ENJOY SAFER TECHNOLOGY®

L'état de la cybersécurité des PME au Canada en 2016

Une étude menée par Ipsos et commanditée par ESET Canada

Date de publication : Octobre 2016

PARTIE 1 : Introduction

Dossiers des clients, historique de comptabilité, secrets professionnels, données personnelles—qu'adviendrait-il de votre entreprise si tous ces renseignements étaient volés ou devenaient soudainement inaccessibles? Pour de nombreuses petites et moyennes entreprises (PME), la cybersécurité est souvent éclipsée par d'autres priorités d'affaires qui accaparent le budget de fonctionnement. Les propriétaires de PME croient souvent qu'ils ne seront pas la cible de pirates informatiques puisqu'ils ne recueillent pas suffisamment de données de grande valeur et, par conséquent, l'attribution de fonds ou de personnel à la cybersécurité tombe dans l'oubli.

En réalité, les PME traitent le même genre de données sensibles que les cybercriminels recherchent dans les grandes entreprises. Les PME ne sont pas protégées des cyberattaques, loin de là. Les petites entreprises sont souvent identifiées comme des portes d'entrée vers les grandes entreprises. Selon Forbes, les cyberattaques coûtent de 400 à 500 milliards de dollars par année aux entreprises, et ces chiffres ne comprennent pas la majorité des attaques puisque celles-ci ne sont pas rapportées. Tous les jours, des cybercrimes sont commis, des logiciels de rançon sont utilisés et des données sont volées sur des ordinateurs infectés. C'est une activité bien établie. Et plus votre petite entreprise prend de l'expansion, plus elle est exposée à un auditoire plus vaste et, du coup, les risques de faire l'objet d'une attaque augmentent.

C'est ainsi que les PME se retrouvent sur la sellette : comparativement aux consommateurs, les PME possèdent plus de fonds et d'actifs numériques pouvant intéresser les pirates criminels et, comparativement aux entreprises, les PME sont moins bien protégées contre les cybercrimes.

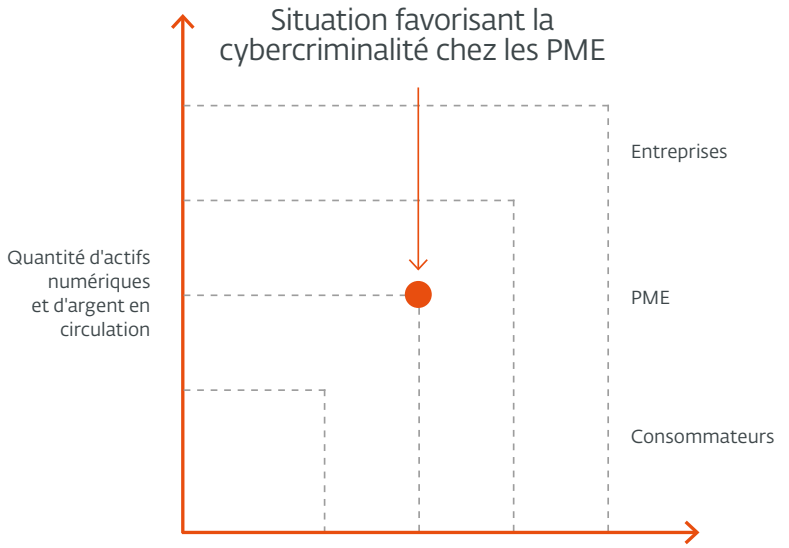
Une nouvelle étude canadienne menée par Ipsos le confirme : le risque de cyberattaques est plus élevé chez les PME canadiennes dont le revenu annuel atteint 10 millions de dollars. En effet, une entreprise sur 4 ayant des revenus de 10 à 24 millions de dollars sera victime d'une attaque, contre seulement une sur 10 dont les revenus sont sous la barre des 10 millions. Toutefois, ces dernières ne sont pas pour autant à l'abri des pirates, loin de là. De nombreuses entreprises de petite taille travaillent fort pour accroître leurs revenus, mais elles ne sont peut-être pas totalement au courant des risques de cybercriminalité inhérents à cette croissance.

Le fait de prévoir des fonds pour contrer les risques accrus de cyberattaques qui découlent de la croissance de votre entreprise est de toute évidence une bonne stratégie. Il n'est pas clair toutefois que ce message soit bien entendu par les PME. Par exemple, cette étude d'Ipsos démontre que selon les répondants, il y a une certaine incohérence entre, d'une part, les ressources attribuées à la cybersécurité par leur entreprise et, d'autre part, la perception du niveau de protection de l'entreprise à l'égard des attaques potentielles. Sept employés d'une PME canadienne sur 10 croient que leur entreprise consacre suffisamment de ressources à cette question, alors que seulement un tiers d'entre eux est « tout à fait convaincu » que leur entreprise est protégée contre les cyberattaques.

