2018

White paper series
Publication 3

OPPORTUNITÉS ET DÉFIS POUR LES **PME** DANS LE CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

OEA Plus de droits pour plus de personnes

aws

OPPORTUNITÉS ET DÉFIS — POUR LES **PME** DANS LE — CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

CRÉDITS

Luis Almagro

Secrétaire général
Organisation des États Américains (OEA)

Équipe technique de l'OEA

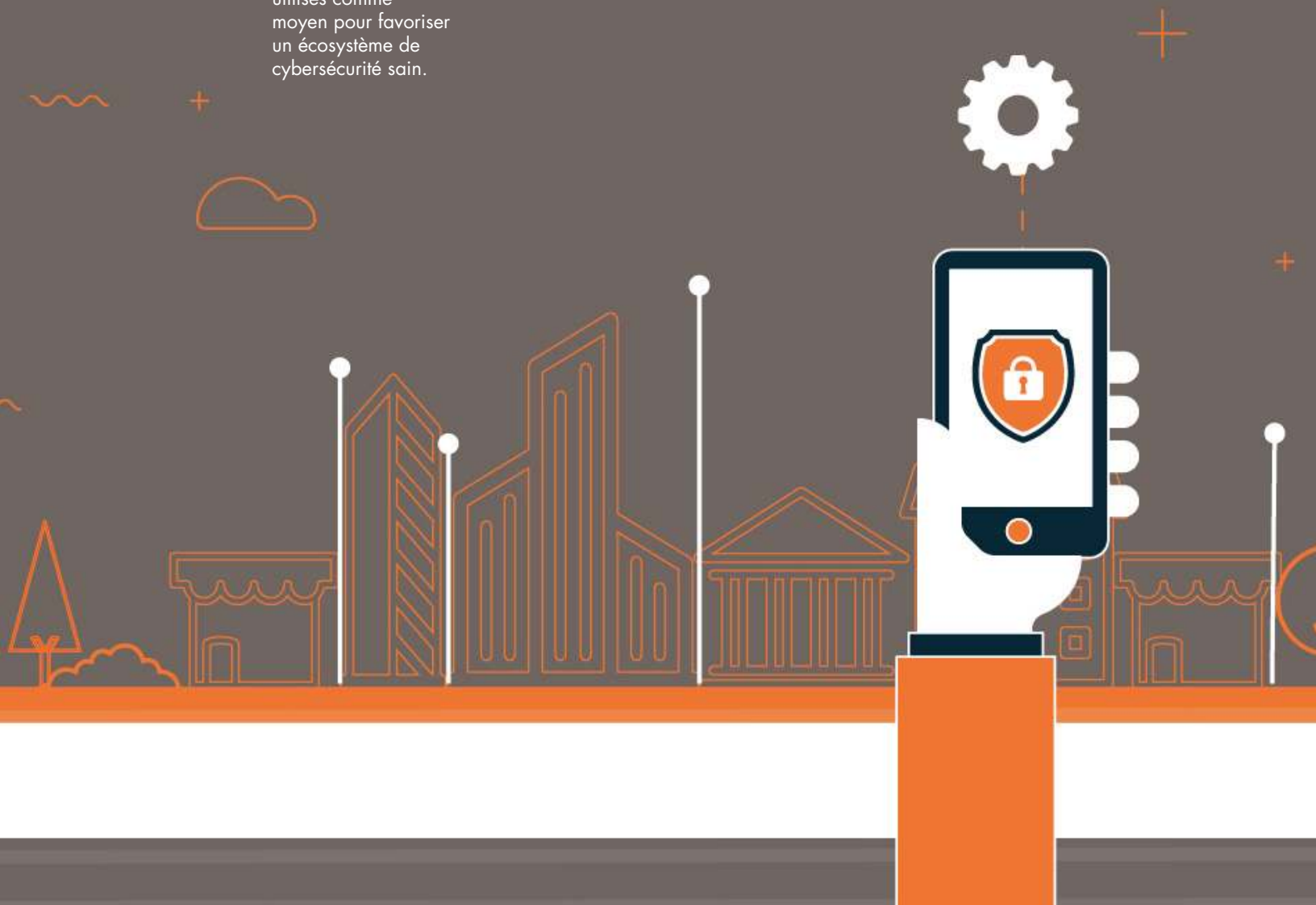
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Nathalia Foditsch
Kerry-Ann Barrett
Bárbara Marchiori de Assis
Gonzalo García-Belenguer
Mariana Cardona

