

LE PAYSAGE CHANGEANT DE LA CYBERSÉCURITÉ SUITE À LA PANDÉMIE DE COVID-19

RÉSULTATS DE L'ENQUÊTE
CANADIENNE SUR LA
CYBERSÉCURITÉ ET LE
CYBERCRIME (ECCC)

PRÉSENTÉE PAR BANA AMMBA



Statistics
Canada

Statistique
Canada

Canada



DANS CETTE PRÉSENTATION

1. À PROPOS DE L'ENQUÊTE
2. LA COLLECTE DE DONNÉES
3. ANALYSE ET TENDANCES
4. ACCÈS AUX DONNÉES



Statistics
Canada

Statistique
Canada

Canada



À PROPOS DE L'ENQUÊTE



Statistics
Canada

Statistique
Canada

Canada



ENQUÊTE CANADIENNE SUR LA CYBERSÉCURITÉ ET LE CYBERCRIME (ECCC)

APERÇU

- L'**ECCC** est une enquête-entreprise, qui recueille des informations concernant :
 - Les mesures de cybersécurité
 - Les types d'incidents de cybersécurité
 - Les coûts associés à la prévention et au rétablissement des incidents de cybersécurité
- L'enquête est menée la Division de l'organisation industrielle et des finances (DOIF) de Statistique Canada.
- Parrainée par **Sécurité publique Canada**
- La dernière itération couvre l'année de référence **2021**
 - Itérations précédentes : 2017, 2019



POPULATION CIBLE ET BASE DE SONDAGE

ECCC 2021

La population de l'ECCC provient du Registre des entreprises (RE) de Statistique Canada.



Enquête-entreprise couvrant les entreprises de **10 employés et plus**



L'échantillon comprend les entreprises dans presque tous les secteurs



Taille de la population cible de **188 359** entreprises
Taille de l'échantillon final de **12 158**



Statistics
Canada

Statistique
Canada

Canada

LA COLLECTE ET LE TRAITEMENT DES DONNÉES



Statistics
Canada

Statistique
Canada

Canada

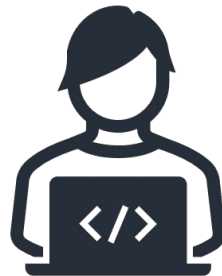


COLLECTE DES DONNÉES

ECCC 2021



La collecte des données s'est déroulée de janvier à mars 2022.



Les données ont été collectées au moyen d'un questionnaire électronique (QE) ou d'un interview téléphonique assisté par ordinateur (ITAO)



Taux de réponse de 73 %



Statistics
Canada

Statistique
Canada

Canada

TRAITEMENT DES DONNÉES : SAISIE ET VÉRIFICATION

Tout au long de la collecte, les données sont évaluées à l'aide de **règles logiques** et d'un **suivi par l'enquêteur**.

Après la collecte, une série complète d'étapes de traitement est entreprise, y compris la vérification et l'imputation (remplacement des données).



Après la collecte, divers types de « **vérifications** » sont effectués pour atténuer les différents types d'erreurs.

1. Erreurs dans le cheminement du questionnaire

Les vérifications éliminent automatiquement les données superflues en utilisant le cheminement logique du questionnaire.

2. Erreurs liées à l'absence de réponse

Les valeurs manquantes ont été complétées manuellement en utilisant les réponses aux questions connexes ou imputées.

3. Erreurs incluant des valeurs aberrantes

Les valeurs identifiées comme aberrantes ont également été



Statistics
Canada

Statistique
Canada

Canada

TRAITEMENT DES DONNÉES : IMPUTATION ET PONDÉRATION

Le processus de **pondération** permet de déterminer le nombre d'entreprises que chaque répondant « représentait » en plus de lui-même.

Exemple : Dans un échantillon aléatoire simple de 2 % d'une population de 100 000 entreprises, chaque entreprise de l'échantillon représente 50 entreprises de la population.



L'**imputation** remplace les informations invalides ou manquantes en utilisant les réponses de donneurs similaires au sein de l'échantillon. Elle est utilisée pour établir des enregistrements de données cohérents en interne.

