NOTE DE RECHERCHE
Février 2021

FÉDÉRATION CANADIENNE DE L'ENTREPRISE INDÉPENDANTE
En affaires pour vos affaires.

LES PME ET LA FRAUDE INFORMATIQUE

Comment les PME canadiennes font face à la cyberfraude durant la pandémie

Andreea Bourgeois, analyste principale

La pandémie continue d'avoir de lourdes répercussions sur les PME. L'impact négatif des fermetures obligatoires et des restrictions de santé publique a pu être atténué, dans une certaine mesure, par l'intégration de la technologie. Pour s'adapter à la nouvelle réalité, un certain nombre de PME se sont tournées vers la technologie et le télétravail. Ce changement les a toutefois exposées aux cyberattaques. D'après les recherches de la FCEI, une entreprise sur vingt en a été victime au Canada au cours des six derniers mois. Ce rapport montre notamment que les chefs de PME ont dépensé en moyenne 6 700 $ depuis mars pour sécuriser leurs systèmes informatiques afin de mieux protéger leur entreprise contre les cyberattaques durant la pandémie.

Qu'est-ce qu'une cyberattaque visant une entreprise?

Une cyberattaque est une tentative de piratage ou d'atteinte d'un système informatique, ou de vol par Internet d'argent ou des données d'un ordinateur. On recense plusieurs types de cyberattaques, notamment les logiciels malveillants (maliciels, logiciels espions), l'arnaque par courriel, l'hameçonnage et la fraude du faux fournisseur, qui visent à tromper les chefs d'entreprise pour qu'ils virent de l'argent sur le compte bancaire de l'escroc en pensant payer un fournisseur. Dans le présent rapport, les termes *cyberattaque* et *cyberfraude* sont utilisés de façon interchangeable.

Cyberattaques : une source d'inquiétude croissante durant la pandémie

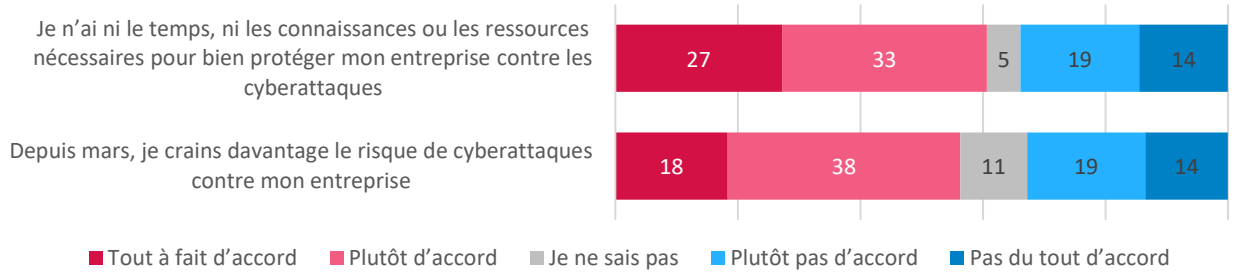
La cyberfraude qui frappe les entreprises a fait l'objet d'un certain nombre de recherches, mais celles-ci portent surtout sur les grandes entreprises et datent presque toutes d'avant la pandémie[1]. Les données les plus récentes de Statistique Canada sur le sujet concernent les entreprises d'au moins dix employés. Le présent rapport cherche à combler cette lacune en s'intéressant principalement aux cyberattaques qui ont touché les plus petites entreprises pendant la pandémie et à leurs effets, entre mars et octobre 2020. Ce rapport estime également le coût financier des investissements réalisés par les PME pour protéger leurs systèmes informatiques contre les cyberattaques, lequel s'avère rédhibitoire pour bon nombre d'entre elles.

La pandémie a clairement changé la donne pour les entreprises à bien des égards. Les gouvernements ont publié des listes d'entreprises essentielles et non essentielles, ce qui a changé la façon de servir les clients et de recevoir des paiements. La technologie a permis à certains chefs d'entreprise de composer un tant soit peu avec les fermetures obligatoires à grande échelle, mais elle a aussi suscité chez eux de nouvelles inquiétudes face au risque de cyberattaques. La fraude informatique peut leur causer du stress, en plus de leur faire perdre du temps, de l'argent, des produits, des services ou des informations précieuses, telles que des bases de données ou des renseignements bancaires.

