Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne

Résultats de l'enquête PwC
Mars 2021

pwc

Executive Summary

La cybersécurité : un facteur indispensable pour la réussite de toute transformation numérique durable des organisations...

La cybersécurité est un facteur indispensable pour une transformation numérique durable et efficace car c'est sur elle que repose le capital confiance-numérique de toute organisation.

Nous assistons depuis environ deux décennies à une transformation numérique des entreprises. Ce phénomène, amplifié par la pandémie de la Covid-19, n'a pas laissé de côté les entreprises évoluant en Afrique francophone subsaharienne.

De nombreuses entreprises de divers secteurs d'activités, incluant les banques, les établissements de santé, les assurances, les fournisseurs des services de communication... adoptent massivement les outils numériques pour booster leur compétitivité et améliorer leur productivité. Cette transformation numérique est également encouragée par les gouvernements à l'exemple de certains pays tels que le Cameroun, le Bénin et la Côte d'Ivoire qui ont adopté, chacun, un plan stratégique national pour le numérique.

Une révolution numérique qui expose les organisations aux risque de cybersécurité...

Cependant, cette révolution numérique expose également l'Afrique francophone subsaharienne à la cybercriminalité, dans un contexte où les entreprises et même les populations ne prennent pas toujours la pleine mesure des risques cyber qui accompagnent la transformation numérique.

D'où la nécessité de la présente étude PwC sur les enjeux et les défis de la cybersécurité pour les organisations en AFSS

Il est dès lors important de mesurer les enjeux relatifs à la cybersécurité afin de définir et prioriser les réponses à adopter pour mettre en place une stratégie de cybersécurité capable de soutenir la productivité et l'agilité de l'entreprise.

C'est dans cette optique que PwC a effectué une enquête portant sur les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne. Il s'agit d'une enquête réalisée auprès de 281 acteurs professionnels, de divers secteurs d'activité, présents dans les pays suivants : Cameroun, Congo, Côte d'Ivoire, Gabon, Guinée, RDC, Sénégal et Madagascar.

Nous avons interrogé les professionnels des entreprises sur leur compréhension et définition des enjeux cyber, des risques cyber ainsi que sur les problématiques relatives à la stratégie globale de cybersécurité au sein de leurs entreprises.

Il ressort de cette étude des messages clés et des actions à mener pour améliorer la posture de l'Afrique francophone subsaharienne en matière de cybersécurité.

Les principaux enseignements

1

L’importance de la cybersécurité commence à être reconnue, mais...

La plupart des entreprises interrogées reconnaissent que la cybersécurité est un sujet prioritaire. Cependant, elles reconnaissent également que la réponse apportée aux risques de cybersécurité est souvent en déphasage avec la stratégie globale de l’entreprise, ce qui ne permet pas de gérer le risque de manière holistique. Il en résulte une stratégie cyber inadaptée, inefficace et non productive.

2

La responsabilité en matière de cybersécurité est encore attribuée au personnel technique

Nous remarquons un intérêt mitigé du leadership à la réponse aux risques cyber.
En effet, plus de 70% des répondants attribuent la responsabilité de sécurisation du cyberespace de l’entreprise au personnel technique. L’enjeu stratégique de la cybersécurité au sein des entreprises semble n'être pas perçu à sa juste mesure.
Ceci dénote un réel besoin de sensibilisation et de responsabilisation du Conseil d’Administration et de la Direction Générale.

3

Une stratégie de gestion des risques pas toujours adaptée au contexte de l’entreprise

La stratégie de cybersécurité devrait être fonction d’une identification méthodique des risques cyber et de leur intégration à la cartographie globale des risques de l’entreprise. La plupart des entreprises interrogées ne disposent pas de programmes holistiques de gestion des menaces et des risques de cybersécurité. Il s’en suit une réponse aux risques non adaptée et souvent inutilement coûteuse.
Ceci relève d’une mauvaise politique de gestion des risques cyber.

4

La gestion des incidents de cybersécurité n’est pas encore maîtrisée

La réponse aux incidents de cybersécurité est un point clé de la cyber résilience. 42% des entreprises interrogées avouent n’avoir mis en place aucun processus de gestion des incidents de cybersécurité. Avec la recrudescence des cyberattaques, ceci dénote la nécessité d’une transition du modèle de continuité des activités vers un modèle de cyber résilience permettant de limiter la possibilité d’une cyber attaque ou de réduire son impact sur les plans financier, réputationnel et réglementaire.

5

Le facteur humain est identifié comme une lacune importante liée aux cyber risques

Il s’agit d’un problème connu qui s’est vu confirmé par cette enquête. En effet, les problématiques du manque de compétences d’une part et de la faible sensibilisation aux types de compétences nécessaires d’autre part, constituent un risque cyber important. Il en ressort la nécessité de développer des compétences diverses en interne pour la prise en charge du risque cyber au sein de toutes les fonctions de l’entreprise.
La cybersécurité reste, plus que jamais, la responsabilité de tous !

Les actions à mener par les entreprises en Afrique francophone subsaharienne

1

L'implication effective de la Direction Générale et du Conseil d'Administration

Une réponse efficace aux risques de cybersécurité commence par une prise de conscience de la part des membres du Conseil d'Administration et du Top Management de l'entreprise. En effet, ceux-ci doivent reconnaître les enjeux de la la cybersécurité et en assurer la prise en compte dans toutes leurs décisions métier. Ceci se fera à travers des sensibilisations, des formations et un accompagnement de ces acteurs clés vers la prise effective de conscience.

2

La gestion effective des risques et cyber menaces

La crise Covid-19 a modifié le paysage des risques cyber. La maîtrise des risques et menaces cyber passe par une cartographie de ces derniers à travers leur identification et leur évaluation. L'identification méthodique des risques cyber de l'entreprise permettra au leadership d'améliorer la prise de décision ainsi que la planification et la priorisation d'un programme pluriannuel de réponses aux risques. Ceci pourra donner lieu à une allocation optimale du budget de cybersécurité en accord avec les besoins réels de l'entreprise.

3

La mise en place d'une stratégie cyber efficace et optimisée

La cartographie des risques cyber doit servir de base à la mise en place d'un plan stratégique de réponse aux risques et d'une feuille de route tenant compte des objectifs globaux et des exigences de l'entreprise. Doté d'une feuille de route, le Top Management pourra ainsi avoir une vision claire de la posture de sécurité actuelle et future de l'entreprise. La mise en place d'un tableau de suivi des programmes permettra d'accroître l'engagement du Leadership à la surveillance des risques cyber.

4

Un programme efficace de cyber résilience

La cyber résilience consiste pour une entreprise à acquérir la capacité de reprendre les activités normales et de minimiser les dommages subis suite à une cyber attaque.
Ceci est une nécessité dans la mise en oeuvre d'une stratégie de cybersécurité et regroupe toutes les fonctions de l'entreprise. L'intégration des contrôles cyber dans le contexte de la transformation digitale devient donc un élément clé et permet également à l'entreprise d'être en conformité avec les réglementations nationales et les standards internationaux.