Équipe technique AWS

Min Hyun
Michael South
Maria Saab

OPPORTUNITÉS ET DÉFIS — POUR LES PME DANS LE — CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

CONTENIDO



OPPORTUNITÉS ET DÉFIS — POUR LES **PME** DANS LE — CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

RÉSUMÉ

Les entreprises de différentes tailles et de différents secteurs dépendent de plus en plus des technologies de l'information et de la communication (TIC), ce qui a été déterminant en matière d'innovation, de productivité et de croissance. Malgré les innombrables avantages et opportunités, l'adoption des technologies de l'information et de la communication engendre des problèmes et les petites et moyennes entreprises (PME) sont généralement confrontées à des défis plus importants que les grandes entreprises. Les PME font face à des problèmes liés à une infrastructure médiocre en termes de technologies de l'information et de la communication, ne savent pas comment gérer correctement les menaces complexes en matière de cybersécurité et sous-estiment l'importance de la protection des données à caractère personnel. Ce livre blanc décrit brièvement certaines des difficultés rencontrées par les PME compte tenu de l'utilisation accrue des technologies de l'information et de la communication. Il aborde également certains points cruciaux quant à la protection des données à caractère personnel et leur confidentialité, ainsi que l'importance de procéder à des changements institutionnels qui permettent la création d'une culture « de prise de conscience de la sécurité ». En outre, ce document explique les différents rôles joués par les gouvernements en tant que facilitateurs d'un écosystème sain, lorsque les règles des marchés publics sont utilisées pour favoriser l'adoption de normes de cybersécurité ou en encourageant les efforts de renforcement des capacités des PME. Finalement, nous aborderons dans l'avant-dernier paragraphe quelques mesures directes permettant aux PME de renforcer leur niveau de préparation à la lutte contre la cybercriminalité.

1 OPPORTUNITÉS ET DÉFIS POUR LES PME DANS LE CONTEXTE D'UNE UTILISATION ACCRUE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Nous trouvons des petites et moyennes entreprises (PME) partout dans les Amériques. En effet, elles sont votre boulangerie de quartier, l'entreprise familiale de vélos ou encore le fournisseur local d'accès Internet et de conception de logiciels. Ces PME sont bien connues pour leur impact positif sur les sociétés et sont considérées comme étant « essentielles à la mondialisation et à une croissance plus inclusives » (OCDE, 2017, p.5) car elles ont démontré être fondamentales pour le développement social et économique des pays. Les « startups » et les organisations « dédiées à la rechercher d'un modèle économique reproductible et flexible » (Blank, 2010) sont également devenues populaires à travers les Amériques au fil des années[1]. Bien que les contributions peuvent varier en fonction des entreprises, pays et secteurs, différentes études suggèrent qu'elles sont en effet fondamentales dans la réduction de la pauvreté et la création d'emplois (exemple, Deijl et al., 2013, Lopez-Acevedo & Tan, 2011).

Ce rôle accru des PME se doit en grande partie à leur dépendance croissante à Internet et aux technologies de l'information et de la communication (TIC) qui leur permettent de tirer profit de l'économie mondiale, de renforcer leurs processus, leur efficacité et d'innover. En effet, les startups sont largement dépendantes des technologies de l'information et de la communication. Elles représentant de nouveaux modèles de création de connaissances, d'innovation et de promotion d'une culture entrepreneuriale. En Amérique latine, par exemple, les startups ont attiré des investissements qui ont plus que doublé au cours des cinq dernières années, bien que ces chiffres soient encore inférieurs à ceux d'autres régions émergentes du monde (Ruvolo, 2018). Un exemple de l'augmentation de l'utilisation des technologies de l'information et de la communication par ces organisations est le développement croissant des nouvelles startups de technologies financières (Fintech) dans les pays d'Amérique latine et de la Caraïbe[2], au cours de ces dernières années. Elles sont des centaines dans la région à utiliser des plateformes en ligne et à inciter l'accès des autres PME au crédit (IDB et Finnovista, 2017).[3]

En dépit de ce rôle accru, les PME font face à des défis spécifiques par rapport aux grandes entreprises. Elles sont confrontées à davantage d'obstacles en matière d'innovation et d'accès aux réseaux de recherche et systèmes de brevetage (Zuniga et al.2016). Diverses études ont également mis en exergue leurs difficultés quant à l'accès aux instruments financiers (OECD, 2017; Zuniga et al.2016). En effet, une mauvaise infrastructure en termes de technologies de l'information et de la communication empêche les PME d'opérer de façon efficace et d'accéder aux marchés internationaux à des coûts compétitifs (OCDE, 2017, p.12). Toutefois, la compétitivité et l'efficacité ne sont pas

[1] Bien que les PME et les startups soient différentes de par leurs méthodes de financement et leur flexibilité, les deux modèles sont moins importants que ceux des grandes entreprises et pourraient faire face à des défis semblables en matière de cybersécurité ainsi que de confidentialité et protection des données. Par conséquent, le terme de « PME » est utilisé de manière indistincte dans ce document.
[2] Les segments Fintech populaires sont les « plateformes de financement alternatives », les « Solutions de paiement », la « gestion financière des entreprise » et la « gestion financière personnelle ». Le Brésil, le Mexique, l'Argentine, la Colombie et le Chili sont les pays de la région où se trouvent la plupart des entreprises Fintech (IDB et Finnovista, 2017).
[3] D'après l'explication de Cathles (2014), il existe un manque d'« indicateurs opportuns de l'entrepreneuriat sur la démographie des entreprises » (p.22) dans les pays d'Amérique latine et de la Caraïbe car seules des « informations partielles sur l'entrepreneuriat » sont disponibles dans la région.

les seules affectées lorsqu'il n'existe pas de bonne infrastructure, de compétences appropriées et une bonne gouvernance. La question de la sécurité est également importante et a fortement attiré l'attention au cours des dernières années à cause de la multiplication des cyberattaques contre les PME. Celles-ci peuvent faire face à des pertes supposant des coûts par habitant plus élevés que ceux des grandes entreprises et de nombreuses PME ne savent pas encore comment s'attaquer au problème (Zec & Kajtazi, 2015).