Le tout dernier sondage sur les cyberattaques effectué par la Fédération canadienne de l'entreprise indépendante (FCEI) montre que 56 % des PME craignent davantage le risque de cyberattaques depuis mars 2020 (Figure 1). C'est encore plus vrai pour les petits employeurs qui ont pu adopter le télétravail, deux tiers d'entre eux s'inquiétant de ce risque. De nombreux chefs d'entreprise ne peuvent se permettre de se faire escroquer parce que leurs marges bénéficiaires sont très minces. Ils sont deux tiers à dire ne pas avoir le temps, les connaissances ou les ressources nécessaires pour protéger leur entreprise contre les cyberattaques, ce qui les rend encore plus vulnérables aux fraudeurs.

Figure 1

Dans quelle mesure êtes-vous d'accord ou pas d'accord avec les énoncés suivants (% des réponses)



1. Statistique Canada, *Le Quotidien*, 20 octobre 2020, *Environ un cinquième des entreprises canadiennes ont été touchées par des incidents de cybersécurité en 2019*, résultats d'un sondage national mené de janvier à mars 2020, Ottawa. Composante du produit nº 11-001-X au catalogue de Statistique Canada [PDF]. [En ligne] www150.statcan.gc.ca/n1/en/daily-quotidien/201020/dq201020a-fra.pdf?st=p-qG4DO2 (Page consultée le 4 novembre 2020).

Méthodologie

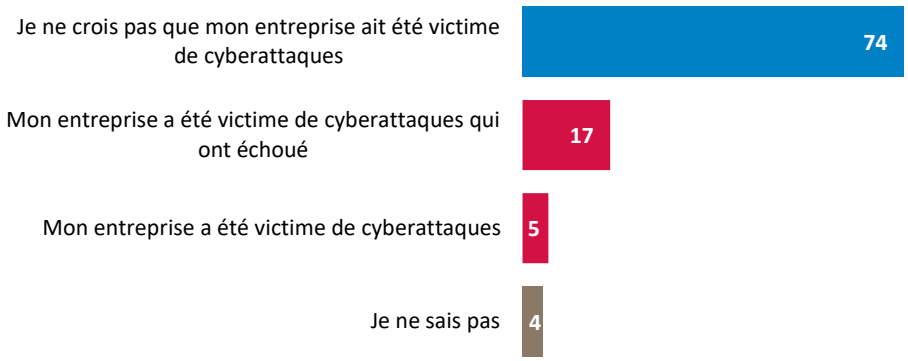
La FCEI a mené le sondage ***Votre entreprise face aux cyberattaques*** du 15 au 29 octobre 2020 auprès de ses membres, propriétaires de PME de tous les secteurs et de toutes les régions du Canada. Ce sondage en ligne a généré 3 040 réponses. La marge d'erreur était de ± 1,8 point de pourcentage, 19 fois sur 20. Les résultats détaillés sont présentés à l'Annexe A.

Impact de la cyberfraude sur les PME pendant la pandémie

Bien qu'environ les trois quarts des PME canadiennes n'aient pas subi de fraude informatique au cours des six derniers mois, près d'une sur six a fait l'objet de cyberattaques qui ont échoué et une sur vingt en a été victime (Figure 2). Si on extrapole ces résultats à l'ensemble de l'économie en se basant sur le pourcentage d'entreprises qui ont fait l'objet de cyberattaques, cela se traduit par environ 61 000 PME victimes de fraude[2].

Figure 2

Parmi les situations suivantes concernant les cyberattaques, quelles sont celles que votre entreprise a vécues depuis mars 2020? (% des réponses)