5

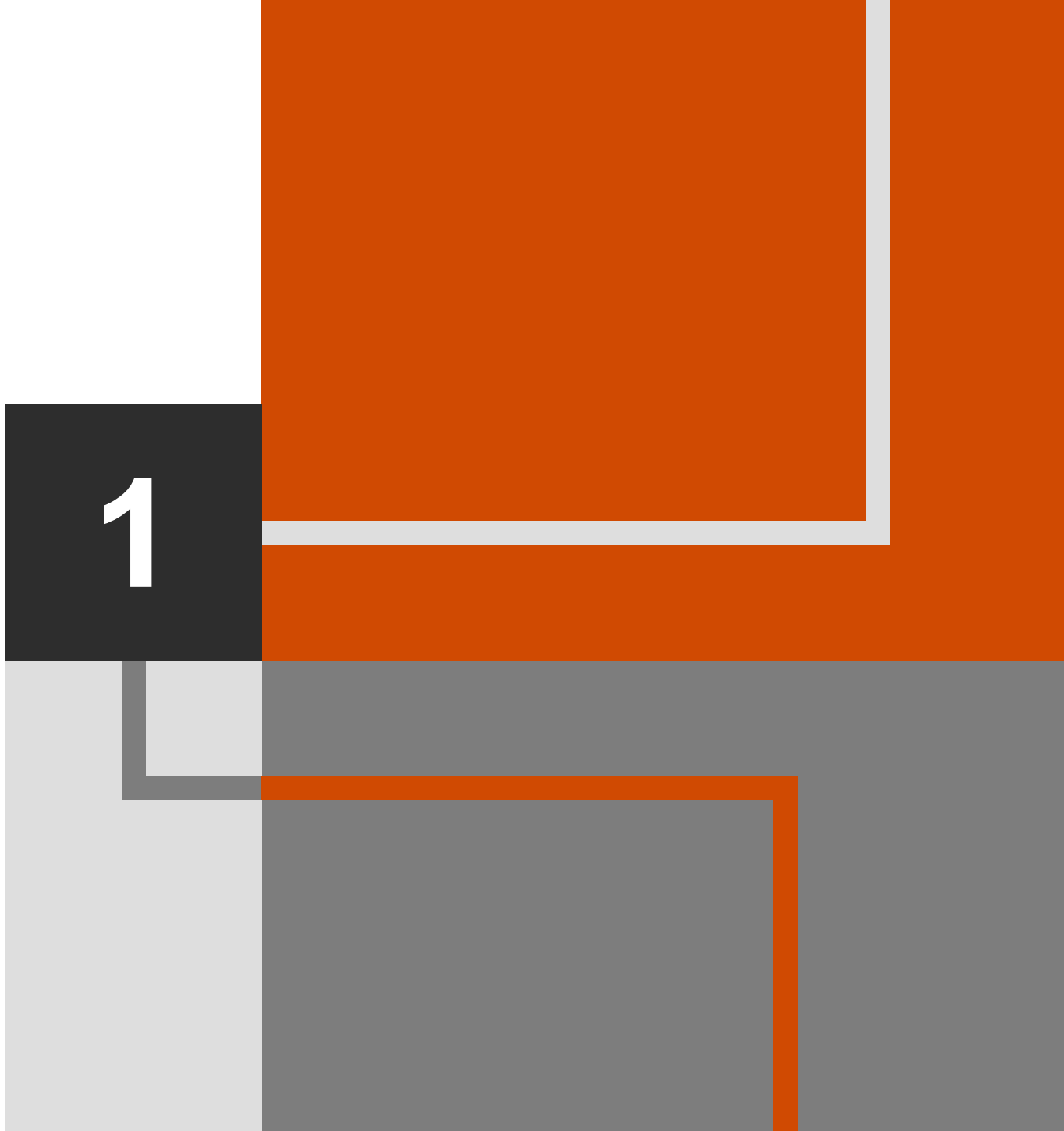
La prise en compte du facteur humain comme élément clé du dispositif de cybersécurité

Le défi majeur en cybersécurité consiste à minimiser l'impact du comportement des utilisateurs sur les dispositifs de protection mis en œuvre. Ceci se fait par une amélioration de la culture d'entreprise, soutenue par une infrastructure humaine et technologique. De plus, le profil des professionnels de cybersécurité et les compétences attendues devraient évoluer en raison de la diversité des risques et des besoins importants d'interactions avec le Comité de Direction et le Conseil d'Administration.

Sommaire

Introduction

L’Afrique francophone subsaharienne face à la cybercriminalité



Importance de la cybersécurité en AFSS

- La cybercriminalité représente la « plus grande menace pour chaque profession, chaque secteur, chaque entreprise du monde », déclarait Ginni Rometty, CEO d'IBM en 2015 à l'occasion d'un Forum économique mondial (WEF). Une prédiction qui s'est confirmée, au regard du nombre sans cesse croissant des cyberattaques déclarées en Afrique.

- Cette situation est favorisée par l'essor de la technologie et le boom numérique, mais également par la faiblesse d'une stratégie globale incluant les infrastructures de sécurité adéquates, le développement d'un personnel qualifié et la mise en place d'un cadre légal et réglementaire. S'il est vrai que nous avons vu émerger des initiatives pour adresser la plupart des problématiques suscitées, il est important de reconnaître malheureusement que les actions entreprises restent isolées, à l'heure où des actions coordonnées entre tous les acteurs de la société, aideraient à une meilleure prise en charge des menaces cyber.

- PwC, au travers de cette enquête, se propose de faire un état des lieux des enjeux et défis de la cybersécurité en Afrique francophone subsaharienne.

Quelques chiffres sur la cybersécurité en Afrique

Selon Africa Cyber Security Market, le marché de la cybersécurité en Afrique est estimé 2,32 milliards de dollars US en 2020 contre 1,33 milliards de dollars US en 2017.

"A l'échelle du Continent, le coût des cybercrimes est estimé à 1,37 milliard d'euros pour une population globale connectée à 23%."

Source www.afrique.latribune.fr (Par Mounir El Figuigui)

"Chez Visa Afrique de l'ouest et Afrique centrale, chaque attaque coûte en moyenne 1,2 million de dollars US, notamment en perte de revenus."

Source www.afrique.latribune.fr (Par Mounir El Figuigui)

2020
Le Sénégal victime d'une attaque cybercriminelle venue du Cameroun : 572 cartes de clients de la BHS dupliquées pour des retraits frauduleux de 20,776 millions de FCFA à travers 117 opérations.

Source: Africa Cybersecurity Magazine

2015
+18 Milliards de FCFA –

Opérateurs télécoms au Cameroun
Détournement du trafic téléphonique via les SIMBOX.

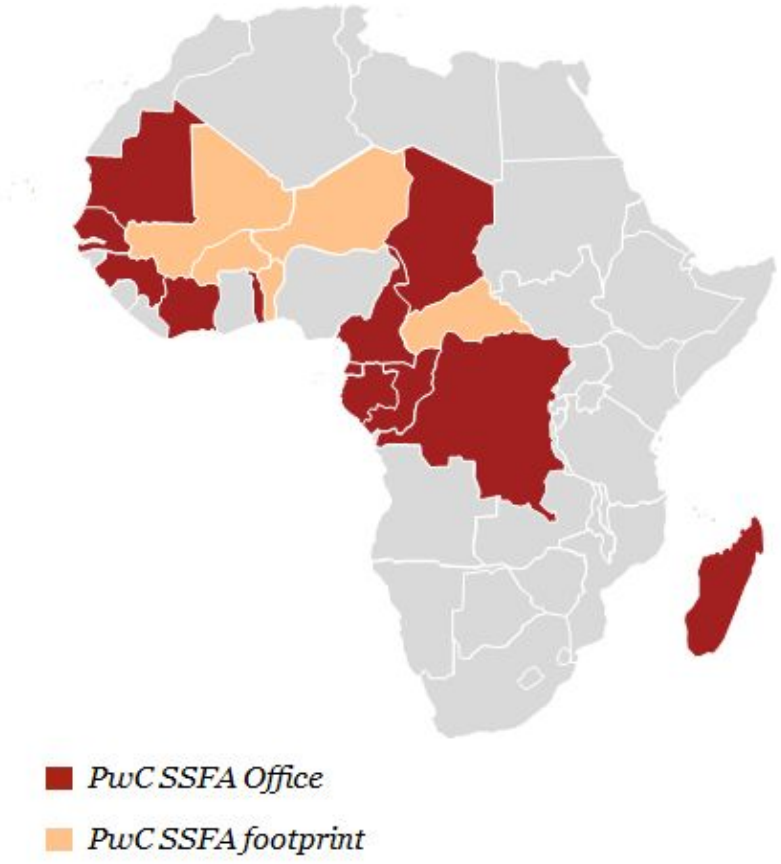
Source:Source: CRTV Web, Agence Ecofin

2020
Vol des données chez Bolloré Transport & Logistics République Démocratique du Congo (RDC) à travers le ransomware Net Walker avec menace de publication d'informations confidentielles.

