrique du Sud	2018	54
Africa Payments: Insights into African transaction flows	SWIFT	Afrique du Sud	2018	38
Digital Access: The future of financial inclusion in Africa	Internal Finance Corporation (IFC)	Afrique du Sud	2018	
Base de données Global Findex 2017	Banque mondiale	USA	2018	18
Kingdom of Morocco Cyber Readiness at a Glance	Potomac Institute for Policy Studies	USA	2018	30
Global Software Survey 2018	BSA (Software Alliance)	USA	2018	20
Cyber threats on African subjects	IDC Herzliya	Israël	2018	37
Le secteur bancaire en Afrique : De l'inclusion financière à la stabilité financière	Banque européenne d'investissement	Luxembourg	2018	253
État de la menace liée au numérique en 2018	Ministère de l'Intérieur	France	2018	112
Sacco Cybersecurity Report 2018	Serianu	Kenya	2018	22
Building Confidence – Solving Banking's Cybersecurity Conundrum	Accenture Security	Irlande	2017	11
Africa Cyber Security Report: Demystifying Africa's Cyber Security Poverty Line	Serianu	Kenya	2017	86
Disrupting Africa: Riding the wave of the digital revolution	PwC	Grande-Bretagne	2016	53
Cyber Crime & Cyber Security: Trends in Africa	Symantec	USA	2016	95
Relever les défis de la cybersécurité en Afrique	Nations Unies	Éthiopie	2014	6


DATAPROTECT
Security is our commitment

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

DATAPROTECT
Security is our commitment

LA FRAUDE BANCAIRE EN AFRIQUE SUBSAHARIENNE

A propos de DATAPROTECT :

DATAPROTECT est une entreprise spécialisée en sécurité de l'information. Fondée en mai 2009 par Ali EL AZZOUZI, un expert en sécurité de l'information ayant mené plusieurs projets de conseil et d'intégration de solutions de sécurité au Maroc et à l'étranger, DATAPROTECT appuie son offre sur une vision unifiée de la sécurité de l'information. Dotée d'un réservoir de compétences pointues en sécurité lui permettant d'assurer une expertise unique sur le marché local et régional.

Depuis sa création, DATAPROTECT ne cesse d'évoluer pour délivrer ses prestations d'excellence à travers une équipe d'experts pluridisciplinaires dotée d'un sens unique de l'intimité client. Aussi, son statut de première entité accréditée PCI QSA au Maroc par le consortium Payment Card Industry Security Standards Council pour les certifications PCI DSS et PA DSS, fait d'elle un cas d'école unique dans la région.

Avec plus de 500 clients en Afrique, Europe et au Moyen-Orient, et en Asie-Pacifique DATAPROTECT est aujourd'hui capable de délivrer ses services en toute agilité, pour des multinationales comme pour des entreprises locales, avec à la clé une réputation établie de pionnier sur la thématique de la sécurité de l'Information.

www.dataprotect.ma

A propos de Sciencetech :

La recherche et l'analyse ont été effectuées par la firme canadienne Sciencetech Communication pour le compte de DATAPROTECT. Sciencetech est spécialisée dans les études de marché et les profils de l'industrie.

www.sciencetech.com