Parfois, ce type d'incohérence se produit lorsque les gens ne sont pas vraiment au courant des menaces auxquelles pourrait faire face leur entreprise. Par exemple, toute organisation qui prend au sérieux sa cybersécurité effectuerait une analyse des risques afin de déterminer quels sont les actifs numériques à risque et d'évaluer le niveau de risque. Une entreprise peut sous-estimer les risques si elle n'est pas au courant que des criminels peuvent vendre les données sur ses clients et en tirer un bon prix sur le marché noir tout en courant peu de risque de se faire arrêter, ou que des personnes malintentionnées peuvent faire de l'argent en louant des serveurs détournés au profit d'activités criminelles.

Ce sondage sur la cybersécurité des PME canadiennes révèle que les entreprises ont beaucoup de bonnes intentions à l'égard de la cybercriminalité et qu'elles sont largement sensibilisées à cette menace. Par exemple, 96 % des employés des PME canadiennes pensent qu'il est important de faire des copies de sauvegarde des fichiers, et 92 % pensent qu'il est important d'installer un logiciel de sécurité des TI sur tous les appareils informatiques. Il est également très encourageant de constater que 88 % des répondants misent sur la « formation sur les procédures de sécurité des TI ». Toutefois, beaucoup de travail reste à faire. Seulement 43 % des employés des PME du Canada sont convaincus que leur entreprise et sa réputation « survivraient et prospéreraient » à la suite d'une cyberattaque. Et seulement 40 % des répondants sont « très satisfaits » des politiques, procédures et produits actuels de sécurité des TI de leur entreprise.

Puisqu'il est démontré que le risque de cyberattaque augmente avec la croissance du revenu, les PME du Canada ont besoin d'être davantage sensibilisées aux menaces et d'accroître leur capacité à y faire face. Il est toujours opportun de préparer les politiques, les procédures et les produits de sécurité afin qu'ils soient adaptés à l'ensemble des menaces puisque celles-ci ne sont pas près de disparaître.



PARTIE 2 : Principales conclusions

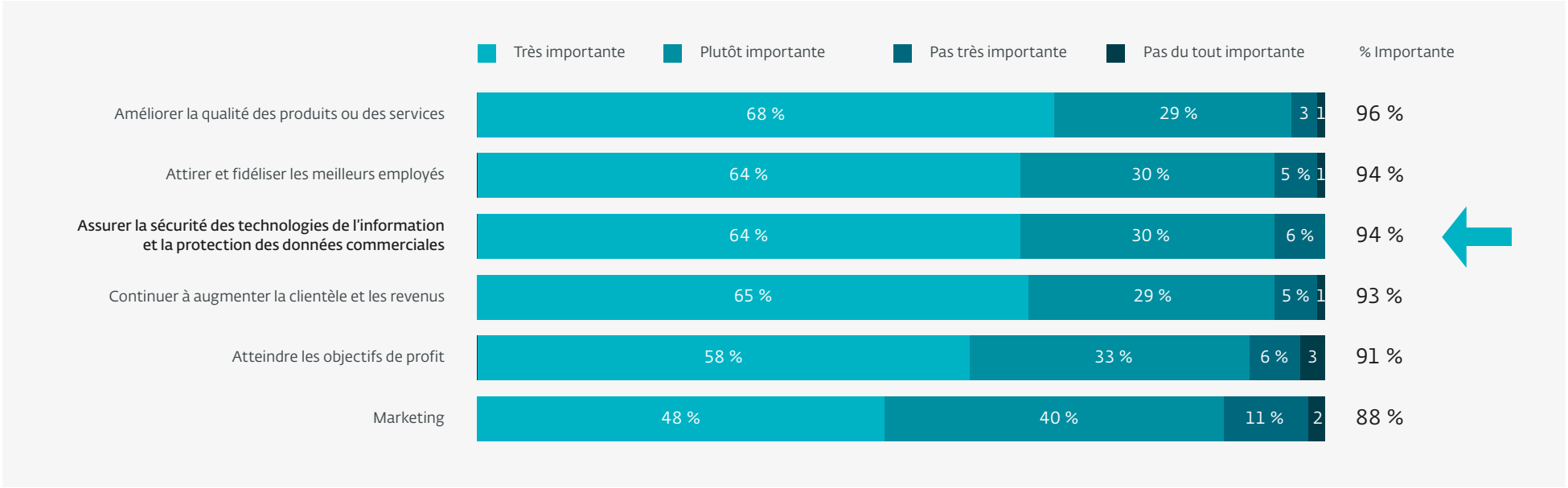
Les petites et moyennes entreprises (PME) du Canada ne sont pas immunisées contre les cyberattaques; en effet, un employé sur 5 (18 %) affirme que la PME où il travaille en a été victime.

Les cyberattaques sont plus susceptibles de se produire dans les PME canadiennes dont le chiffre d'affaires dépasse 10 millions de dollars. Par exemple, parmi les victimes de cyberattaque, trois répondants sur dix (29 %) étaient des employés d'une entreprise ayant des revenus annuels de 25 à 99 millions de dollars et un répondant sur quatre (24 %) était un employé d'une entreprise ayant des revenus annuels de 10 à 24 millions de dollars ou de plus de 100 millions de dollars. En comparaison, seulement un répondant sur dix travaillait pour une entreprise générant des revenus de 1 à 9 millions de dollars (13 %) ou de moins d'un million de dollars (12 %).