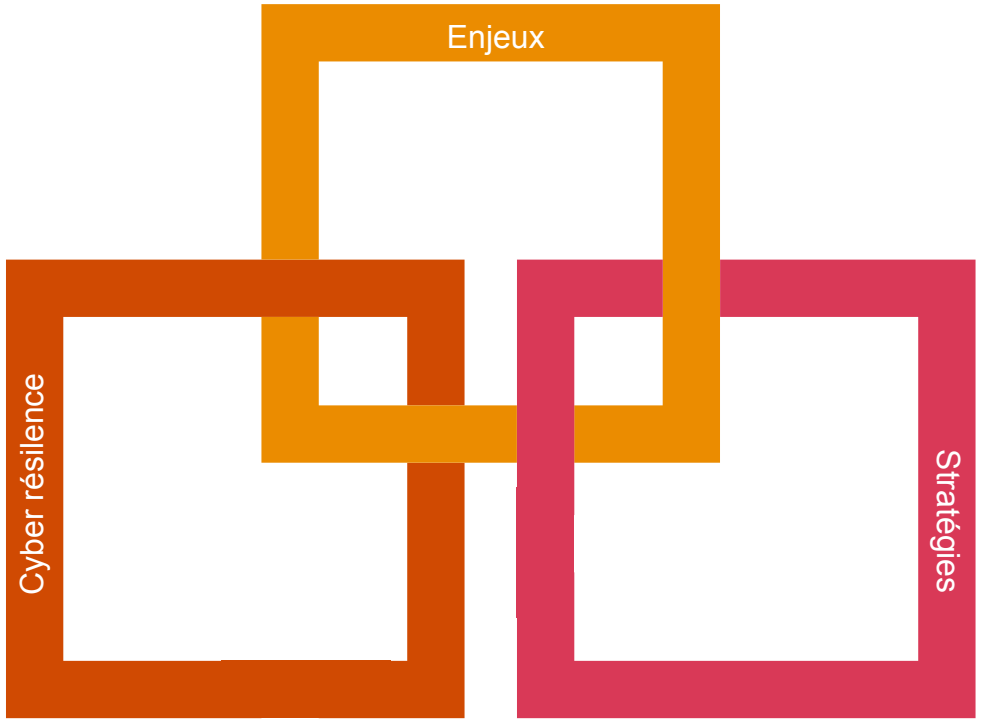
Source: lemondeinformatique.fr

2019
Accès frauduleux au Système de la BCEAO (Côte D'Ivoire) pour émission des transferts frauduleux d'argent pour un total de FCFA 237 Millions.

Source: CIO Mag, le quotidien Sénégalais Libération.



Dans ce contexte, nous avons initié une enquête sur la cybersécurité en AFSS autour de 03 sujets clés…



Enjeux
Les enjeux de la cybersécurité en Afrique francophone subsaharienne

Stratégies
Les stratégies de gestion des risques cyber implémentées en Afrique francophone subsaharienne

Cyber résilience
La cyber résilience en Afrique francophone subsaharienne

2

Les enjeux

L’importance de la cybersécurité ne fait pas encore l’unanimité

“

Les pirates informatiques ou les cyber-mercenaires n’ont pas nécessairement des motivations monétaires comme la cybercriminalité traditionnelle. Ils volent plutôt des données privées pour les monétiser d’une autre manière – généralement dans le but de fournir des conseils ou des informations, sur la base des données, afin de partager la valeur d’un avantage concurrentiel.

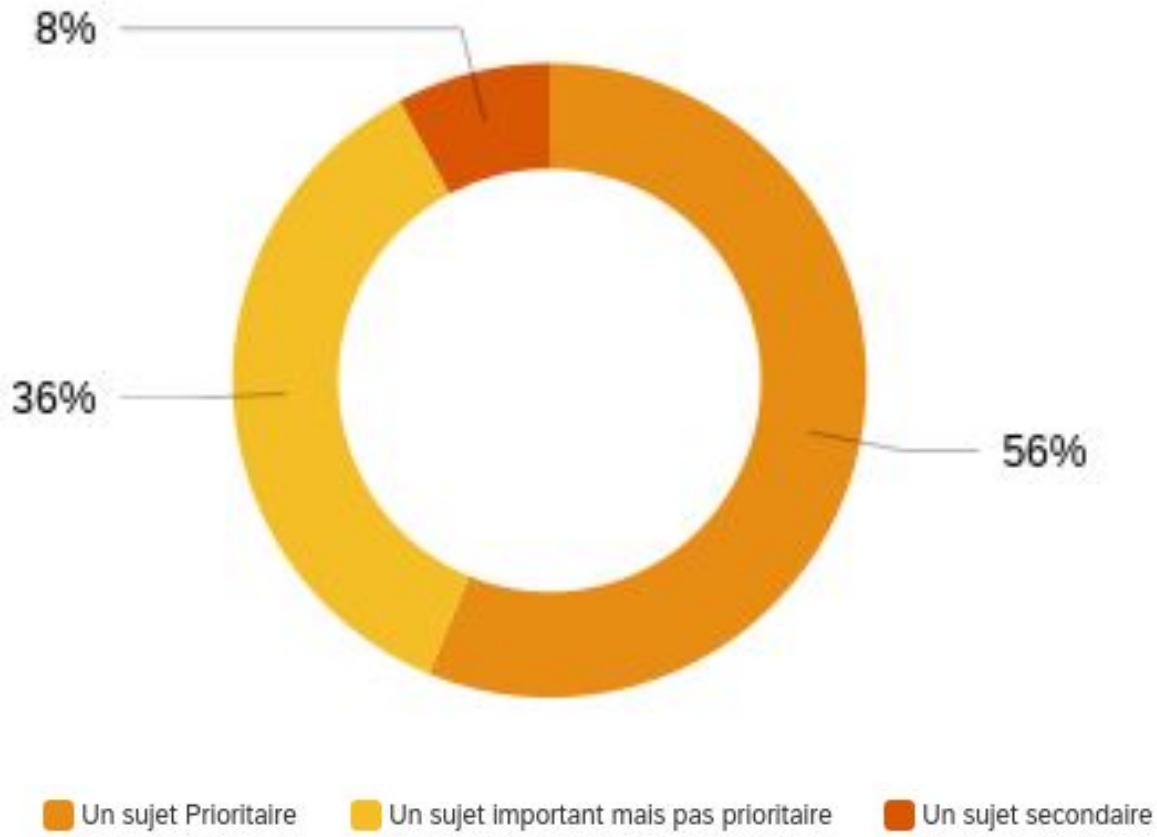
Kaspersky

La cybersécurité: un sujet prioritaire pour les entreprises

56%

La plupart des entreprises reconnaissent que la cybersécurité est un sujet prioritaire ayant un impact considérable sur la politique commerciale et l'image de marque de l'entreprise. Toutefois, un pourcentage important d'entreprises considère encore qu'il s'agit d'un sujet important mais pas prioritaire.

La cybersécurité au sein de votre entreprise est...



Des considérations différentes selon les secteurs d'activité

72%

Secteur financier

53%

Industrie, fabrication et automobile

65%

Technologie, médias et télécommunications

38%

Marché de consommation

57%

Énergie, services publics et ressources

29%

Gouvernement et secteur public

La majorité des entreprises du secteur financier reconnaît que la cybersécurité est d'une importance capitale. Toutefois, certains secteurs d'activité notamment le secteur public, le gouvernement et le marché de consommation semblent moins concernés par la cybersécurité. Ceci dénote d'un manque de maturité dans ces secteurs d'activité et pose le problème de la gestion des risques cyber émanant des tiers, compte tenu de l'interconnexion qui pourrait exister entre les différents secteurs d'activité. D'autre part, le faible niveau de maturité des uns peut mettre tout l'écosystème à risque.

La cybersécurité : une importance capitale pour les entreprises en AFSS

Evaluation de l'importance de la cybersécurité

Sur échelle de 0 à 5, l'importance de la cybersécurité est évaluée à 3.6 en moyenne par les répondants en Afrique francophone subsaharienne. Ce qui fait de la cybersécurité un sujet d'importance capitale en AFSS.

Il est à noter que les répondants du secteur financier présentent la moyenne la plus élevée (4,05) tandis que ceux du Marché de consommation totalisent la moyenne la plus faible (2,88).

Comment évaluez vous l'importance de la cybersécurité au sein de votre entreprise (0 étant le risque le plus faible et 5 le risque le plus fort ?)