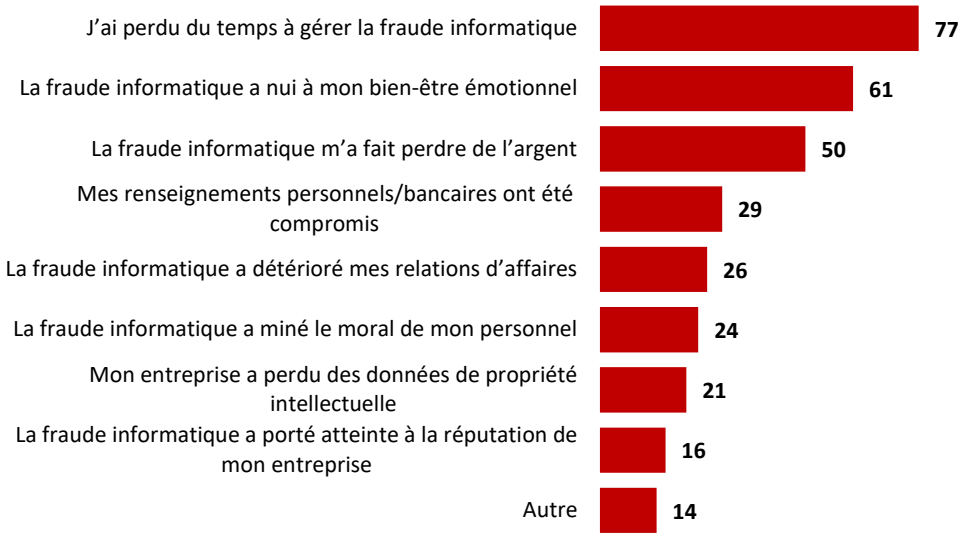
Les préjudices causés par la fraude informatique ne se limitent pas aux pertes financières. Les principaux coûts cachés qui en découlent se comptent en temps investi pour gérer la situation, sans oublier le stress que ce type de fraude génère chez les propriétaires (Figure 3). Lorsqu'une entreprise fait l'objet d'une cyberattaque, le propriétaire doit s'occuper du problème, ce qui l'oblige à délaisser le travail qu'il doit faire pour assurer la productivité de son entreprise. Trois quarts des victimes de cyberattaques déclarent avoir perdu du temps, et près des deux tiers disent avoir subi un stress additionnel. Par ailleurs, une victime sur deux fait état de pertes financières résultant directement de cyberattaques survenues depuis mars. Ces pertes d'argent s'ajoutent aux baisses de revenus que les petites entreprises subissent déjà à cause de la pandémie, ce qui rend la situation encore plus difficile pour elles.

2. Source : Calculs de la FCEI établis en extrapolant des données de sondage au nombre de PME au Canada basé sur le tableau Nombre d'entreprises canadiennes, avec employés, juin 2021 de Statistique Canada. [En ligne] (Page consultée le 11 janvier 2021).

Les entreprises qui œuvrent dans les secteurs de la construction, de la fabrication ou de la vente en gros et qui ont permis à leurs employés de travailler à distance ou ont modifié leur présence en ligne sont deux fois plus susceptibles d'être victimes de fraude informatique (10 % en moyenne, contre 5 % pour l'ensemble des répondants).

Figure 3

Quels autres effets la fraude informatique a-t-elle eus sur vous ou votre entreprise depuis mars? (% des réponses)



Tout comme l'a montré le sondage de la FCEI sur la cyberfraude effectué en 2015, les entreprises du secteur du commerce de gros ont le plus de risques de subir des cyberattaques. Les grossistes tendent à avoir davantage de fournisseurs et une clientèle variée et à utiliser une multitude de moyens pour communiquer avec eux. En plus des courriels, la technologie est largement utilisée dans ce secteur pour les paiements, les commandes, etc., d'où le risque élevé de cyberattaques auquel il est exposé (Tableau 1).

Les entreprises d'au moins 20 employés risquent également plus de faire l'objet de cyberattaques. Les employés d'entreprises de cette taille sont plus nombreux à être connectés à un réseau ou à accepter et traiter des commandes et des paiements, ce qui explique que ces entreprises aient davantage de points d'accès qui les exposent aux risques de cyberattaques.

Tableau 1

Les entreprises les plus susceptibles d'être victimes de fraude ou de tentative de fraude, selon la taille de l'entreprise et le secteur