Au fil des années, les défis rencontrés par les entreprises dans la lutte contre la cybercriminalité ont changé en raison de l'évolution des types de risques. Dans la première décennie des années 2 000, les organisations ont dû s'attaquer aux problèmes posés par les logiciels espions, le phishing automatique et les proxys de contournement de sites. Or, elles doivent aujourd'hui faire face à des défis plus complexes comme celui du spear phishing désormais courant (Symantec, 2018). Les menaces plus sophistiquées telles que les « ransomware » peuvent même « infecter l'organisation et enregistrer des mécanismes de nettoyage pour couvrir leurs traces » (Bitdefender, 2017, p.2). En effet, selon PwC (2018), les cybermenaces constituent la principale inquiétude des PDG aux États-Unis.

Outre la complexité accrue des menaces, la cybersécurité devrait être vue sous différents angles. Une grande variété de définitions de la cybersécurité ont été données, bien que beaucoup de celles-ci ne soient pas complètes et interdisciplinaires comme elles devraient l'être (Craigen et al., 2014). Comme nous l'expliquons brièvement ci-dessous, la compréhension de la cybersécurité s'est développée au fil des années et englobe désormais les violations et activités purement techniques mais également les différents types d'exploitations et d'utilisations des données non autorisées. En effet, la confidentialité et protection des données personnelles[4] fait également partie des défis à relever par la plupart des entreprises.

[4] Différents cadres réglementaires traitent les « données personnelles » d'une façon différente à celle des autres données. Bien que le concept n'ait pas été appliqué de la même façon d'un pays à l'autre, il fait généralement référence à des données permettant à un individu d'être identifié personnellement.

PME, CONFIDENTIALITÉ ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

2

Depuis les révélations de 2013 sur des activités de surveillance internationale dans les pays étrangers[5], plusieurs nations de la région ont entamé des discussions et créé des cadres juridiques et politiques visant à protéger les données à caractère personnel et la vie privée, puis ont sensibilisé davantage aux risques cybernétiques (Maciel et al., 2016). La sécurité peut ainsi être comprise plus largement et englober également les aspects liés à la protection des données. Les PME doivent comprendre la façon dont les données doivent être collectées, stockées, exploitées, utilisées et protégées.

La législation relative à la confidentialité et protection des données à caractère personnel n'est pas nouvelle dans les Amériques et existe dans différents pays de la région depuis plus de trente ans (Cerda, 2012). Cependant, différents cadres ont été mis en place, avec différents niveaux de maturité. La plupart des pays des Amériques n'ont pas d'autorité de protection des données personnelles et les seuls pays des Amériques signataires de la « Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » sont l'Argentine, le Mexique et l'Uruguay.[6] Face à ce scénario, aucun niveau minimum de protection des données ou de normes de confidentialité ne doivent être garanties dans les pays des Amériques. Toutefois, cela ne signifie pas que les PME ne doivent pas prendre au sérieux la protection et confidentialité des données personnelles, ni de façon plus large, la cybersécurité. En offrant un niveau de protection solide, les PME créent des avantages compétitifs et la confiance est renforcée.

En effet, non seulement la confiance pourrait être affectée par une mauvaise gestion de la protection et confidentialité des données personnelles mais le cycle de vente pourrait même se voir touché et des pertes financières pourraient survenir en cas de violation de ces données. Selon CISCO (2018), le cycle de vente des entreprises peut se voir profondément affecté en raison des préoccupations des consommateurs en matière de confidentialité des données. À leur tour, les organisations « matures en termes de protection des données à caractère personnel » sont moins susceptibles de subir des retards dans leur cycle de vente ou des violations de données. De plus, les entreprises ayant un modèle organisationnel hybride en matière de protection des données personnelles (par rapport à un modèle centralisé ou décentralisé) se sont avérées moins enclin aux retards dans les ventes (CISCO, 2018). Comme nous pouvons le constater, les PME devraient également essayer de créer un modèle de gouvernance qui bénéficie à la cybersécurité.

Outre la gouvernance de l'entreprise, les produits et services eux-mêmes peuvent être conçus de sorte que les protections soient mises en place « dès la conception ». Ce concept très vaste comprend différents aspects comme expliqué dans l'encadré ci-dessous.

[5] Ces révélations ont démontré que les États-Unis avaient placé sous surveillance les pays étrangers. En effet, les révélations ont signalé que la « NSA, National Security Agency et d'autres organismes responsables de l'application de la loi et de la sécurité nationale aux États-Unis ont utilisé des dispositions de la loi FISA (Foreign Intelligence Surveillance Act) et de la USA PATRIOT Act pour obtenir des données électroniques de tiers » (Castro, 2013). , page 1). Clarke et al. (2013) ont fait valoir que « les préoccupations étrangères concernant la surveillance américaine peuvent réduire directement la part de marché des sociétés de technologie basées aux États-Unis et, de plus, peuvent justifier indirectement les mesures protectionnistes » (page 212).

[6] Consulte el "Cuadro de firmas y ratificaciones del Tratado 108", disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=wWwV2sLp

ENCADRÉ #1 La protection des données personnelles dès la conception

Le concept de « protection des données personnelles dès la conception » existe depuis plusieurs années et est essentiel à la sécurité des données. Il désigne généralement « l'intégration de la confidentialité dans les technologies de l'information, les pratiques commerciales et les infrastructures en réseau, dès le départ, comme une fonctionnalité essentielle. Cela signifie construire la confidentialité d'entrée de jeu, avec prévoyance » (Cavoukian, 2012, p.39).