Note moyenne attribuée à l'importance de la cybersécurité au sein des entreprises en AFSS

Les Gouvernements et les institutions publiques ne sont pas toujours en avant garde…

29%

Seuls 29% des répondants des institutions publiques interrogés pensent que la cybersécurité est un sujet prioritaire pour leur institutions.

Vu que les Gouvernements de l'Afrique francophone subsaharienne semblent être lents à apprécier l'importance du risque de cybersécurité et à adopter et mettre en place les réponses appropriées y compris des plans stratégiques de cybersécurité, les institutions publiques de l'Afrique francophone subsaharienne sont elles dotées des outils et des moyens nécessaires pour relever les nouveaux défis que l'avenir leur réserve en matière de cybersécurité ?

L'utilisation des technologies de l'information et de la communication (TIC) est désormais incontournable dans nos pays. Les bienfaits qu'elles procurent constituent des supports et des facilitateurs de croissance pour les états de l'Afrique francophone subsaharienne ; les Gouvernements étant ultimement responsables de la croissance nationale. Toutefois, au vu des nombreuses cyberattaques répertoriées sur le cyberespace africain, chacun de nos Gouvernements est interpellé. En effet, en 2018, une information selon laquelle tous les contenus des serveurs du siège de l'Union Africaine (UA) ont été systématiquement transmis à Shanghai a été relayée par de nombreux médias. De nombreux défacements de sites web publics ont également été reportés notamment en Côte d'ivoire, au Cameroun et au Sénégal. Ces cyberattaques témoignent de la progression des menaces cyber et du risque qu'elles représentent pour la sécurité des institutions publiques en Afrique francophone subsaharienne.

Le rôle des gouvernement et des institutions publiques face à la cybersécurité.

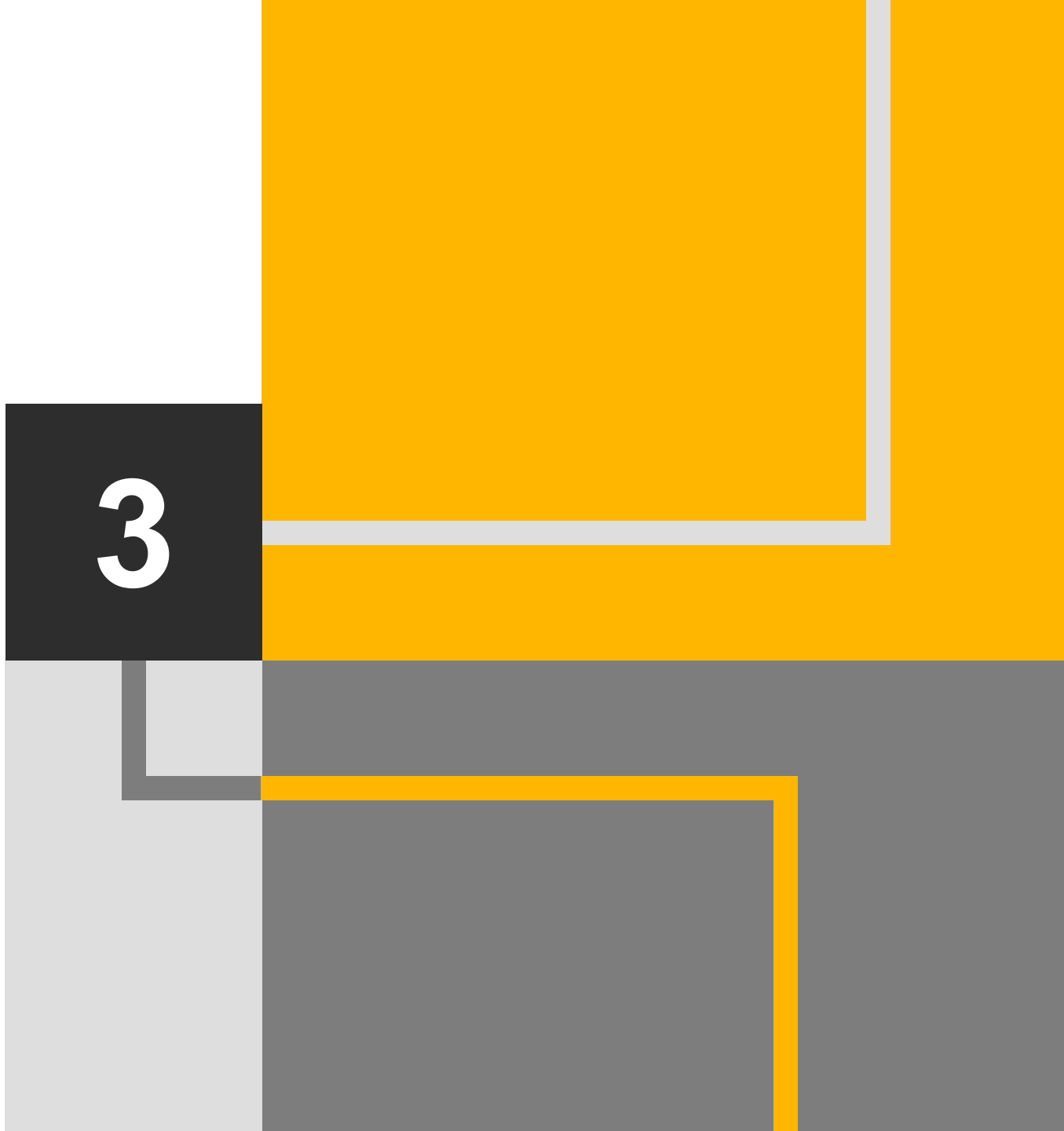
Face à la cybersécurité, les Gouvernements ont une double responsabilité : celle de se protéger en tant qu'Institution et celle de mettre en place un cadre nécessaire pour la protection des organisations, des personnes et des infrastructures publiques. Ceci passe, entre autres, par la mise en place d'une stratégie nationale, l'adoption des lois et réglementations, la création des organes de régulation, la mise sur pied de dispositifs de veille sécuritaire et de réponse aux incidents, l'identification des utilisateurs, les audits de conformité, la formation et la sensibilisation du capital humain, la coopération, etc.

La cybersécurité: une importance mitigée pour les gouvernements et institutions publiques en AFSS

Dans le rapport 2015 de l'UIT sur l'Indice de cybersécurité (GCI), seuls le Cameroun et la Côte d'Ivoire apparaissent dans le top 10 des états Africains présentant un engagement en matière de cybersécurité. Depuis lors, au sein des pays de l'Afrique francophone sub-saharienne, nous notons sur le plan législatif la mise en place des instruments de régulation de la cybersécurité. Mais beaucoup reste encore à faire…

Les stratégies

Les programmes de gestion des risques et des menaces cyber sont quasi absents



“

Une bonne stratégie de cybersécurité doit être alignée sur la stratégie d’entreprise pour soutenir la croissance par la gestion efficace des risques, des ressources et de la gouvernance et pour faire face aux menaces cyber