De plus, parmi les entreprises dont les employés affirment n'avoir jamais été victimes de cyberattaque, 76 % étaient des petites entreprises tandis que 70 % étaient des entreprises de taille moyenne.

Compte tenu de la fréquence dans les médias des cyberattaques et des fuites de renseignements, il n'est peut-être pas surprenant que deux employés sur trois (64 %) affirment qu'il est très important que leur entreprise participe à des activités visant à « assurer la sécurité des technologies de l'information et la protection des données commerciales ».

Q: Dans quelle mesure jugez-vous importantes les activités suivantes pour votre entreprise?



Les attaques

Parmi les entreprises qui ont été victimes d'une cyberattaque, soit deux répondants sur dix (18 %), les cibles les plus fréquentes étaient les serveurs (43 %), puis le réseau (36 %), les appareils des utilisateurs (31 %), les kiosques ou terminaux de point de vente (9 %) ou d'autres types d'attaque (8 %).

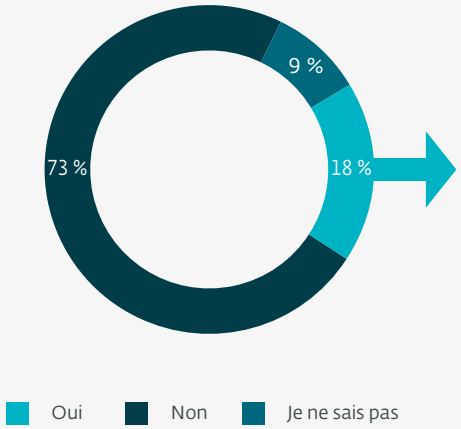
Durant l'attaque, une victime sur trois (33 %) ne pouvait plus accéder notamment à ses appareils ou à son réseau. Deux victimes sur dix affirment que leur entreprise « a perdu de l'argent parce qu'elle a dû payer pour remettre sur pied les fichiers, l'équipement informatique ou le réseau » (26 %), que « des renseignements exclusifs ou des renseignements sur les clients ont été volés » (23 %), ou que leur entreprise « a subi des pertes puisque l'attaque l'a empêchée de servir ses clients » (21 %). Un peu plus de deux répondants sur dix (23 %) ont subi une attaque d'une autre nature.

18 %
des entreprises ont déjà été victimes d'une cyberattaque

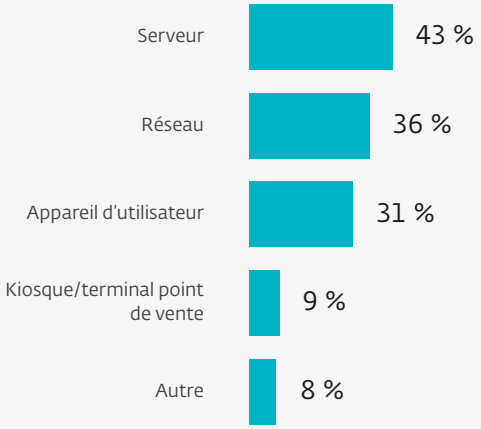
43 %
des attaques ciblaient les serveurs

Q: Votre entreprise a-t-il déjà été victime d'une cyberattaque?