Les chefs d'entreprise peuvent opérationnaliser ce concept de différentes manières, notamment en développant des logiciels qui intègrent des exigences en matière de confidentialité telles que la réduction de la collecte de données, l'utilisation de processus d'anonymisation ou l'utilisation du « cryptage par défaut »[7] (Cavoukian, 2012). En raison des grandes quantités de données que les PME peuvent collecter, exploiter et stocker, relever le défi de la protection des données personnelles est plus important que jamais, mais aussi plus difficile qu'auparavant. En effet, plusieurs modèles d'affaires reposent sur le « big data » et les « fragments numériques laissés par les utilisateurs des technologies et réutilisés par la suite pour analyse » (D'Acquisto et al., 2015, p.22). Pour cette raison, réduire la collecte et protéger les données personnelles tout en permettant leur transformation, exploitation et analyse de manière utile et pertinente pour les secteurs privé et public est un défi majeur.

Certains cadres réglementaires contiennent expressément des règles relatives à la « protection des données à caractère personnel dès la conception ». Ainsi, le règlement général sur la protection des données (GDPR), entré en vigueur dans l'Union européenne en 2018, a établi des attentes en matière de « protection dès la conception » et stipule également que « par défaut, seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement » soient traitées.[8] Par conséquent, un suivi de ces exigences devra être opéré lors de l'entrée des entreprises sur les marchés publics, comme décrit par la suite dans ce document.

En dépit du développement croissant des mesures de lutte contre la cybercriminalité et la protection des données personnelles au cours des dernières années, toutes les PME ne sont pas pleinement conscientes des avantages de leur mise en œuvre et manquent parfois de ressources et compétences.

[7] Voir l'étude de cas "Using Encryption by Default" de la New America Foundation, disponible sur https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-1-using-transit-encryption-default/

[8] Article 25 (2), GDPR: « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. 3En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».

SENSIBILISATION DES PME À LA CYBERSÉCURITÉ

3

Le niveau de sensibilisation et de préparation en matière de cybersécurité et protection des données varie considérablement selon les PME. Alors que certaines sembleraient avoir compris et mis en œuvre des mesures visant à protéger leurs ressources et leurs compétences, d'autres n'en ont appliquées aucunes. Effectivement, partie de ce problème repose sur un manque de « Culture de sécurité », définie comme regroupant des « attitudes, croyances et perceptions partagées par les membres d'un groupe définissant des normes et des valeurs qui déterminent à leur tour la manière dont ils agissent et réagissent face au risque et au système de contrôle des risques » (Lopes et Oliveira , 2014, page 278). Le manque de culture de sécurité pourrait conduire à une compréhension limitée de la sécurité au sein des PME qui cherchent à mettre en œuvre des mesures pour protéger les couches physiques et logiques de leurs réseaux mais qui sous-estiment la composante humaine telle que la formation des employés et le contrôle de la conformité (Lopes et Oliveira, 2014).

Si le renforcement de la culture de sécurité au sein des PME est nécessaire, que devrait-on faire à ce sujet ? En ce sens, sensibiliser et former les employés est sans aucun doute essentiel. Beyer et. Al. (2015) affirment que « la sécurité ne fait actuellement pas partie des contrats psychologiques dans la plupart des organisations » (p.8). Ils expliquent également certains points clés des campagnes de sensibilisation comme la suppression des tâches de sécurité non réalistes, l'accent mis sur les changements de comportement et l'implication progressivement des employés. L'aspect humain de la cybersécurité ne doit donc pas être sous-estimé et celles-ci sont quelques-unes des façons de le renforcer. Une étude empirique tentant d'expliquer les aspects organisationnels, technologiques et psychologiques de la cybersécurité dans les PME a révélé qu'une grande majorité des employés (les deux tiers) ne signalaient pas leurs erreurs à leurs supérieurs (Zec et Kajtazi, 2015)[9]. De plus, « l'absence de politiques internes en matière cybernétique dans les PME » et les « faibles investissements financiers » ont également été considérés comme des facteurs clés plaçant les PME en position de vulnérabilité (Zec & Kajtazi, 2015, p.237). Dans une autre étude empirique, Burgurcu et al. (2010) ont constaté que la sécurité de l'information peut être améliorée si l'on développe une culture de « prise de conscience de la sécurité » au sein de l'organisation et que reconnaître la « loyauté, réputation et bonne image » (p.544) des employés qui respectent les règles de sécurité peut avoir un impact positif sur la façon dont ceux-ci perçoivent les avantages d'une telle conformité, en modifiant leurs comportements et leurs attitudes de manière positive. Étant donné que les employés perçoivent les efforts de conformité comme une tâche fastidieuse, l'allocation d'une certaine quantité de temps, qui ne perturbe pas leurs routines, à des efforts de sensibilisation et de conformité, puis la simplification des procédures, pourraient atténuer cette perception (Bulgurcu et al., 2010; Lopes & Oliveira, 2014). De même, les avancées technologiques qui permettent d'automatiser facilement certaines tâches,

[9] Alors que beaucoup d'employés pourraient ne pas avoir l'intention de cacher leurs erreurs, il semblerait que l'aspect humain des organisations est important lors de l'évaluation des vulnérabilités des entreprises. Zec et Kajtazi (2015) ont également suggéré que les traits de personnalité devraient être pris en compte lors du recrutement de professionnels à des postes liés à la sécurité de l'information (exemple, ceux qui ont une plus forte propension à la culpabilité devraient être plus performants lorsqu'il s'agit de garantir la sécurité de l'entreprise).

devraient également être prises en compte par les PME lors de l'évaluation des options.