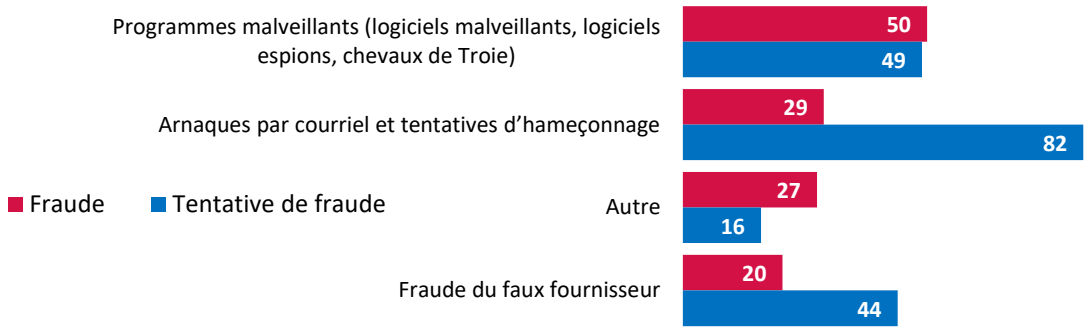
	Tentatives de fraude	Fraude avérée
Par taille	Entreprises d'au moins 20 employés	Entreprises d'au moins 20 employés
Par secteur	Entreprises des secteurs de la fabrication, du commerce de gros, des services professionnels et des services aux entreprises	Entreprises des secteurs de la construction, de la fabrication, du commerce de gros, des transports et des services aux entreprises

Les types de fraude informatique les plus fréquents

La fraude informatique se présente sous de nombreuses formes. Les programmes malveillants (p. ex. maliciels, logiciels espions, chevaux de Troie) sont de loin le type de pratiques frauduleuses le plus courant ***entraînant une perte*** pour une PME sur deux qui en est victime (Figure 4). Il existe d'autres types de fraude, comme les tentatives d'hameçonnage et les courriels frauduleux, qui visent par la ruse à amener les propriétaires d'entreprise à fournir des renseignements sensibles ou à virer des fonds. Les arnaques par courriel et les tentatives d'hameçonnage sont les types de fraude les plus utilisés dans environ 82 % des cas, et 30 % des PME approximativement en ont été victimes. Quant à la fraude du faux fournisseur, qui consiste à tromper la victime pour qu'elle vire de l'argent sur le compte d'un escroc, elle touche un chef d'entreprise sur cinq à peu près.

Figure 4

Types de tentatives de cyberfraude et types de cyberfraude subie par les PME pendant la pandémie (% des réponses)



Les PME et la prévention contre la cyberfraude

Nos données de sondage montrent que les chefs de PME ont dépensé en moyenne 6 700 $[3] dans des outils de sécurité des TI destinés à protéger leur entreprise des risques de cyberfraude durant la pandémie. Cela comprend le fait de passer d'une version gratuite d'un logiciel à une version payante, d'investir dans des logiciels de sécurisation des systèmes, de recourir davantage aux services d'un consultant de TI externe qu'ils utilisaient déjà, de rallonger les heures de travail de leur personnel des TI ou de fournir une formation additionnelle à leurs employés en matière de cybersécurité.

Malgré la situation difficile dans laquelle les chefs de PME se trouvent depuis mars, environ 33 % ont fait des investissements supplémentaires pour protéger leur entreprise contre la fraude (Figure 5). Ceux qui ont investi dans de nouvelles technologies ou ont fait des mises à niveau ont

3. La question exacte du sondage se trouve à l'Annexe.

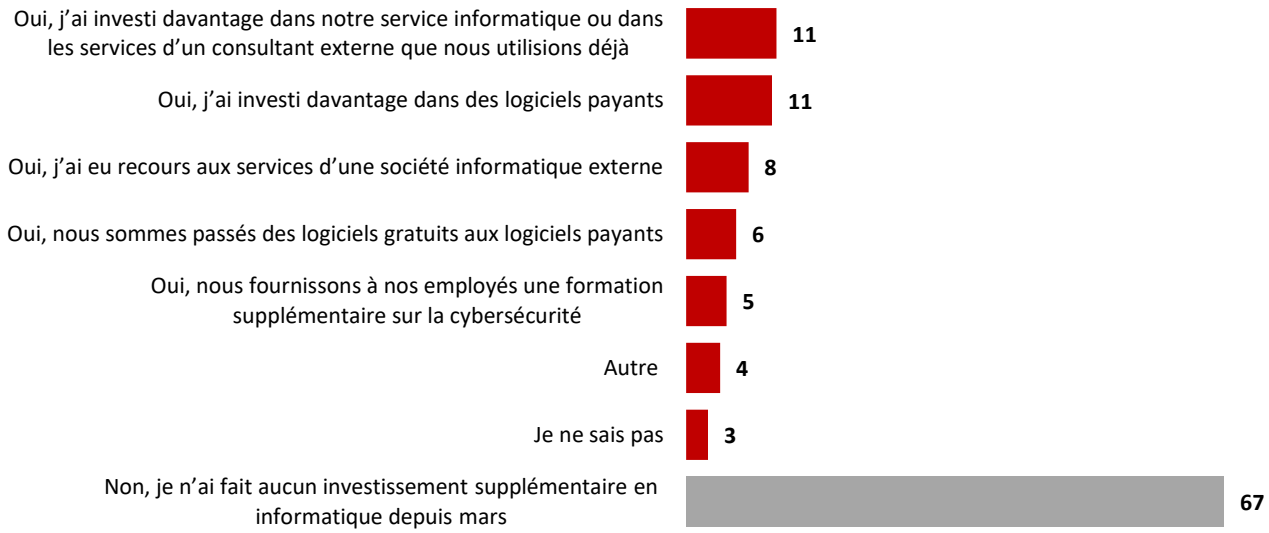
majoritairement choisi d'acquérir des logiciels payants, de renforcer leur service des TI ou de recourir davantage aux services de consultation externe qu'ils utilisaient déjà.