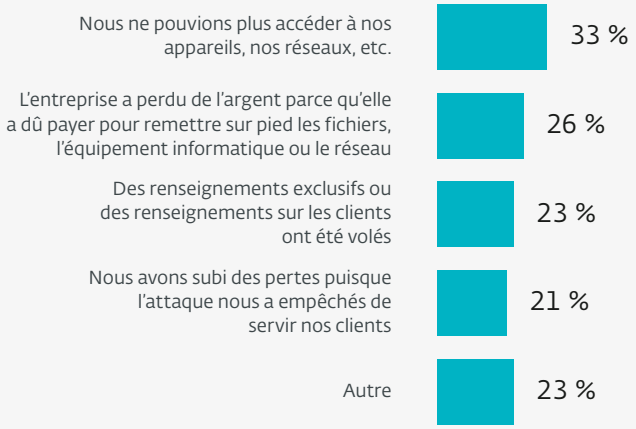
A déjà été victime d'une cyberattaque



Ce qui a été piraté



Nature de l'attaque

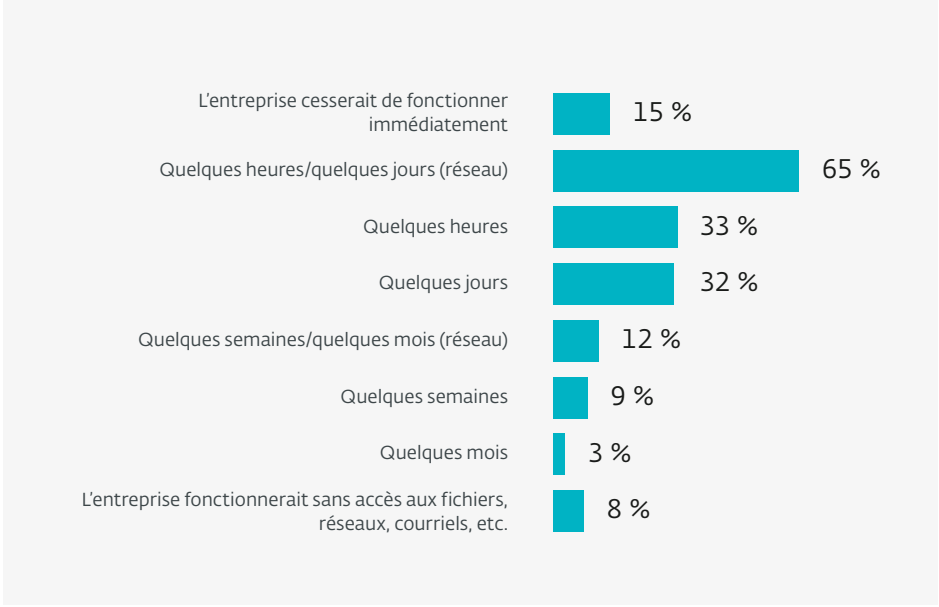


Ce qui est particulièrement inquiétant, c'est que la majorité des PME canadiennes, qui représentent 98 % des entreprises du pays selon Statistiques Canada, serait incapable de fonctionner pendant plus de quelques jours sans accès à ses données. Soixante-cinq pour cent des PME du Canada ne peuvent fonctionner plus de quelques heures ou quelques jours sans pouvoir accéder à leurs données, et 15 % des PME canadiennes devraient cesser immédiatement leurs opérations.

65 %
des entreprises du pays seraient incapables de fonctionner pendant plus de quelques jours si elles n'avaient plus accès à leurs données

15 %
des PME canadiennes cesseraient de fonctionner immédiatement

Q: Selon vous, combien de temps votre entreprise pourrait-elle fonctionner sans un accès à ses fichiers numériques, réseaux, courriels, etc.?



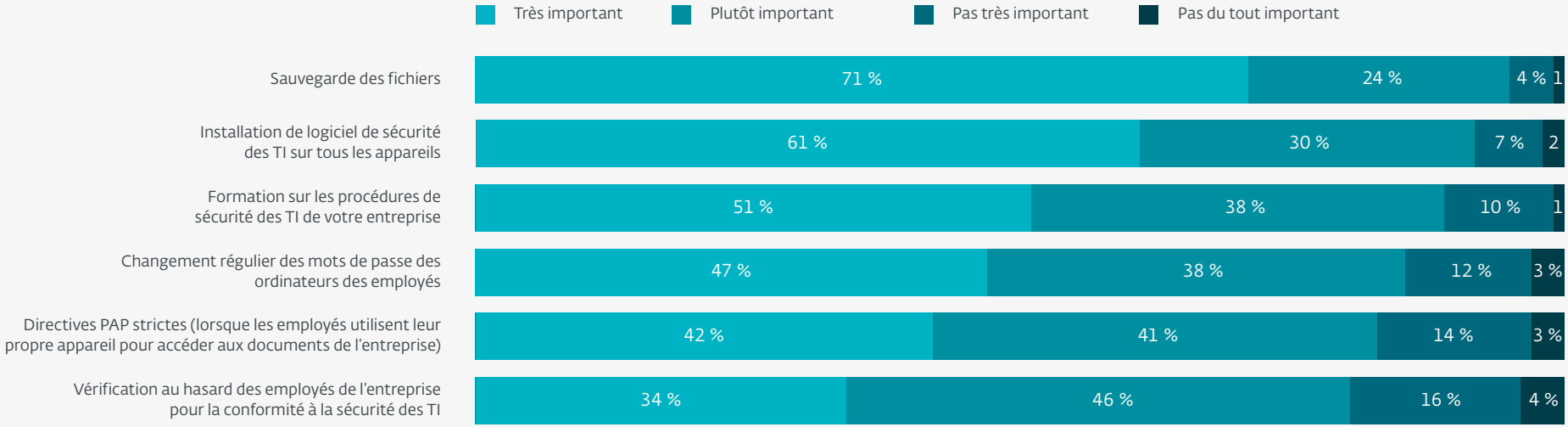
Importance des politiques, procédures et produits de TI

Pour une majorité d'employés de PME canadiennes, il est important que leur entreprise protège et sauvegarde l'information commerciale. Par exemple, neuf répondants sur dix pensent que sauvegarder des fichiers (96 %) et installer un logiciel de sécurité des TI sur tous les appareils (92 %) sont des mesures de sécurité importantes que leur entreprise devrait prendre. Les mesures suivantes viennent ensuite : formation sur les procédures de sécurité des TI de l'entreprise (88 %), changement régulier des mots de passe des ordinateurs des employés (86 %), directives PAP strictes lorsque les employés utilisent leur propre appareil pour accéder aux documents de l'entreprise (83 %) et vérification au hasard des employés de l'entreprise pour la conformité à la sécurité des TI (81 %).