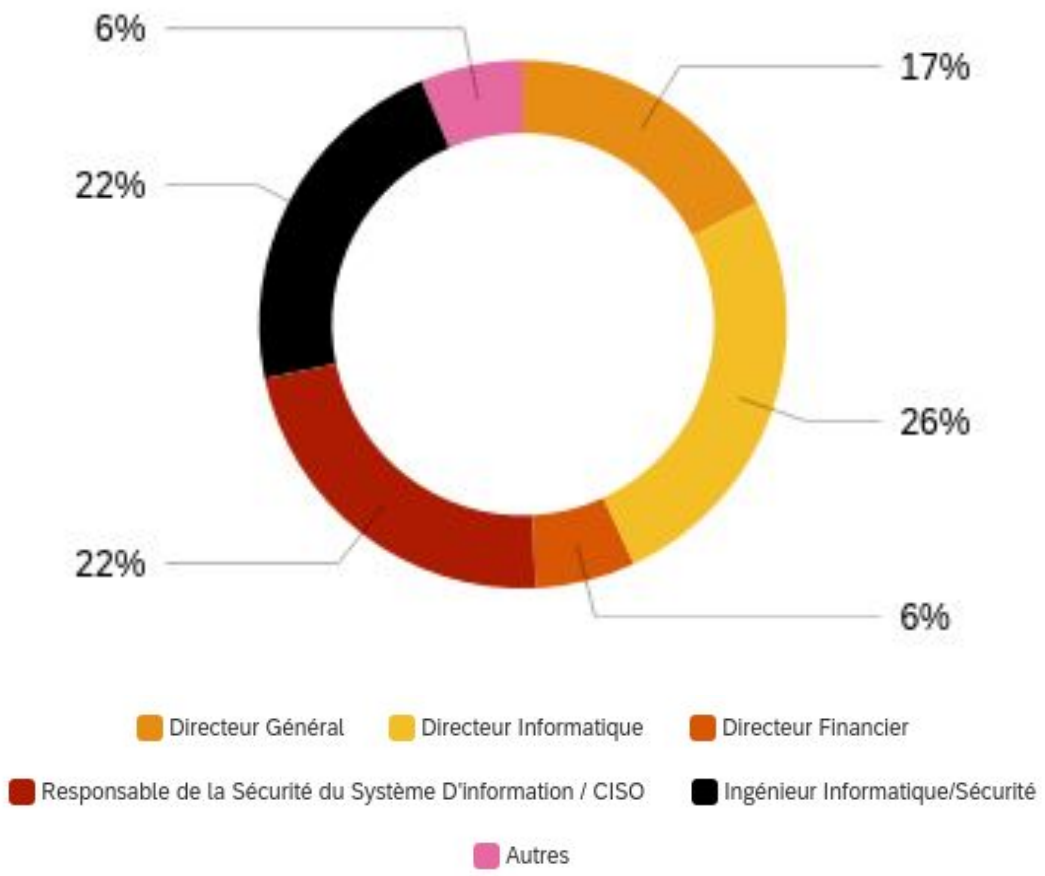
Lydie Ngo Nogol
Responsable de la Sécurité des Systèmes d’Information,
PwC Afrique Francophone Subsaharienne

La responsabilité en matière de cybersécurité : une perception à changer

Quels sont les rôles au sein de votre organisation qui sont principalement responsables de la mise en place de la stratégie de cybersécurité ?

70%

70% des répondants estiment que la cybersécurité est de la responsabilité du personnel technique : Directeur informatique (26%), Ingénieur informatique (22%), RSSI(22%).
La responsabilité de la mise en place de la stratégie de cybersécurité n'est pas attribuée à la Direction Générale. Ceci dénote un réel besoin de sensibilisation et de formation du Top Management des entreprises.



Une évaluation des risques peu fréquente et des remédiations non systématiques

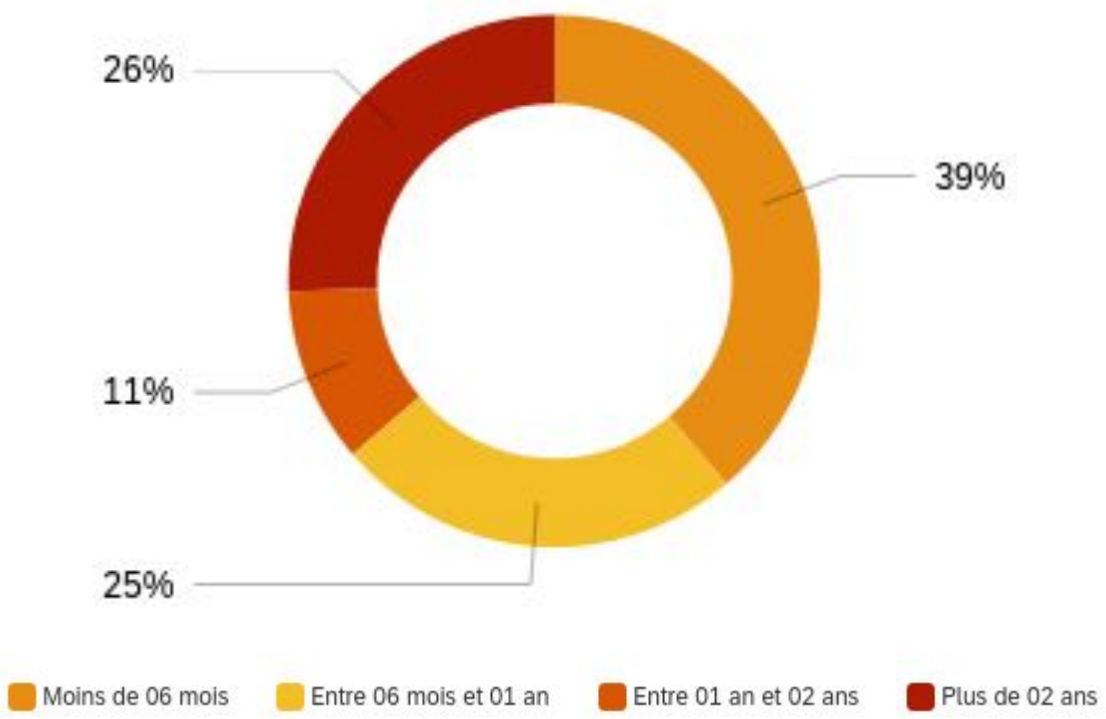
Cartographie des risques

Moins de 40% des répondants ont effectué une analyse des risques durant les 06 mois précédant l'enquête. 26% des entreprises n'ont pas effectué une analyse des risques depuis plus de deux ans parmi lesquelles 16% des entreprises du secteur financier interrogées.

Les actions nécessaires pour la correction des écarts constatés à la suite de l'analyse des risques ont été mises en place partiellement ou pas du tout dans 64% des entreprises interrogées.

Ce constat concerne tous les secteurs d'activité dont 65% pour le secteur financier.

A quand remonte la dernière fois que votre entreprise a élaboré / documenté une cartographie des risques liés à la cybersécurité ?



Les programmes de gestion des risques et des cyber menaces : une pratique peu répandue en AFSS

28%

35%

Gestion des cyber menaces

Seules 28% des entreprises interrogées déclarent avoir mis en oeuvre un programme complet de gestion des cyber-menaces (Threat Management Programme).

Il est à noter que 56% des répondants du secteur financier ont soit mis en oeuvre ce programme partiellement ou pas du tout. Il en est de même pour 75% des répondants appartenant aux gouvernements et secteurs publics et pour 71% des répondants du secteur Technologie, Media et Télécommunications.

Gestion des risques de cybersécurité émanant des tiers

Seuls 35% des répondants déclarent avoir mis en place un programme de gestion des risques de cybersécurité émanant des tiers (Supply chain, Support Technique, etc.).

Parmi les 65% qui n'en disposent pas, 31% ont déclaré avoir prévu de s'en doter à moyen terme tandis que 19% ne pensent pas le faire (dont 9% du secteur financier et 33% du secteur gouvernement et secteur public).

“

La sécurité ne doit pas être une affaire de spécialiste, mais un nouveau paradigme commun. Cela passe avant tout par la sensibilisation des populations.