Par ailleurs, les firmes qui ont déjà subi des cyberattaques sont plus susceptibles de faire des investissements pour améliorer la technologie qu'elles utilisent afin de se protéger. Il n'est pas surprenant de voir que les PME qui ont modifié leurs activités en ligne depuis mars (p. ex. création d'un site Web, acceptation des paiements électroniques, des commandes ou des réservations par Internet) ont eu davantage tendance à faire des investissements additionnels en technologie.

Quels que soient les investissements supplémentaires que les PME font pour se protéger contre les cyberattaques, les outils employés ne sont peut-être pas sûrs à 100 %. De plus, en cas de fraude, les PME ont malheureusement peu de voies de recours. Une cyberassurance peut toutefois les protéger contre certains risques liés à Internet, comme l'atteinte à la sécurité des données.

Figure 5

Depuis le mois de mars, avez-vous fait des investissements supplémentaires en informatique autres que ceux que vous faites d'habitude afin de protéger vos systèmes? (% des réponses)



Malheureusement, quels que soient les investissements supplémentaires que les PME font pour se protéger contre les risques de cyberattaques, peu de recours s'offrent à elles en cas de fraude. Une cyberassurance peut toutefois les protéger contre les risques liés à Internet, comme l'atteinte à la sécurité des données.

Qu'est-ce qu'une cyberassurance?

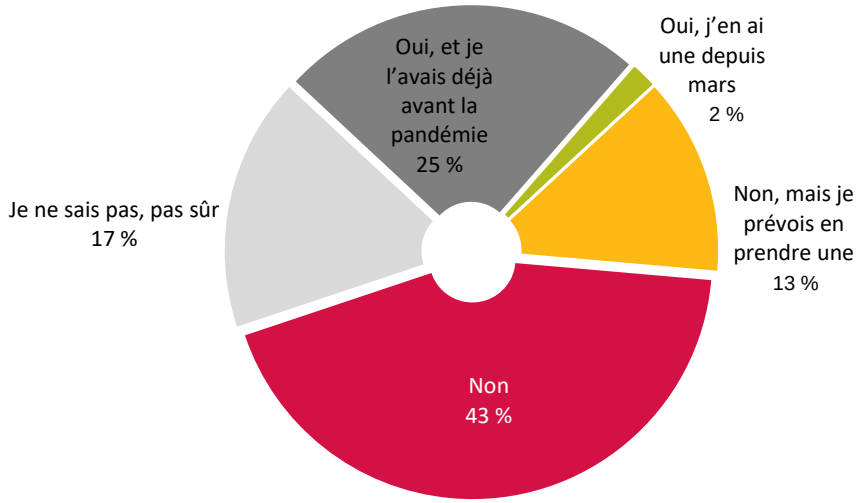
Une cyberassurance est un produit d'assurance destiné aux entreprises qui couvre la responsabilité découlant de l'utilisation des ordinateurs et des réseaux informatiques dans le cas de vol de données privées, de la transmission de virus informatiques et de la violation des marques commerciales ou du droit d'auteur[4].