D'après PwC (2018), le nombre de membres du conseil chargés de surveiller les risques liés à la sécurité et à la confidentialité des données est inférieur à un tiers. Cette réalité devrait changer compte tenu du fait que les préoccupations en matière de sécurité et de confidentialité influent directement sur les résultats et par conséquent, la rentabilité des entreprises. Par ailleurs, l'embauche d'un dirigeant dont la fonction principale est de veiller à la protection et la sécurité des données dans l'entreprise est une tendance maintenant courante dans les grandes organisations. En effet, les deux tiers des entreprises « Fortune 1 000 » ont déjà désigné un « chief data officer» [Directeur des Données] ou un « chief privacy officer » [chef de la protection des renseignements personnels], bien qu'il existe une « confusion et un désaccord évidents sur le mandat et l'importance » de leurs rôles (NewVantage Partners, 2018 , p.8). L'existence d'un tel professionnel, également appelé « Directeur des systèmes d'information (CIO, en anglais) », n'est pas encore une tendance répandue au sein des petites organisations (PwC, 2018). Toutefois, ce scénario devrait changer car de plus en plus d'organisations font face aux défis et opportunités apportées par les nouvelles technologies.

Comme démontré ci-dessus, chaque organisation individuelle est responsable de ses activités ainsi que de la protection des données qu'elle amasse, stocke et utilise. Néanmoins, les gouvernements peuvent également jouer un rôle dans la promotion d'un écosystème favorable à la sécurité et ce rôle est brièvement décrit ci-après.

LE RÔLE DU GOUVERNEMENT DANS LA PROMOTION D'UN ÉCOSYSTÈME DE CYBERSÉCURITÉ SAIN POUR LES PME

4

Le secteur privé « agit comme un laboratoire qui identifie, développe et met en œuvre les meilleures pratiques en matière de cybersécurité et fournit des orientations pour l'élaboration des politiques nationales et internationales » (Shackelford et al., 2015, p.360). Les PME, même si elles font partie de ce groupe, pourraient ne pas disposer de toutes les ressources techniques, humaines et financières nécessaires leur permettant de comprendre l'ensemble des mesures de cybersécurité et de protection des données qu'elles doivent adopter, mettre en œuvre et utiliser. Ainsi, les gouvernements des Amériques ont un rôle à jouer pour soutenir la création d'un écosystème de cybersécurité sain pour les PME.

Comme le démontre Mazzucato (2013), il est erroné de supposer que l'État ne joue pas de rôle dans la promotion des technologies, car certaines des principales entreprises technologiques ont largement bénéficié des politiques gouvernementales visant à permettre la prise de risques. Elle a souligné le rôle des politiques décentralisées et « orientées vers la mission » telles que celles qui ont conduit à la création de technologies comme Internet, le World Wide Web, la technologie de communication cellulaire et le GPS qui ont également été créées avec l'aide de fonds publics (Mazzucato, 2013). La question de la sécurité pose de nouveaux défis aux gouvernements qui doivent maintenant, non seulement favoriser la création et l'adoption de ces technologies, mais aussi développer un écosystème sain qui privilégie les besoins en matière de cybersécurité. Ce rôle, comme décrit par la suite, est, entre autres, mené à bien par la sensibilisation, le renforcement des capacités et des interventions plus directes telles que l'établissement de règles de sécurité minimales en matière de cybersécurité sur les marchés publics.

Les efforts en matière de marchés publics ont été utilisés pour promouvoir la justice sociale et le changement pendant plusieurs décennies (McCrudden 2006 et 2007). Les marchés publics ont permis une plus grande accessibilité aux dispositifs dans différents pays comme les États-Unis, le Japon, le Canada et le Royaume-Uni et cela a eu un impact positif sur les personnes handicapées (Tibben & Astbrink, 2012). L'on observe la même chose en matière de cybersecurité car certains pays ont déjà établi des règlements permettant de garantir des exigences minimales de cybersécurité sur les marchés publics.

ENCADRÉ #2 Les marchés publics utilisés comme moyen pour favoriser un écosystème de cybersécurité sain.

Le règlement général sur la protection des données (RGPD), récemment entré en vigueur en Europe comme décrit ci-dessus, est un exemple de cadre qui inclut des règles sur le traitement des données à caractère personnel sur les marchés publics. Pour cette raison, « les organismes gouvernementaux devront examiner et exercer une diligence raisonnable à l'égard des contrats existants et futurs en vertu desquels les données personnelles sont traitées » (Tucker, 2018).

Aux États-Unis, certaines réglementations relatives aux exigences de cybersécurité dans les contrats gouvernementaux ont même été testées au niveau administratif. L'Institut national des normes et technologies (NIST, en anglais) a établi, par exemple, que « les exigences de sécurité s'appliquent à tous les composants des systèmes et organisations non-fédéraux qui traitent, stockent ou transmettent des informations contrôlées non classifiées ou qui assurent la sécurité de ces composants ». Ces exigences sont « destinées à être utilisées par des organismes fédéraux dans des instruments contractuels ou autres accords établis entre ces entités et des organisations non-fédérales » (SP 800-171 Rév. 1).[10] Reynolds (2018) note que de telles règles ont même été contestées au niveau administratif, puisque le Government Accountability Office des États-Unis a rendu deux décisions relatives à l'application de ces dites règles. L'on s'attend donc à ce que « davantage d'agences intègrent explicitement des exigences en matière de cybersécurité dans les appels d'offre » et que « les offrants qui ne peuvent démontrer d'une pleine conformité à celles-ci peuvent être disqualifiés car ne remplissent pas les conditions techniques ou bien rétrogradés à des fins d'évaluation » (Reynolds, 2018).