86 %
des employés changent régulièrement leurs mots de passe

61 %
de tous les employés croient qu'il est très important d'installer un logiciel de sécurité des TI sur tous les appareils

Q: Dans quelle mesure jugez-vous importants les politiques, procédures et produits de TI (technologies de l'information) suivants pour la protection et la sauvegarde de l'information commerciale de votre entreprise?

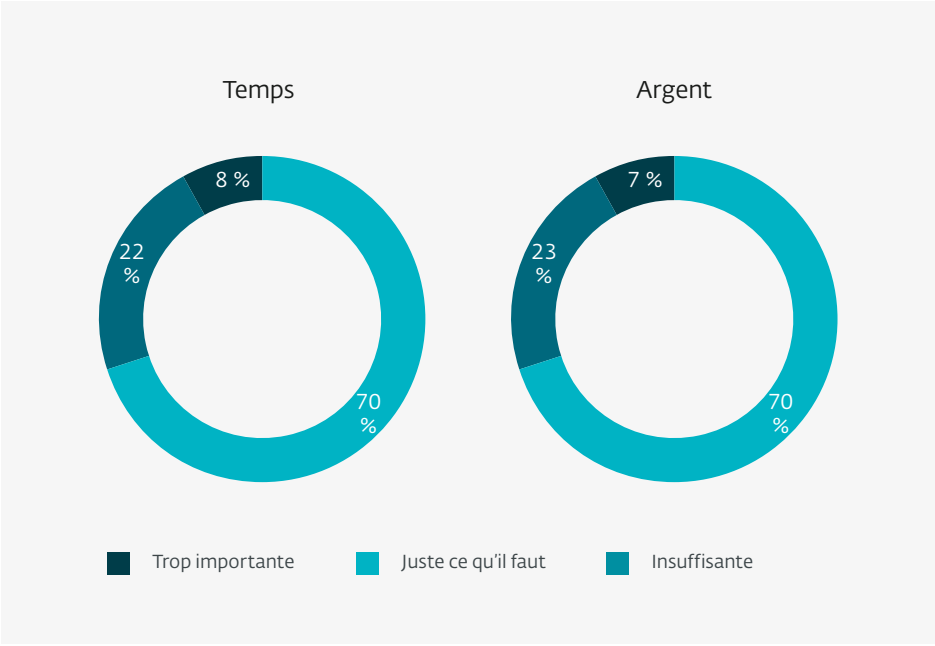


Les PME canadiennes en font-elles assez?

Seulement deux employés canadiens sur dix (22 %) affirment que leur entreprise ne consacre pas suffisamment de temps à la sécurité des TI. Sept répondants sur dix (70 %) jugent que le temps qui y est consacré est approprié, tandis que seulement un sur dix (18 %) croit que son employeur y consacre trop de temps.

Quant à l'argent consacré à la sécurité des TI, un employé sur quatre (23 %) affirme que son entreprise ne dépense pas suffisamment. Tout comme pour le temps consacré, sept répondants sur dix (70 %) estiment que les sommes consacrées à la sécurité des TI sont suffisantes. En outre, seulement une personne sur dix (8 %) croit que son employeur dépense trop d'argent à ce chapitre.

Q: Selon vous, la somme de temps et d'argent consacrée par votre entreprise à la sécurité des TI est trop importante, juste ce qu'il faut ou insuffisante?



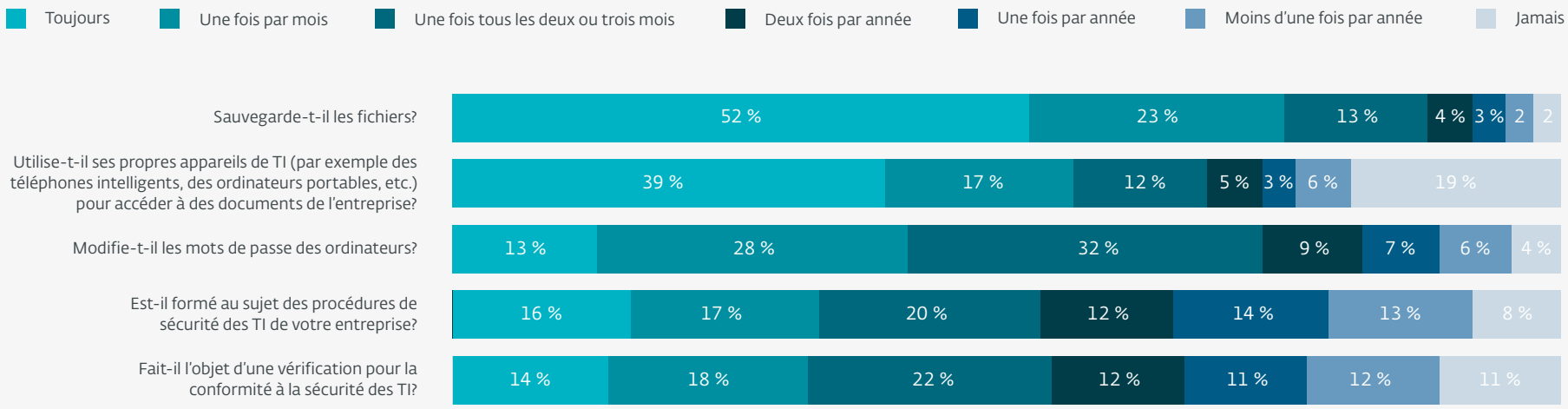
Cela dit, les employés des PME canadiennes à qui on a demandé dans quelle mesure ils sont convaincus que leur entreprise et ses données sont protégées contre les cyberattaques ont répondu dans une proportion de un sur trois (33 %) qu'ils sont « tout à fait convaincus ». Cela signifie que plus de la moitié (67 %) ont des doutes sur la capacité de l'entreprise à se protéger et à protéger ses données en cas de cyberattaque. En outre, seulement deux employés sur cinq (40 %) se disent « très satisfaits » des politiques, procédures et produits actuels de sécurité des TI de leur entreprise.