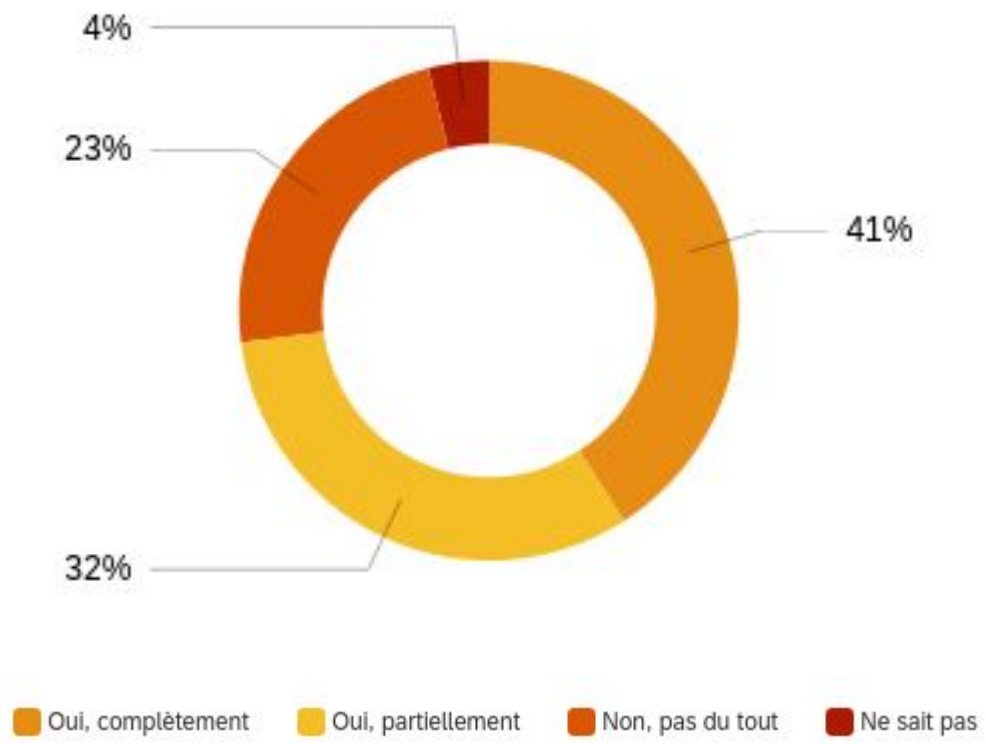
Lacina Koné
Directeur Général de Smart Africa

La sensibilisation à la cybersécurité : une pratique pas encore maîtrisée

55%

55% des répondants ne disposent pas d'un programme de sensibilisation à la cybersécurité ou estiment que le programme de sensibilisation à la cybersécurité existant ne répond pas complètement aux besoins de l'entreprise en matière de cybersécurité.

Votre entreprise a-t-elle mis en place un programme de formation et de sensibilisation à la sécurité de l'information pour vos employés et tiers



La cyber résilience

4

La gestion des incidents de cybersécurité n’est pas encore maîtrisée

“

Pour faire face aux risques cyber dans un contexte de COVID 19 et de généralisation du télétravail, les entreprises doivent se doter d'une feuille de route et disposer d'un budget leur permettant de couvrir les aspects liés au capital humain, aux processus et à la technologie y compris la conformité

Valery Kapnang
Associé PwC en charge de la cybersécurité

A propos des solutions technologiques

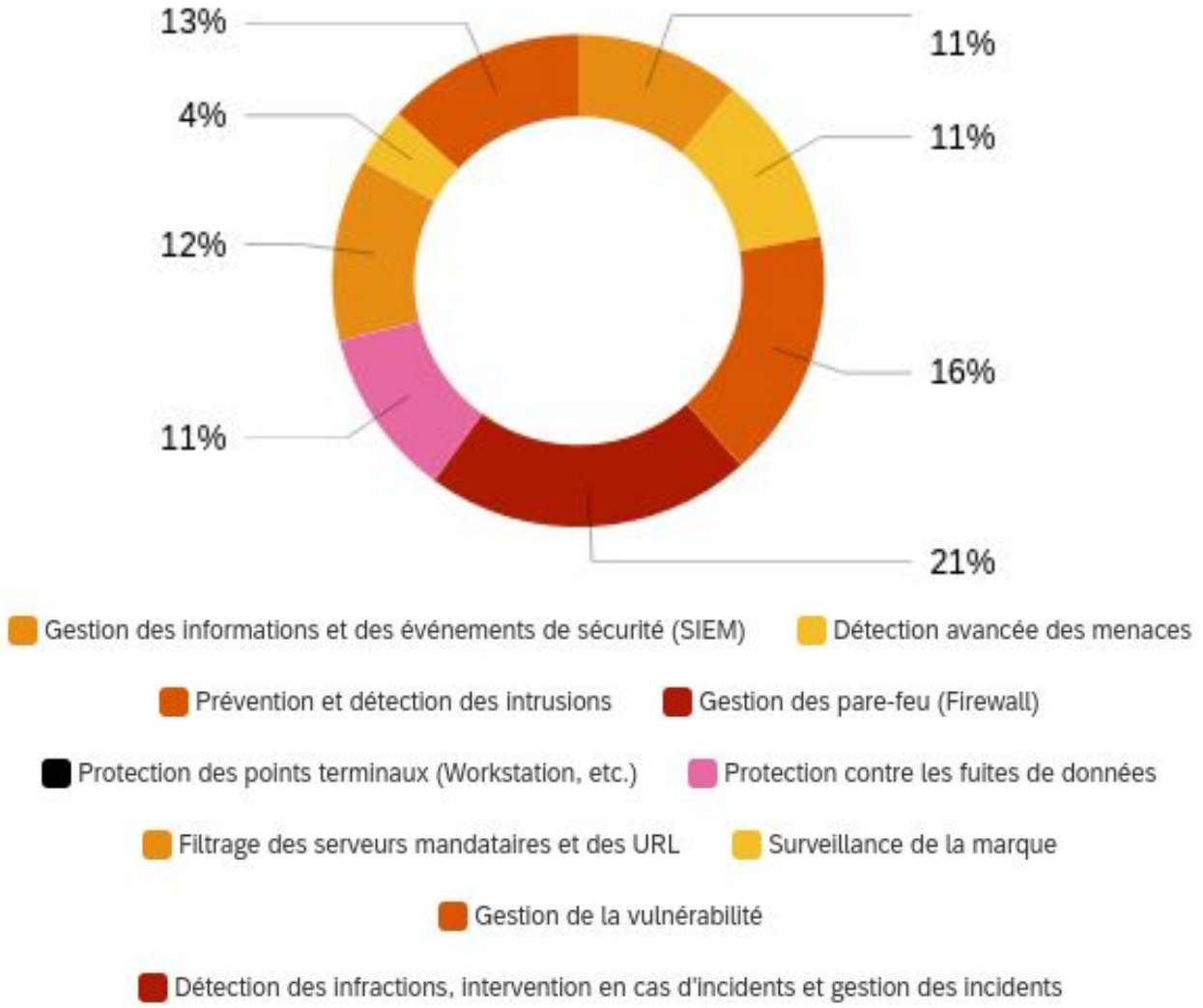
21%

21% des solutions de sécurité mises en place concernent les pare-feux

Les solutions de sécurité les plus utilisées sont les pare-feux (21%). Les autres solutions de sécurité mises en place comprennent les systèmes de prévention et détection des intrusions (16%), la gestion des vulnérabilités (13%), le filtrage des serveurs mandataires et des URLs (12%), la protection contre les fuites (11%), la détection avancée des menaces (11%), la gestion des informations et des événements de sécurité (11%).