Dans certains cas, et conformément aux cadres juridiques et réglementaires des différents pays des Amériques, les objectifs sécuritaires justifient la passation directe de marchés publics. L'Argentine, la Bolivie, le Brésil, le Costa Rica, le Guyana, le Honduras, la Jamaïque, le Panama et le Pérou en sont quelques exemples, où les considérations sécuritaires sont des « circonstances spéciales » qui pourraient « rendre impossible un processus concurrentiel » (Benavides et al., 2016, p. 48). Ce cas pourrait

[10] NIST. SP 800-171 Rev. 1 https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

s'appliquer à la cybersécurité et l'on pourrait prédire les occasions pour lesquelles l'embauche directe d'entreprises pourrait être justifiée car les avantages d'un niveau minimum de cybersécurité pourraient être considérés comme plus importants que les réductions de coûts des produits et services n'incluant pas de cybersécurité. Alors que les PME devraient s'efforcer à appliquer les normes en matière de cybersécurité[11], les gouvernements devraient les aider à prendre les mesures qui s'imposent. Les règles relatives aux marchés publics pourraient évoluées ou être modifiées afin d'offrir des incitations aux PME qui choisissent d'adopter et d'appliquer ces normes. En outre, une approche par étapes, dans laquelle des entreprises de différente taille sont invitées à respecter différents niveaux de cybersécurité, peut être développée de manière à éviter de surcharger les petites entreprises.

Comme le souligne une étude conjointe publiée en 2017 par l'OEA, la Banque interaméricaine de développement et le ministère colombien des Technologies de l'information et de la Communication (OEA et al. 2017), le rôle du gouvernement devrait également consister à renforcer les capacités, à sensibiliser, ainsi qu'à élaborer des politiques pour des interventions plus directes[12]. Des programmes gouvernementaux visant à aider les PME existent déjà et se sont avérés utiles pour développer un écosystème favorable pour celles-ci. Une évaluation des programmes d'aide aux PME dans quatre pays d'Amérique latine (Chili, Colombie, Mexique et Pérou) a révélé des impacts positifs statistiquement significatifs, notamment en termes de ventes et de performance des entreprises (Lopez-Acevedo & Tan, 2011). Effectivement, au Chili la participation à des programmes destinés aux PME tels que les activités de networking et les programmes de promotion des exportations, avait un lien avec des améliorations positives à court et moyen termes. En Colombie, les exportations et investissements en R & D des PME ayant bénéficiées de l'aide d'un fonds gouvernemental ont subi un impact positif (Lopez-Acevedo & Tan, 2011).
Les politiques axées sur les efforts de renforcement des capacités pourraient également engendrer le développement de contenus, de connaissances et de cours et programmes de formation pouvant être utiles aux PME. De tels contenus pourraient être développés par les autorités publiques seules ou en partenariat avec des entreprises privées expertes en cybersécurité. Les initiatives de renforcement des compétences et de sensibilisation pourraient, par exemple, cibler le développement d'outils de sensibilisation et aligner les campagnes nationales (GFCE, 2017)[13].

Comme nous l'expliquons par la suite, le rôle du gouvernement est très large. Même si les gouvernements ont joué un rôle actif et, dans de nombreux cas, ont servi de pilier fondamental au succès des PME, il reste encore beaucoup à faire. Un tel scénario est particulièrement vrai si l'on considère que l'adoption de nouvelles technologies couplée à l'augmentation de la quantité de données collectées, exploitées, stockées et utilisées par les entreprises augmente à un rythme exponentiel.

En comprenant le scénario décrit ci-dessus, les gouvernements auront la possibilité non seulement de protéger les PME, mais aussi de favoriser un écosystème plus sûr qui puisse permettre l'émergence de la confiance et la prospérité économique. Il est donc possible de conclure que les secteurs privé et public ont tous deux un rôle à jouer. Chaque PME devrait également développer des efforts concrets visant à créer un écosystème sûr et adopter des mesures visant à renforcer leur préparation en matière de lutte contre la cybercriminalité.

[11] Les PME devraient, par exemple, examiner les exigences établies par les normes officielles en matière de cybersécurité comme le cadre de cybersécurité de l'Institut national des standards et de la technologie (NIST, National Institute of Standards and Technology), les rapports du Service Officiel de Contrôle (SOC, Service Organization Control) et la norme de l'Organisation internationale de normalisation (ISO) en matière de cybersécurité. Chacune possède des caractéristiques différentes et correspond à une méthodologie différente.
[12] Comme exemple de ces dits efforts le Département de la sécurité intérieure des États-Unis, a mené à bien le «mois de la sensibilisation à la cybersécurité », qui est « une campagne annuelle de sensibilisation à l'importance de la cybersécurité ». Le STOP. PENSE. CONNECTE. ™ est un autre effort de sensibilisation mené par une coalition d'acteurs publics et privés ainsi que des ONG pour aider « les individus à comprendre non seulement les risques liés à l'utilisation d'Internet, mais également l'importance d'un comportement responsable en ligne ». Plus d'informations sur https://www.dhs.gov/national-cyber-security-awareness-month et sur www.stopthinkconnect.org/.
[13] Le « Programme mondial pour le renforcement des capacités en matière cybernétique » de 2017, élaboré par le Forum Mondial sur la Cyber Expertise (GFCE, en anglais) a identifié différentes initiatives pour le renforcement des capacités et la sensibilisation (GFCE, 2017)