Deux types de non-réponse, traités différemment :

1. **La non-réponse complète** : Les enregistrements sont abandonnés et pris en compte dans le processus de pondération.
2. **Non-réponse partielle** : Les réponses manquantes sont corrigées manuellement ou imputées



LIGNES DIRECTRICES SUR LA DIFFUSION DES INDICATEURS DE QUALITÉ

Le **ECDC** comporte **6 niveaux** d'indicateurs de qualité

- **A** (Excellent)
- **B** (Très bon)
- **C** (Bon)
- **D** (Acceptable)
- **E** (À utiliser avec précaution)
- **F** (Trop peu fiable pour être publié)

Cette lettre de qualité est déterminée en employant une formule qui tient compte de l'erreur-type, des taux d'imputation et des taux de réponse.



ANALYSE ET TENDANCES



Statistics
Canada

Statistique
Canada

Canada



LES CHANGEMENTS SOCIÉTAUX ACCÉLÉRÉS PAR LA PANDÉMIE DE COVID-19 ONT EU UN IMPACT SANS PRÉCÉDENT SUR LES ACTIVITÉS DES ENTREPRISES CANADIENNES.

- Selon l'Enquête sur la technologie numérique et l'utilisation d'Internet, de 2019 à 2021, davantage d'entreprises canadiennes ont réalisé des ventes par commerce électronique (+8 points de pourcentage) et ont offert à leurs employés la possibilité de télétravailler (+14 points de pourcentage).
- Une présence croissante en ligne créé de nouvelles opportunités, mais expose les entreprises à de nouveaux risques en matière de confidentialité, de protection des données et de cybersécurité.



Statistics
Canada

Statistique
Canada

Canada

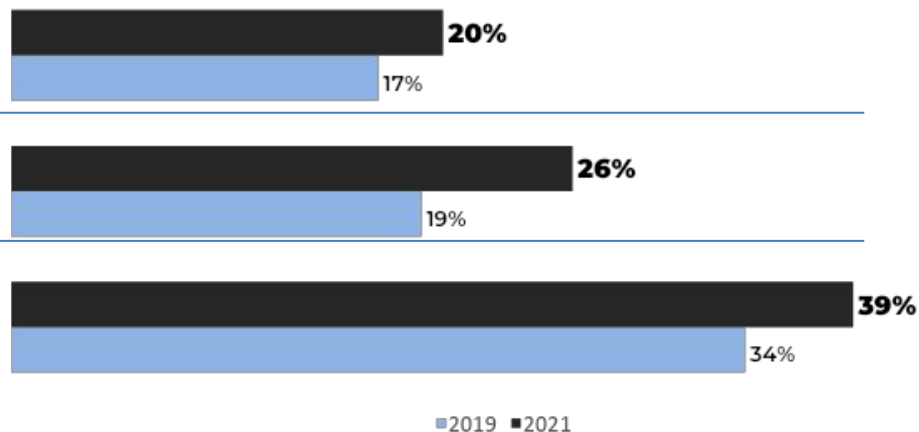


LES ENTREPRISES CANADIENNES DEVIENNENT DE PLUS EN PLUS SENSIBLE À LA CYBERSÉCURITÉ

L'erreur humaine est depuis longtemps reconnue comme une source majeure d'incidents de cybersécurité. Il est important d'accroître les connaissances de tous les employés en matière de cybersécurité pour améliorer la résilience de l'organisation.

% entreprises qui :

- Ont fourni une **formation** formelle de cybersécurité à des employés non informaticiens
- Disposaient de **politiques écrites** en matière de cybersécurité
- Ont mené des activités pour identifier les risques pour la cybersécurité selon un **horaire** précis



LES ENTREPRISES CANADIENNES DÉPENSENT DAVANTAGE POUR LA PRÉVENTION ET LA DÉTECTION DES INCIDENTS DE CYBERSÉCURITÉ

Les dépenses moyennes de prévention en 2021 s'élevaient à 52 000 \$.

Une augmentation substantielle de 46 % à partir de 2019 (supérieure au taux d'inflation de +4 % sur la même période)



Les grandes entreprises ont dépensé en moyenne 340 000 \$ de plus



Les petites entreprises ont dépensé 9 000 \$ de plus en moyenne

La protection des informations personnelles est la raison la plus fréquemment invoquée (66 %) pour justifier le temps ou l'argent consacrés à la cybersécurité.