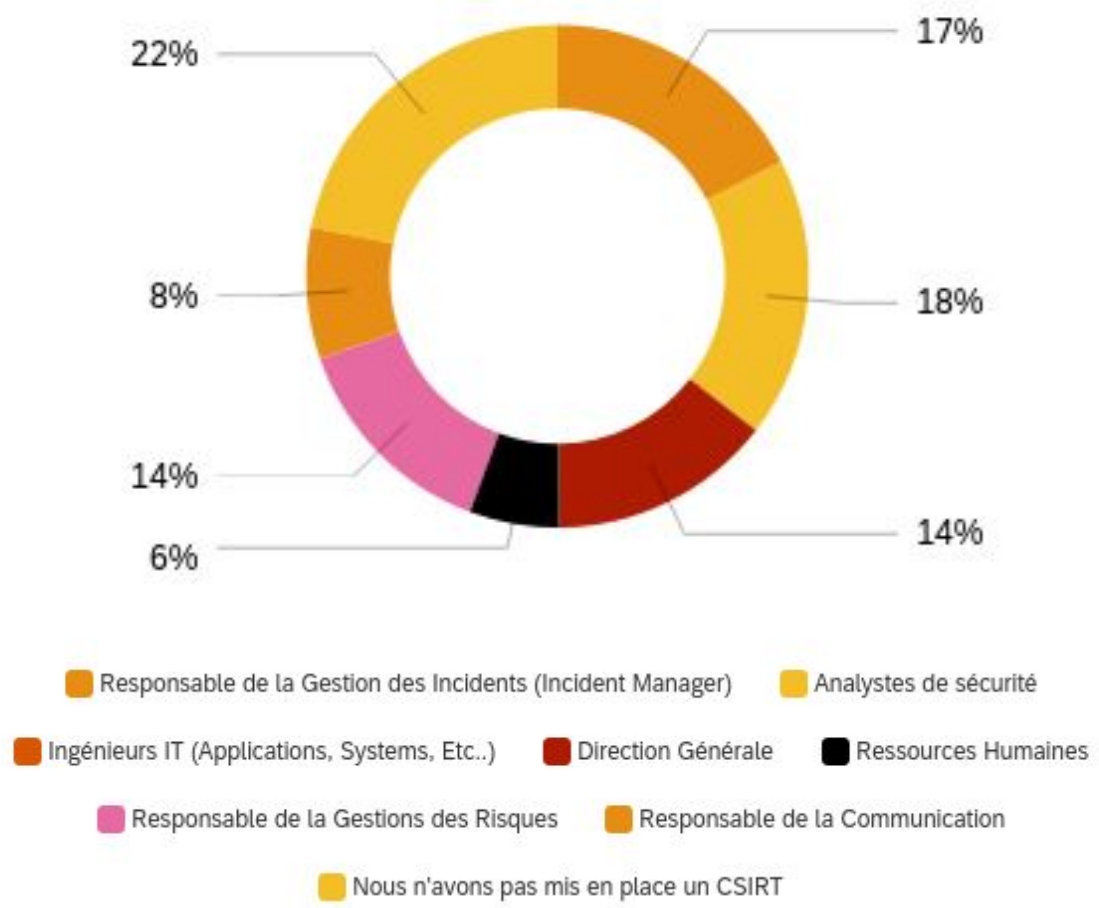
Toutefois, les solutions de surveillance de la marque sont très peu implémentées (4%) tandis que les solutions de protection des terminaux ne le sont pas.

Quels types de services/solutions de sécurité avez-vous mis en place pour assurer la cybersécurité des données et des systèmes critiques de votre entreprise?



La mise en place d'un CSIRT : une pratique non systématisée

Au cas où vous avez mis en place un CSIRT (Cyber Security Incident Response Team), quels sont les rôles au sein de votre entreprise qui composent le CSIRT?



22%

Par ailleurs, 22% des répondants déclarent n'avoir pas mis en place un CSIRT.
Pour les autres répondants, le CSIRT se compose des analystes de sécurité (18%), du responsable de la gestion des incidents (17%), de la Direction Générale (14%), du responsable de la gestion des risques (14%), du responsable de la communication (8%) et des Ressources Humaines (6%).
Nous sommes encore face à une réponse majoritairement technologique et une faible implication de la Direction Générale.

Des incidents de cybersécurité de plus en plus récurrents et l’absence d’une culture de police d’assurance

37%

Incidents

37% des entreprises interrogées ont détecté des incidents de cybersécurité au cours des 06 derniers mois.

Les secteurs les plus touchés sont le secteur financier (43%), le gouvernement et le secteur public (38%), la Technologie, médias et télécommunications (44%) et l'énergie, utilities et ressources (41%).

56% des entreprises de plus de 500 personnes ont détecté des incidents de cybersécurité au cours des 06 derniers mois. Il en est de même pour 33% des entreprises comprenant entre 100 et 500 personnes et 25% des entreprises de moins de 100 personnes.

47%

Police d’assurance

47% des entreprises interrogées ne disposent pas d’une police d’assurance pour les incidents de cybersécurité. Parmi celles-ci, 36% ont détecté des incidents de cybersécurité au cours des 06 derniers mois et 28% ne prévoient pas de s’en doter à moyen terme.

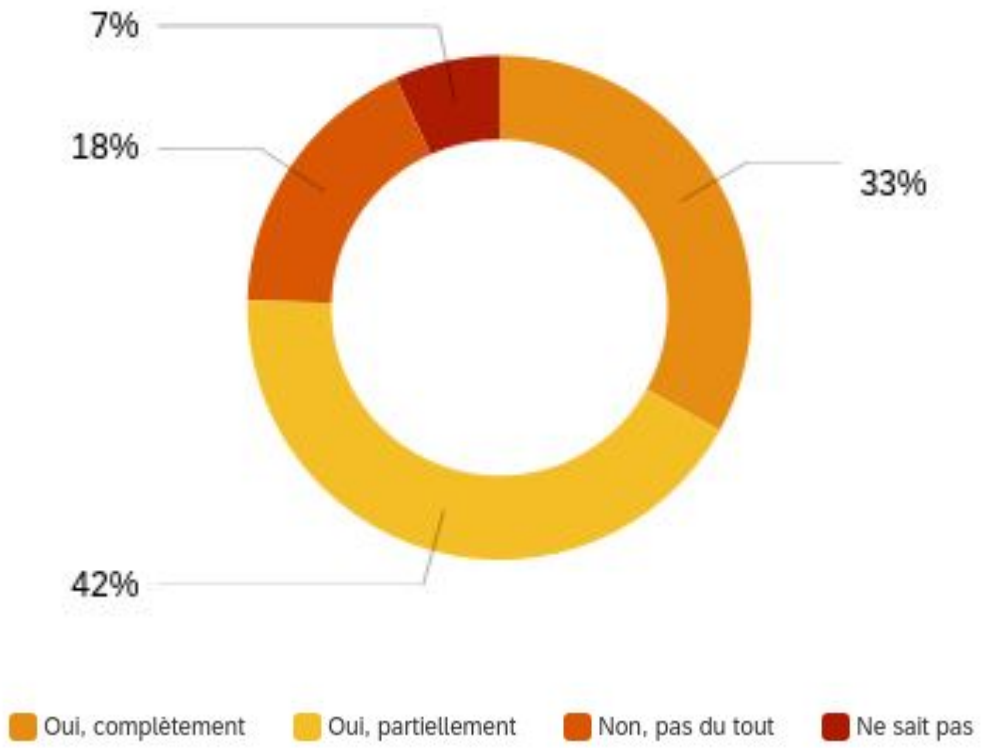
33% des répondants ne disposent pas d’informations relatives à l’existence d’une telle police d’assurance.

La gestion des cyberattaques : un challenge pour les entreprises en AFSS

Gestion d’une cyber attaque

42% des répondants estiment que leur entreprise ne peut que faire partiellement face à une cyber attaque tandis que 18% estiment que leur entreprise ne peut pas faire face à une cyberattaque.

Selon vous, votre entreprise est-elle capable de gérer une cyberattaque ?



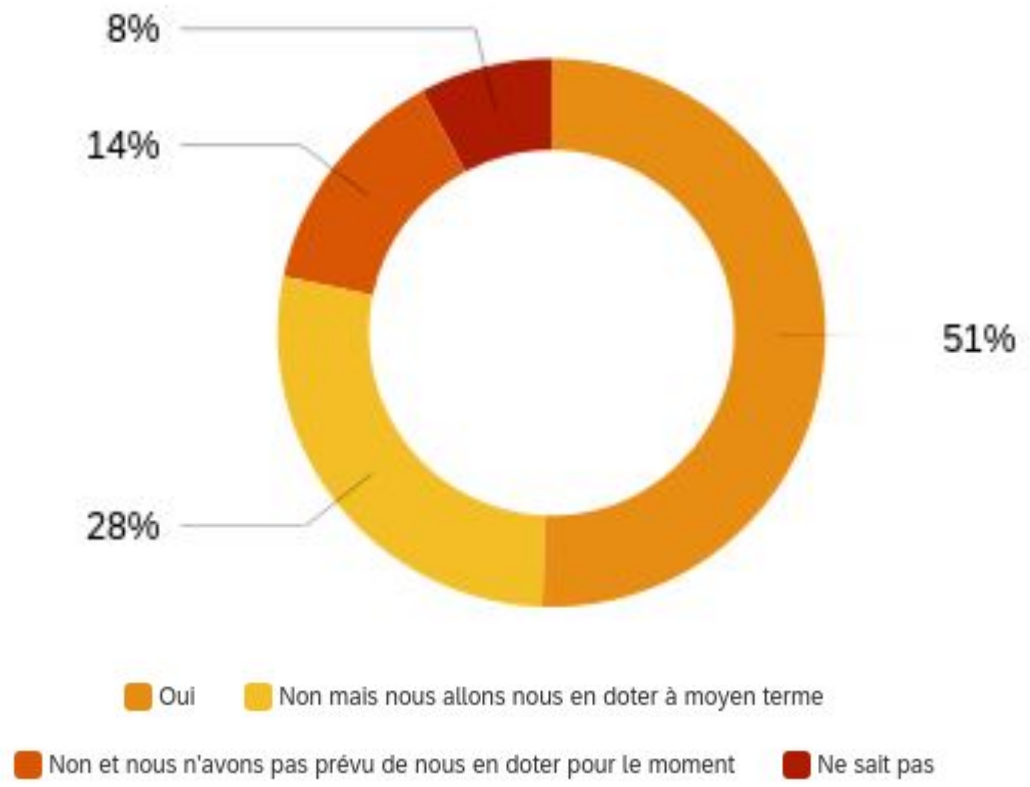
La gestion des incidents de cybersécurité : un processus non maîtrisé