MESURES ACTIVES POUVANT ÊTRE PRISES PAR LES PME POUR RENFORCER LEUR CYBERSÉCURITÉ 5

Compte tenu des défis et opportunités décrits ci-dessus, différentes mesures peuvent être prises par les PME désireuses de renforcer leur préparation à la lutte contre la cybercriminalité. La liste ci-après décrit certaines de ces mesures:

1. **Choisir un employé qui prenne en charge tous les aspects liés à la cybersécurité et à la protection des données personnelles.** Cette personne devra, si possible, se consacrer pleinement à ces tâches. Si un tel engagement n'est pas possible en raison de contraintes budgétaires, s'assurer qu'une personne soit responsable, au moins à temps partiel, de cela et lui assurer une formation adéquate. Il est important de choisir une personne ayant les compétences et la personnalité requises car ce poste exige une attention et des connaissances particulières;

2. **Créez une « culture de sécurité » au sein de votre PME.** Las políticas internas, las campañas de sensibilización y los programas de desarrollo de capacidades Des politiques internes, des campagnes de sensibilisation et des programmes de renforcement des capacités sont quelques-uns des moyens permettant d'atteindre cet objectif. Différents programmes peuvent être créés pour différents types d'employés, mais tous devraient au minimum prendre conscience de l'importance de la cybersécurité. De plus, évitez de perturber ou de surcharger les employés et donnez-leur suffisamment de temps pour suivre de telles formations.

3. **Concevoir des produits et services qui intègrent la protection des données personnelles** (Lire les concepts de « protection dès la conception » et de « protection par default » décrits auparavant). Il ne s'agit pas seulement d'une pratique socialement responsable mais cela permet d'éviter toute responsabilité potentielle en matière de sécurité et confidentialité. En outre, les entreprises qui intègrent de telles concepts dans leurs activités principales ont des avantages compétitifs qui pourraient porter leurs fruits;

4. **Chercher toute assistance disponible, en particulier celle liée aux efforts du gouvernement pour aider les PME.** Il existe de nombreuses ressources disponibles en ligne qui doivent être soigneusement étudiées. Compte tenu de la nature du sujet, un effort constant de mise à jour des connaissances et des compétences est nécessaire;

5. **Se conformer aux normes officielles en matière de cybersécurité et de protection des données et aux exigences en matière de marchés publics.** Dans le cas où de telles exigences n'existeraient pas, en informer les décideurs et les législateurs. Il est dans l'intérêt de tous d'avoir une entreprise et un écosystème gouvernemental sains et sûrs.

LES RÉFÉRENCES 6

• Benavides, J. L., M'Causland Sánchez, M. C., Flórez Salazar, C., & Roca, M. E. (2016). Public Procurement in Latin America and the Caribbean and IDB-financed Projects - A Normative and Comparative Study. Inter-American Development Bank.

• Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. A framework for progressive engagement of staff in cyber security. Retrieved from https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

• Bitdefender. (2017). The Global Threat Landscape Report - 2017. Retrieved from https://download.bitdefender.com/resources/files/News/CaseStudies/study/181/Bitdefender-Business-2017-Whitepaper-threat-landscape-crea2186-en-EN-GenericUse.pdf

• Blank, S. (2010). What's A Startup? First Principles. Retrieved April 3, 2018, from https://steveblank.com/2010/01/25/whats-a-startup-first-principles/

• Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34, 523–548.

• Castro, D. (2013). How Much Will PRISM Cost the U.S. Cloud Computing Industry? (p. 9). ITIF. Retrieved from http://www2.itif.org/2013-cloud-computing-costs.pdf

• Cathles, A. (2014). Entrepreneurship Data for Latin America and the Caribbean -What Is There and What Is Missing? Inter-American Development Bank. Retrieved from https://publications.iadb.org/bitstream/handle/11319/6744/CTI_TN_Enterpreneurship_Data_for_Latin_America_and_the_Caribbean.pdf

• Cavoukian, A. (2012). Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Information and Privacy Commissioner of Ontario. Retrieved from http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

• Cerda Silva, A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. In Hacia una Internet Libre de Censura: propuestas para América Latina I (Eduardo Bertoni). Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. Retrieved from http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

• CISCO. (2018). Privacy Maturity Benchmark Study. CISCO. Retrieved from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study-2018.pdf

• Clarke, R., Morell, M., Stone, G., Sunstein, C., & Swire, P. (2013). Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. White House Review Group on Intelligence and Communications Technologies. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

• Cook, K. (2017). Effective Cyber Security Strategies for Small Businesses. Walden Dissertations and Doctoral Studies. Retrieved from http://scholarworks.waldenu.edu/dissertations/3871

• Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, (4(10)), 13–21.

• D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y.-A. de, & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. European Union Agency For Network And Information Security (ENISA).