Statistics
Canada

Statistique
Canada

Canada

18% des **entreprises** canadiennes ont déclaré avoir été touchées par des incidents de cybersécurité en 2021

↓ **3 points de pourcentage** à partir de 2019



En comparaison, selon l'**enquête canadienne sur l'utilisation d'Internet** :

70 % des **Canadiens** ont été confrontés à des incidents de cybersécurité en 2022

↑ **12 points de pourcentage** de 2020

Ces tendances peuvent refléter un changement dans les stratégies des cybercriminels, mais pourraient également être le résultat d'une plus grande disponibilité des outils permettant aux entreprises d'identifier et d'intercepter les activités malveillantes.



Statistics
Canada

Statistique
Canada

Canada





IMPACT FINANCIER Du CYBERCRIME

Les entreprises touchées par des incidents de cybersécurité en 2021 ont subi des conséquences financières plus graves qu'en 2019.

Coût moyen de la reprise après un incident

	2021	2019
Tous les entreprises	19 000 \$	11 000 \$
Grandes entreprises	172 000 \$	73 000 \$



Statistics
Canada

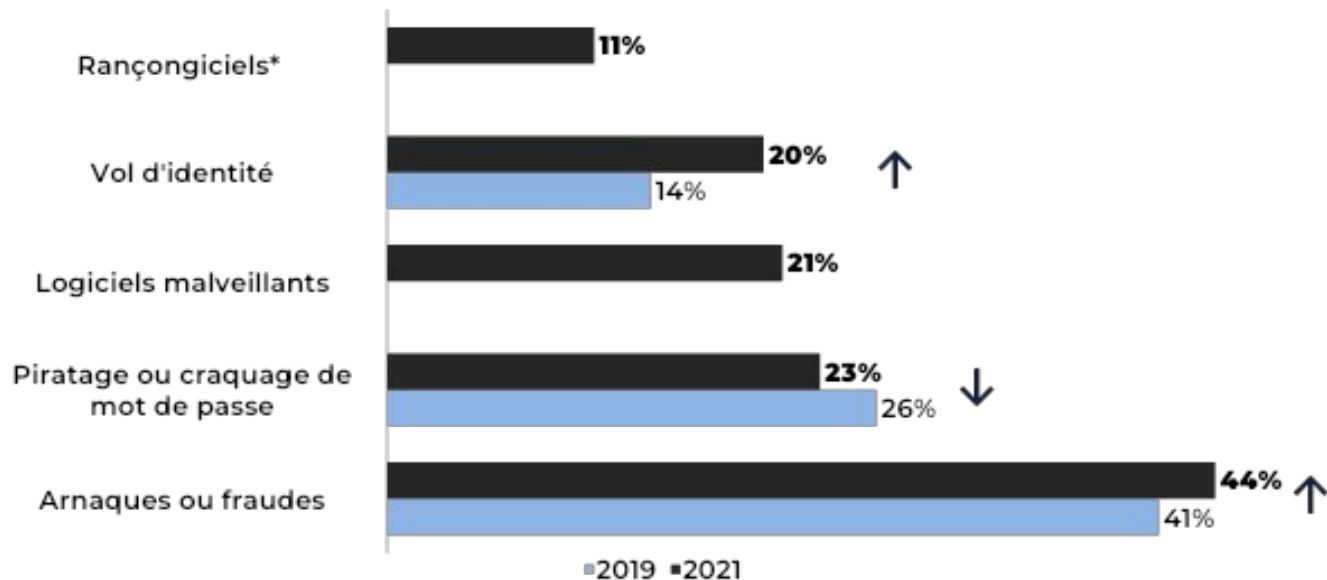
Statistique
Canada

Canada

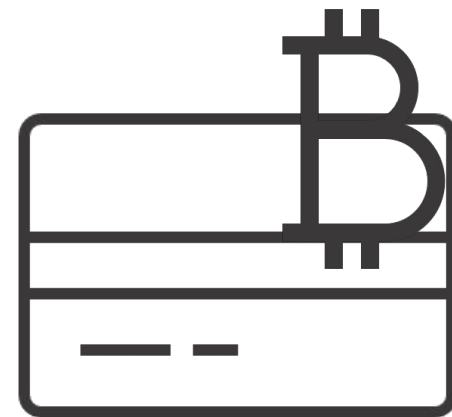


LES MÉTHODES UTILISÉES POUR COMMETTRE DES CYBERCRIMES

En % des entreprises touchées par des incidents de cybersécurité :