42%

Un pourcentage élevé des répondants avoue n'avoir pas mis en place un processus (42%), ni une cellule (62%) de gestion des cyberattaques. Ceci traduit une faiblesse en matière de cyber résilience et dénote un besoin en développement de compétences en matière de cybersécurité notamment à travers des formations et un accompagnement.

Une bonne stratégie cyber devrait prendre en compte la mise en place des contrôles nécessaires pour mitiger l'impact d'une potentielle cyberattaque.

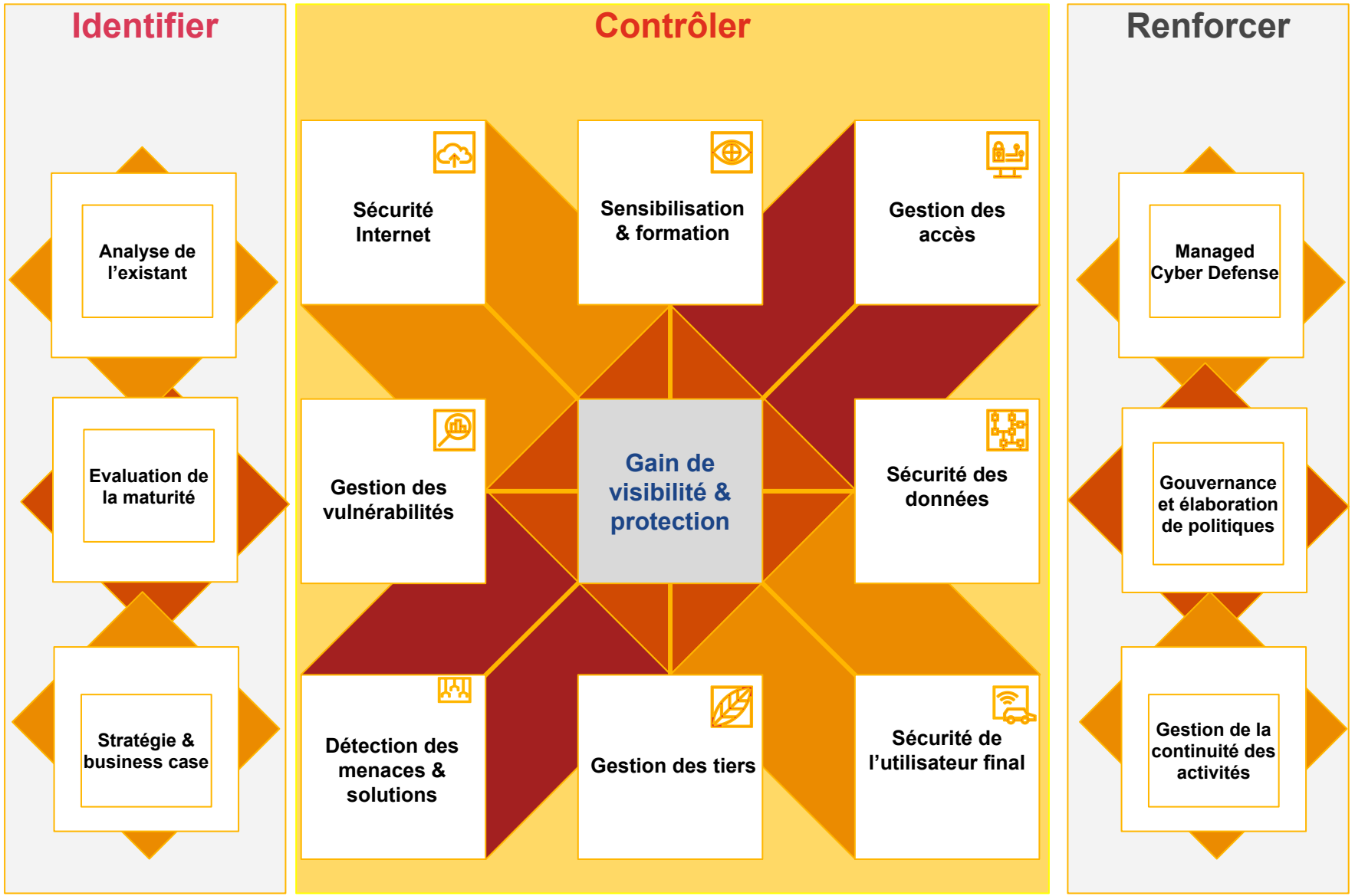
Avez vous mis en place un processus de gestion des incidents de cybersécurité ?



Découvrez l’offre PwC en matière de cybersécurité

Une approche basée sur 03 grands axes

Découvrez notre approche en matière de cybersécurité basée sur les trois piliers suivants : Identifier, Contrôler et Renforcer pour vous aider à faire face à vos enjeux et défis liés à la cybersécurité.



Annexes

5

A propos de l’enquête

- Cette enquête a été effectuée entre septembre et novembre 2020.
- Elle porte sur 281 réponses obtenues de personnes localisées en RDC (37%), au Cameroun (16%), en côte d’Ivoire (13%), à Madagascar (11%), au Sénégal (10%), en Guinée-Conakry (8%), au Congo (3%) et au Gabon (2%).
- L'échantillonnage est basé sur une population constituée des travailleurs dans chaque pays secteur agricole exclu (source Banque Africaine de Développement).
- Les répondants appartiennent principalement au secteur financier (27%), Technologie, médias et télécommunications (18%), Énergie, services publics et ressources (15%), Industrie, fabrication et automobile (7%), Marché de consommation (3%), Gouvernement et secteur public (8%), autres (22%).
- Parmi les réponses, 29% proviennent des entreprise ayant plus de 500 personnes, 36% proviennent d’entreprise comprenant entre 100 et 499 personnes et 35% proviennent d’entreprises de moins de 100 personnes.
- Plus de 150 organisations ont participé à l’enquête.

Abréviations

AFSS : Afrique Francophone Subsaharienne

CSIRT : Computer Security Incident Response Team

RDC : République Démocratique du Congo

RSSI : Responsable de la Sécurité des Systèmes d'Information

SIEM : Security Information and Event Management

SSFA : Sub-Saharan Francophone Africa

Glossaire

CSIRT : Organisme qui reçoit des signalements d'atteintes à la sécurité, analyse les rapports concernés et répond à leurs émetteurs. Un CSIRT peut être un groupe déjà établi ou une équipe se réunissant ponctuellement.

Cybermenace : Activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.

Cyber risque : Tout risque de perte financière, d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes d'information (SI).

Cyber résilience : La cyber résilience consiste pour une entreprise à acquérir la capacité de reprendre les activités normales, de minimiser et réparer les dommages subis suite à une cyber attaque.

Cybersécurité : Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, etc.

SIEM : Système permettant à une entreprise de centraliser toutes les informations de sécurité en un seul outil. Il permet de collecter les données auprès des logiciels antivirus, des pare-feux, des serveurs, etc. pour une analyse centralisée.

Third Party Risk Management : Processus d'identification, d'évaluation et de contrôle des risques pouvant survenir tout au long du cycle de vie des relations avec des tiers.

Contact

Valéry Kapnang
Associé
valery.kapnang@pwc.com
+237 6 77 50 29 80

Mitie Design RITM3322312 (09/20).