La préparation

On a demandé aux répondants à quelle fréquence leurs employés obtiennent de l'information, reçoivent de la formation ou exécutent certaines procédures liées à la sécurité des TI. Trois personnes sur quatre (75 %) affirment que leurs employés sauvegardent les fichiers de façon continue ou mensuelle. La moitié des répondants (56 %) indique que les employés utilisent leurs propres appareils de TI pour accéder à des documents de l'entreprise tous les mois ou plus souvent, et quatre personnes sur dix (42 %) sont d'avis que leur personnel change leurs mots de passe tout aussi fréquemment. Seulement une personne sur trois (34 %) affirme que le personnel reçoit de la formation sur les procédures de sécurité des TI de l'entreprise de façon continue ou mensuelle, et une personne sur trois également (32 %) indique que le personnel fait l'objet d'une vérification pour la conformité à la sécurité des TI tout aussi régulièrement.

42 %
des employés modifient leurs mots de passe chaque mois ou plus souvent

34 %
des répondants affirment que le personnel reçoit une formation sur les procédures de sécurité des TI de l'entreprise de façon continue ou mensuelle

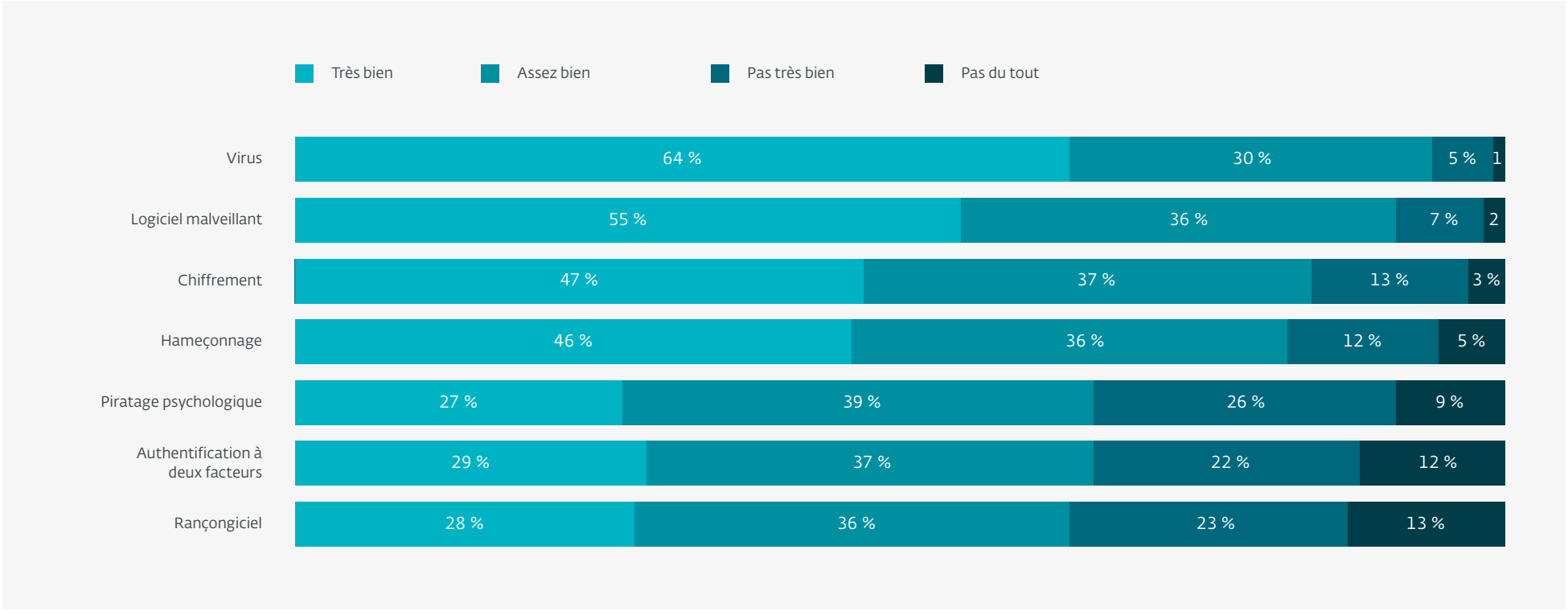


Les employés des PME canadiennes semblent avoir une bonne connaissance générale des termes relatifs à la sécurité des TI, mais on pourrait certainement faire mieux. Outre deux exceptions, moins de la moitié des répondants affirme « très bien » connaître les termes suivants : virus (64 % connaissent très bien ce terme), logiciel malveillant (55 %), chiffrement (47 %), hameçonnage (46 %), authentification à deux facteurs (29 %), rançongiciel (28 %) et piratage psychologique (en anglais, social engineering) (27 %).