• Deijl, C., de Kok, J., & Veldhuis-Van Essen, C. (2013). Is Small Still Beautiful? Literature Review of Recent Empirical Evidence on the Contribution of SMEs to Employment Creation. Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Retrieved from http://lup.lub.lu.se/record/cfac576e-a5c4-4802-b5f3-7989d9bffd46

• GFCE. (2017). Global Agenda for Cyber Capacity Building. Retrieved from https://www.thegfce.com/documents/publications/2017/11/20/gfce-global-agenda

• IDB, & Finnovista. (2017). Fintech: Innovations you may not know were from Latin America and the Caribbean. Inter-American Development Bank and Finnovista. Retrieved from https://publications.iadb.org/bitstream/handle/11319/8265/FINTECH-Innovations-You-May-Not-Know-are-from-latin-America-and-the-Caribbean.pdf?sequence=7&isAllowed=y

• Lopes, I., Oliveira, P. (2014). Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In. Rocha Á., Correia A., Tan F., Stroetmann K. (eds) New Perspectives in Information Systems and Technologies, Volume 1. Advances in Intelligent Systems and Computing, vol 275. Springer, Cham . Lopez-Acevedo, G., & Tan, H. W. (2011). Impact evaluation of small and medium enterprise programs in Latin America and the Caribbean (No. 61641) (pp. 1–146). The World Bank. Retrieved from http://documents.worldbank.org/curated/en/587801468183890334/Impact-evaluation-of-small-and-medium-enterprise-programs-in-Latin-America-and-the-Caribbean

• Maciel, M., Foditsch, N., Belli, L., & Castellon, N. (2016). Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean. In 2016 Cybersecurity Report. OAS / IDB.

• Mazzucato, M. (2013). The Entrepreneurial State: Debunking Public vs. Private Sector Myths. Anthem.

• McCrudden, C. (2006). Corporate Social Responsibility and Public Procurement (SSRN Scholarly Paper). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=899686

• McCrudden, C. (2007). Buying Social Justice: Equality, Government Procurement, and Legal Change. Oxford University Press. Retrieved from http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199232420.001.0001/acprof-9780199232420

• NewVantage Partners, (NVP). (2018). Big Data Executive Survey 2018 - Executive Summary of Findings. Retrieved from http://newvantage.com/wp-content/uploads/2018/01/Big-Data-Executive-Survey-2018-Findings-1.pdf

• OAS, IDB, & MINTIC. (2017). Impact of Digital Security Incidents in Colombia 2017. Retrieved from http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

• OECD. (2017a). Active with Latin America and the Caribbean. Retrieved from http://www.oecd.org/global-relations/Active-with-Latin-America-and-the-Caribbean.pdf

• OECD. (2017b). Enhancing the Contributions of SMEs in a Global and Digitalised Economy (Meeting of the OECD Council at Ministerial Level). Paris. Retrieved from https://www.oecd.org/mcm/documents/C-MIN-2017-8-EN.pdf

• PwC. (2018). Revitalizing privacy and trust in a data-driven world - Key findings from The Global State of Information Security Survey 2018 (p. 23). Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

• Reynolds, T. (2018, January). Top Five Government Contractor Cybersecurity Considerations for 2018. Retrieved from http://govcon.mofo.com/defense/top-five-government-contractor-cybersecurity-considerations-for-2018/

• Ruvolo, J. (2018, February 28). Global tech firms and investors are reshaping Latin America's startup environment. TechCrunch. Retrieved from http://social.techcrunch.com/2018/02/27/global-tech-firms-and-investors-are-reshaping-latin-americas-startup-environment/

• Shackelford, S., Fort, T. L., & Prenkert, J. D. (2015). How Businesses Can Promote Cyber Peace. University of Pennsylvania Journal of International Law, 36(2). https://doi.org/10.2139/ssrn.2393528

• Symantec. (2018). Rethinking Security for the Cloud GenerationWelcome to the Cloud Generation. Retrieved from https://www.symantec.com/theme/cloud-generation

• Tibben, W., & Astbrink, G. (2012). Government ICT Purchasing: What differences do accessibility criteria make for people with disabilities? University of Wollongong and GSA Information Consultants. Retrieved from http://accan.org.au/index.php?option=com_content&view=article&id=495:government-ict-purchasing-what-differences-do-accessibility-criteria-make-for-people-with-disabilities&catid=98:access-for-all&Itemid=234

• Tucker, I. (2018, January). Government procurement prepares for GDPR. Retrieved from https://www.lexology.com/library/detail.aspx?g=4cbf7ab3-2082-44d3-a41e-f2edc4537d48

• Zec, M., & Kajtazi, M. (2015). Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy. In The European Conference on Information Systems Management; Reading (pp. 231–239). Reading, United Kingdom, Reading: Academic Conferences International Limited. Retrieved from https://search-proquest-com.proxyau.wrlc.org/docview/1776778140/abstract/1F1546EA8CF452FPQ/1

• Zuniga, P., Negri, F. de, Dutz, M., & Rauen, A. (2016). Conditions for Innovation in Brazil: a review of key issues and policy challenges. IPEA, (218), 110.

OPPORTUNITÉS ET DÉFIS — POUR LES PME DANS LE — CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

OPPORTUNITÉS ET DÉFIS POUR LES PME DANS LE CONTEXTE D'UNE PLUS GRANDE ADOPTION DES TIC

OEA | Plus de droits pour plus de personnes

aws

White paper series
Publication 3

2018