La cyberassurance couvrant les cyberrisques est un produit relativement nouveau et en constante évolution[5]. Ce type d'assurance peut couvrir les frais de défense pour les procédures réglementaires, les frais juridiques et pénalités civiles, les frais de gestion en cas de crise, les frais de restauration des données électroniques et des programmes informatiques, les frais liés à l'interruption des activités commerciales, etc. À l'heure actuelle, environ 60 % des entreprises n'ont pas d'assurance cyberrisques bien que 13 % envisagent d'en souscrire une dans un avenir proche (Figure 6). À peu près un quart d'entre elles étaient couvertes par une cyberassurance avant mars 2020[6]. À noter, par ailleurs, qu'une poignée d'entreprises (2 %) ont pris une police d'assurance cyberrisques malgré les conditions économiques difficiles (Figure 6).

Les secteurs du commerce de gros, de la finance, de la location à bail et de l'immobilier, et des services professionnels sont ceux qui se procurent le plus fréquemment une cyberassurance. Les entreprises qui ont été victimes de cyberattaques et celles qui ont dû passer à la vente en ligne ou exiger le télétravail durant la pandémie sont également plus susceptibles d'avoir une cyberassurance.

Figure 6

Avez-vous une assurance cyberrisques pour votre entreprise? (% des réponses)



4. Définition traduite librement vers le français et basée sur le Merriam-Webster's Law Dictionary (en anglais seulement), Merriam-Webster. [En ligne] (Page consultée le 5 novembre 2020).
5. Bureau d'assurance du Canada, 2020 (en anglais seulement). [En ligne] Protect your organization from cyber crime (ibc.ca) (Page consultée le 24 novembre 2020).
6. FCEI, sondage sur la cybersécurité, octobre 2019 à janvier 2020, 2 778 réponses, données pour le Canada, marge d'erreur de ± 1,8 %, 19 fois sur 20. La question 14 montre que 28 % des répondants ont une assurance cyberrisques.

Conclusion

La fraude informatique est une source de préoccupation croissante pour quantité de PME, surtout pour celles qui commercialisent à présent leurs produits ou leurs services en ligne. Durant la pandémie, environ 61 000 PME ont fait l'objet de cyberattaques, en particulier celles qui œuvrent dans les secteurs de la vente en gros, de la fabrication et de la construction, celles qui se sont adaptées plus rapidement à la situation et qui ont fait le virage numérique ou ont permis le télétravail.

Les pertes et les coûts associés à la cyberfraude peuvent être considérables et les chances de récupérer les données ou l'argent volés sont faibles. Les propriétaires de PME ont dépensé en moyenne 6 700 $ pour mieux protéger leurs systèmes informatiques afin d'assurer la survie de leur entreprise pendant la pandémie.

Étant donné que la deuxième vague de COVID-19 touche de nombreuses régions canadiennes et que les gouvernements ont imposé de nouvelles fermetures d'entreprises, la technologie va continuer de jouer un rôle plus important dans le fonctionnement des entreprises. Dans la circonstance, connaître les risques, investir dans des outils technologiques bien adaptés et étudier les avantages de la cyberassurance sont les meilleurs moyens qu'ont les PME pour se protéger contre la fraude.

Meilleures pratiques et recommandations

Pour les propriétaires de PME

La FCEI formule les recommandations suivantes à l'intention des propriétaires de PME afin de les aider à protéger leur entreprise contre la cyberfraude :

- **Se tenir informé** des cyberrisques auxquels sont exposées les entreprises en consultant le site Web du Bureau d'assurance du Canada (en anglais seulement), la page Cybersécurité du gouvernement du Canada (sécurité nationale et défense), le site et les ressources de la FCEI et ceux d'autres associations professionnelles.
- **Sensibiliser les employés** à la cyberfraude et les former pour qu'ils sachent comment la détecter et la contrer.
- **Partager l'information** sur les arnaques et les meilleures pratiques en matière de prévention avec d'autres propriétaires de PME au sein de la communauté, que ce soit directement ou par le biais d'associations professionnelles.
- Évaluer les avantages d'avoir une **cyberassurance** pour l'entreprise. Le Bureau d'assurance du Canada met à la disposition des chefs d'entreprise des renseignements utiles sur les cyberrisques et la cyberassurance (en anglais seulement).

- **Signaler les cas de cyberfraude** à la police ou à d'autres autorités, comme le Centre antifraude du Canada, le Bureau de la concurrence ou le Bureau d'éthique commerciale (Office de Certification Commerciale du Québec).