64 %
des employés des PME canadiennes connaissent très bien le terme « virus »

29 %
des employés des PME canadiennes connaissent très bien le terme « authentification à deux facteurs »

Q: Dans quelle mesure connaissez-vous chacun des termes suivants :



PARTIE 3 : Cinq choses à savoir sur la protection de votre PME

Pour une petite entreprise, la cybersécurité peut représenter un défi de taille quand le temps et les ressources se font rares, mais de nombreuses pistes de solution existent, notamment des partenaires, des conseillers et des fournisseurs qui peuvent vous aider à répondre aux besoins propres à votre entreprise. Voici cinq éléments importants que vous devriez savoir sur la protection de votre entreprise et de ses actifs :

1 Les menaces à la sécurité des PME proviennent à la fois de l'intérieur et de l'extérieur.

Les deux principales menaces qui émanent de l'intérieur d'une entreprise sont la perte de données résultant d'erreurs commises par les utilisateurs et le vol ou la fuite d'information comme les listes de clients. De l'extérieur, les deux principales menaces sont l'hameçonnage ou le piratage psychologique (en anglais social engineering) et les rançongiciels. L'hameçonnage consiste à tromper les employés afin qu'ils révèlent des données relatives aux clients (codes d'accès aux comptes bancaires, aux réseaux sociaux ou à d'autres systèmes) par le biais d'un lien ou d'un courriel malveillant. Ces codes d'accès peuvent ensuite être utilisés pour détourner des données, des ressources et de l'argent. Les rançongiciels sont des logiciels malveillants (ou maliciels) qui gardent en otage des fichiers jusqu'à ce qu'une rançon soit payée. Une étude menée par ESET Canada en avril 2016 a révélé que 63 % des Canadiens ne sont pas protégés contre les rançongiciels ou qu'ils ne savent pas s'ils le sont.

2 L'unique solution miracle n'existe pas, mais ce n'est pas aussi complexe que cela puisse paraître.

Il n'y a pas de recette miracle pour protéger toutes les entreprises, petites ou grandes. La sécurité de votre entreprise passe simplement par la recherche des possibilités de perte de données et des points d'entrée potentiels, puis par l'obtention de conseils sur les meilleures façons de colmater ces brèches. Cela dit, vous pouvez faire appel à des fournisseurs de services gérés ou infonuagiques pour vous aider à protéger votre entreprise, mais vous ne pouvez pas vous décharger de votre responsabilité à l'égard de la sécurité. Vous êtes ultimement l'unique responsable de toute perte de données ou de revenus.

3 Les PME doivent continuer à mettre à jour et à niveau leurs services de sécurité afin de suivre la croissance de leur entreprise, et ce, non seulement quant au nombre d'appareils protégés par un antivirus, mais également en évaluant constamment les solutions de sécurité propres à leurs pratiques commerciales qui évoluent.

À mesure que votre entreprise évolue (nouveaux représentants, travailleurs à distance, employés qui utilisent leurs propres appareils, etc.), son réseau se complexifie et se ramifie. Par exemple, le fait d'avoir des employés qui travaillent de la maison ou d'ailleurs exige que votre réseau soit accessible de n'importe où dans le monde. Il est donc possible que vos employés utilisent des réseaux Wi-Fi non sécuritaires ou qu'ils perdent leurs appareils, ce qui pourrait mettre en danger votre entreprise, vos données et vos ressources.

4 Vos employés sont à la fois votre meilleur actif et votre maillon le plus faible.

Il est plus facile que vous ne le pensez d'utiliser votre personnel pour lutter contre la cybercriminalité. Faire en sorte que vos employés sachent qu'ils font partie intégrante de la sécurité de l'entreprise est une facette importante d'une bonne stratégie en matière de cybercriminalité. Pour ce faire, une formation régulière et la vérification du comportement des employés sont de mise. Assurez-vous que votre personnel connaît les menaces actuelles et les façons de procéder. Un employé pourrait ainsi ne pas cliquer accidentellement sur un lien d'hameçonnage ou visiter un site Web compromis.

5 Certaines mesures de sécurité de base peuvent vous aider.

Exigez que vos employés utilisent des mots de passe ou des phrases passe difficiles à trouver sur tous les appareils et qu'ils les modifient souvent. Mieux encore, mettez en place un système d'authentification à deux facteurs qui requiert un mot de passe ET une deuxième validation, soit sur un appareil mobile ou encore une identification biométrique comme une empreinte digitale.

De plus, vous devriez mettre à jour les logiciels et les micrologiciels au besoin, et ne pas attendre avant d'installer un correctif. L'utilisation d'un logiciel de sécurité à plusieurs niveaux est essentielle. Ce logiciel devrait être installé sur chaque appareil et sur chaque serveur constituant un point d'entrée. Les copies de sauvegarde doivent aussi être faites régulièrement. Ainsi, si vous deviez être victime d'une cyberattaque ou si vos fichiers étaient ciblés par un rançongiciel, vous auriez l'esprit tranquille sachant que vos données importantes ont été sauvegardées et qu'elles peuvent être facilement accessibles.

PART 4 : Méthodologie

Voici les principales conclusions d'un sondage réalisé par Ipsos entre le 22 et le 24 août 2016 au nom d'ESET Canada. Dans le cadre de ce sondage, on a interrogé en ligne un échantillon de 1 003 adultes canadiens employés d'une petite entreprise (définie comme une entreprise qui compte de 5 à 99 employés) ou d'une entreprise de taille moyenne (définie comme une entreprise qui compte de 100 à 499 employés) qui travaillent dans le domaine des TI, qui occupent un poste de haute direction ou qui possèdent une excellente connaissance des politiques et des procédures de TI de l'entreprise et qui proviennent du panel canadien en ligne d'Ipsos.

On a ensuite utilisé la pondération afin d'équilibrer les données démographiques pour s'assurer que la composition de l'échantillonnage reflète la population adulte selon les données du recensement et pour fournir des résultats représentatifs de l'ensemble de la population. La précision des sondages en ligne d'Ipsos est mesurée au moyen d'un intervalle de crédibilité. Dans ce cas, les résultats du sondage se situent à plus ou moins 3,5 points de pourcentage (19 fois sur 20) de ce qu'ils auraient été si tous les adultes canadiens avaient pris part au sondage. L'intervalle de crédibilité sera plus large parmi les sous-ensembles de la population. Tous les sondages et toutes les enquêtes sur échantillons peuvent être sujets à d'autres sources d'erreur, notamment des erreurs de couverture et de mesure.

Contact

Pour obtenir de plus amples renseignements sur cette étude, veuillez communiquer avec Sean Simpson, Vice-président, Affaires publiques, Ipsos au numéro (416) 324-2002 ou à l'adresse *sean.simpson@ipsos.com*

Ipsos
Ipsos est le chef de file canadien en matière d'information commerciale et le fournisseur principal du pays en matière de recherche sur l'opinion publique. L'entreprise exerce ses activités dans huit villes et elle emploie plus de 600 professionnels de recherche et employés de soutien au Canada. L'entreprise dispose du plus vaste réseau de centres d'appels du Canada, et des plus grands panels pré-recrutés, composés de foyers ou de répondants en ligne. Le personnel des études de marché canadiennes et des pratiques liées aux affaires publiques d'Ipsos est constitué de conseillers de recherche expérimentés ayant une vaste expérience de l'industrie. Ces pratiques offrent le meilleur ensemble d'outils de recherche du Canada, qui permet aux clients d'obtenir une information pertinente, à partir de laquelle ils peuvent agir. Ipsos est une entreprise du groupe Ipsos, chef de file mondial des études par enquêtes. Pour en savoir davantage, visitez *www.ipsos.ca*

ESET Canada
Depuis plus de 25 ans, ESETMD est un chef de file dans le développement de logiciels de sécurité à l'intention des entreprises et des consommateurs du monde entier. Ses solutions de sécurité couvrent une vaste gamme de besoins, de la protection des appareils mobiles et des points d'entrée à l'authentification à deux facteurs, en passant par le chiffrement. Les produits hautement performants d'ESET sont faciles à utiliser et procurent aux consommateurs et aux entreprises une tranquillité d'esprit qui leur permet d'exploiter le plein potentiel de leur technologie. Jour et nuit, ESET protège et surveille discrètement vos appareils et met à jour vos outils de défense en temps réel pour assurer la protection des utilisateurs et le fonctionnement ininterrompu de l'entreprise.

En 2015, ESET a ouvert un nouveau bureau à Toronto, le plus grand pôle technologique du Canada. Ce bureau s'ajoute au centre de recherche d'ESET de Montréal afin de mieux répondre à la demande des clients de l'ensemble du Canada.

Pour obtenir plus d'information, visitez le site *www.eset.com* et consultez le blogue d'ESET à l'adresse *www.welivesecurity.com* pour prendre connaissance de nouvelles études ou commentaires sur les tendances actuelles et les questions relatives à la cybersécurité.

Les produits d'affaires ESET sont offerts par un vaste réseau de partenaires revendeurs qui s'étend à l'ensemble du Canada et de l'Amérique du Nord. Les produits destinés aux consommateurs sont offerts dans les magasins Best Buy, Bureau en gros, London Drugs et en ligne sur *www.eset.com*

Si vous désirez parler à un représentant d'ESET afin de discuter des besoins liés à la sécurité de votre entreprise, faire un essai personnalisé d'un produit ou assister à une démonstration, veuillez communiquer avec nous par téléphone au (416) 637-1465 ou par courriel à *james.chalmers@eset.ca* directeur des partenaires et des alliances d'ESET Canada.