Pour les gouvernements, les forces de l'ordre et d'autres autorités

La FCEI émet les recommandations suivantes à l'intention des gouvernements, des forces de l'ordre et d'autres autorités (banques, compagnies d'assurance, etc.) pour les inciter à prévenir la fraude dont font l'objet les PME du Canada :

- **S'assurer d'avoir des ressources adéquates à la lutte contre la cybercriminalité** et publier annuellement les résultats, notamment les statistiques présentant un intérêt pour les PME.
- **Compenser une partie des investissements réalisés dans de l'équipement et des programmes de protection** en accordant aux PME des incitatifs financiers (p. ex. des crédits d'impôt).
- **Informer de façon proactive** les entreprises et les associations professionnelles au sujet des ressources disponibles et des meilleures pratiques en matière de prévention.
- Offrir des **services adaptés tout spécialement aux PME** en ce qui concerne la cyberassurance et les cyberattaques.

Annexe A

Résultats du sondage – *Votre entreprise face aux cyberattaques*

Méthode d'enquête : *Web*
Période de sondage : *15 octobre – 2 novembre 2020*
Date de la mise en tableaux : *2 novembre 2020*
Total des réponses : *3 040*
À titre de comparaison, pour un échantillon probabiliste ayant un nombre égal de répondants, la marge d'erreur serait de plus ou moins [1,8] %, 19 fois sur 20.

% des réponses :

1. Depuis mars 2020, est-ce que la majorité de vos employés ont réussi à accomplir certaines ou la plupart de leurs tâches principales en télétravail (travail à domicile)? (Sélectionner une seule réponse)

12,6 Oui, la majorité de mes employés ont réussi à accomplir *la plupart* de leurs tâches principales en télétravail
7,8 Oui, la majorité de mes employés ont réussi à accomplir *certaines* de leurs tâches principales en télétravail
79,6 Non, la majorité de mes employés ne font pas de télétravail

2. Dans quelle mesure avez-vous changé votre *gamme* d'activités commerciales *en ligne* (commandes par Internet avec récupération des marchandises en personne, paiements ou réservations en ligne, etc.) depuis mars 2020? (Sélectionner toutes les réponses pertinentes)

66,6 Aucun changement *Ne peut être combiné*
4,1 Nous avons créé un site Web pour notre entreprise pour la première fois
9,8 Nous avons commencé à accepter les commandes en ligne
3,4 Nous avons commencé à accepter les réservations en ligne
11,5 Nous avons commencé à accepter les paiements en ligne
14,1 Autre (préciser)
1,6 Je ne sais pas *Ne peut être combiné*

3. Dans quelle mesure êtes-vous d'accord ou pas d'accord avec les énoncés suivants? (Sélectionner une réponse par ligne)

	Tout à fait d'accord	Plutôt d'accord	Plutôt pas d'accord	Pas du tout d'accord	Je ne sais pas
Depuis mars, je crains davantage le risque de *cyberattaques* contre mon entreprise	*18,3*	*38,0*	*19,2*	*13,5*	*11,0*
Je n'ai ni le temps, ni les connaissances ou les ressources nécessaires pour bien protéger mon entreprise contre les cyberattaques	*27,2*	*33,4*	*19,4*	*14,5*	*5,5*

4. Parmi les situations suivantes concernant les *cyberattaques*, quelles sont celles que votre entreprise a vécues depuis mars 2020? (Sélectionner toutes les réponses pertinentes)

a. *4,9* Mon entreprise a été victime de cyberattaques (j'ai perdu de l'argent, des produits/services ou des données importantes)
b. *16,9* Mon entreprise a été victime de cyberattaques qui ont échoué (je n'ai pas perdu d'argent, de produits/services ou de données importantes)
c. *74,9* Je ne crois pas que mon entreprise ait été victime de cyberattaques *Ne peut être combiné* *Passer à la Q8*
d. *4,1* Je ne sais pas/pas sûr *Ne peut être combiné* *Passer à la Q8*

Si Q4 = b poser la Q5

5. Depuis mars 2020, quels types de cyberattaques (tentatives de fraude) votre entreprise a-t-elle déjà subis? (Sélectionner toutes les réponses pertinentes)

50,1 Programmes malveillants (logiciels malveillants, logiciels espions, chevaux de Troie)
83,0 Arnaques par courriel et tentatives d'hameçonnage (c'est-à-dire des courriels frauduleux visant à vous amener à fournir des renseignements personnels/bancaires ou à transférer de l'argent)
44,7 Fraude du faux fournisseur (c'est-à-dire qu'un fraudeur ayant usurpé l'identité d'un de vos fournisseurs vous demande de virer de l'argent sur un compte factice)
16,4 Autre (préciser)

Si Q4 = a, poser la Q6

6. **Depuis mars 2020, quels types de cyberattaques *ont fait perdre* à votre entreprise de l'argent, des produits, des services ou des renseignements importants?**
(Sélectionner toutes les réponses pertinentes)

53,4 Programmes malveillants (logiciels malveillants, logiciels espions, chevaux de Troie) *Ne peut être combiné*
30,8 Arnaques par courriel et tentatives d'hameçonnage (c'est-à-dire des courriels frauduleux visant à vous amener à fournir des renseignements personnels/bancaires ou à transférer de l'argent)
21,8 Fraude du faux fournisseur (c'est-à-dire qu'un fraudeur ayant usurpé l'identité d'un de vos fournisseurs vous demande de virer de l'argent sur un compte factice)
29,3 Autre (préciser)

7. **Quels autres effets la fraude informatique a-t-elle eus sur vous ou votre entreprise depuis mars?** (Sélectionner toutes les réponses pertinentes)

21,3 Mon entreprise a perdu des données de propriété intellectuelle (p. ex. la base de données commerciales) *Ne peut être combiné*
30,1 Mes renseignements personnels/bancaires ont été compromis
78,7 J'ai perdu du temps à gérer la fraude informatique
26,5 La fraude informatique a détérioré mes relations d'affaires (avec des clients, des fournisseurs)
16,2 La fraude informatique a porté atteinte à la réputation de mon entreprise
24,3 La fraude informatique a miné le moral de mon *personnel*
62,5 La fraude informatique a nui à *mon* bien-être émotionnel (stress)
50,7 La fraude informatique m'a fait perdre de l'argent
14,0 Autre (préciser)

8. **Depuis le mois de mars, avez-vous fait des investissements *supplémentaires* en informatique autres que ceux que vous faites d'habitude afin de protéger vos systèmes?** (Sélectionner toutes les réponses pertinentes)

67,5 Non, je n'ai fait aucun investissement supplémentaire en informatique depuis mars *Ne peut être combiné* *Passer à la Q10*
6,3 Oui, nous sommes passés des logiciels *gratuits* aux logiciels *payants*
10,8 Oui, j'ai investi davantage dans des logiciels payants
7,8 Oui, j'ai eu recours aux services d'une société informatique externe
11,3 Oui, j'ai investi davantage dans notre service informatique interne ou dans les services d'une société/consultant informatique externe que nous utilisions déjà
5,1 Oui, nous fournissons à nos employés une formation supplémentaire sur la cybersécurité
4,3 Autre (préciser)
2,8 Je ne sais pas/pas sûr *Ne peut être combiné* *Passer à la Q8*

9. **Depuis mars 2020, quels investissements supplémentaires avez-vous dû faire pour sécuriser vos systèmes informatiques (logiciel antivirus, formation, société/consultant informatique externe) ?** (Entrer un montant approximatif).

Les résultats sont calculés en excluant les réponses de moins de 100 $ ou de plus de 50 000 $.

Moyenne de *6 700 $*

10. **Veuillez nous donner plus de précisions sur les cyberattaques que vous avez subies depuis mars 2020.**

11. **Avez-vous une *assurance cyberrisques* pour votre entreprise?** (Sélectionner une seule réponse)

24,5 Oui, et je l'avais déjà avant la pandémie
1,7 Oui, j'en ai une depuis mars
13,2 Non, mais je prévois en prendre une
43,5 Non
17,1 Je ne sais pas/pas sûr

« Cyberattaques »
Cyberattaques : Une cyberattaque est toute tentative visant à endommager un système informatique, à voler des données ou à voler de l'argent par Internet.

« Assurance cyberrisques »
Assurance cyberrisques : Produit d'assurance qui protège les entreprises et les particuliers contre les risques liés à Internet, par exemple les atteintes à la sécurité des données.