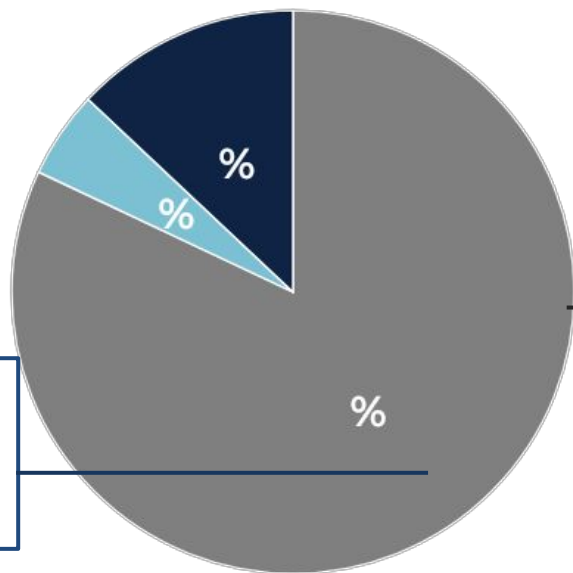
Environ **2 %** des entreprises canadiennes ont été touchées par un **rançongiciel** en 2021



En % des entreprises touchées par les rançongiciels :

N'a pas payé de rançon

Ne connaissaient pas la valeur des rançons payées ou ne savaient pas si un paiement avait été effectué.



A signalé une valeur pour les paiements de rançon effectués :

- La plupart des paiements étaient inférieurs à 100 000 \$
- 55 % payés en cryptomonnaie*



Statistics
Canada

Statistique
Canada

Canada

LES DÉFIS DE LA MESURE DES RANÇONGIERS



Les statistiques sur les rançongiciels du ECCC peuvent différer de celles d'autres sources pour diverses raisons : par exemple, la population cible (↑ PME), la réticence à déclarer, la présentation des données...

En ce qui concerne la présentation, par exemple : un rapport de la société de conseil Dragos a révélé une augmentation de **87 %** des attaques de rançongiciels contre les organisations industrielles en 2022

Toutefois, ce chiffre était basé sur des données qui montraient une augmentation absolue de seulement quelques centaines d'incidents au niveau mondial.

Au Canada, environ 2 % des entreprises ont été touchées par des incidents de cybersécurité, ce qui représente environ **4 000** entreprises.



Statistics
Canada

Statistique
Canada

Canada



PERPETRATEURS

d'incidents visant à voler de l'argent ou à exiger le paiement d'une rançon en 2021

Une partie
externe

71%
Pas de
changement
significatif

4%
+2 % pts

Un employé
interne

Fournisseur,
client ou
partenaire

9%
+8 % pts

24%
-7 % pts

Des entreprises
ne savaient pas



ACCÈS AUX DONNÉES



Statistics
Canada

Statistique
Canada

Canada



LES CENTRES DE DONNÉES DE RECHERCHE (CDR) DE STATISTIQUE CANADA



Ces centres encouragent et facilitent la recherche en utilisant les microdonnées de Statistique Canada dans des installations sécurisées gérées par Statistique Canada.



Les utilisateurs de données agréés sont considérés comme des employés de Statistique Canada et ont accès à une grande variété de données, y compris des enquêtes sociales et commerciales, des données administratives et des données couplées.



Les chercheurs universitaires affiliés à une institution partenaire peuvent bénéficier d'un accès gratuit lorsqu'ils mènent des recherches autonomes. L'université d'Ottawa est un partenaire principal.

Les chercheurs intéressés doivent soumettre une proposition de projet pour que l'accès soit approuvé. La proposition sera évaluée sur la base de plusieurs critères afin de déterminer si l'accès aux microdonnées est approprié pour le projet.



L'ENVIRONNEMENT DE FICHIERS COUPLABLES (EFC)

- L'Environnement de fichiers couplables (EFC) est un environnement de Statistique Canada dans lequel les microdonnées d'entreprises sont couplées à diverses sources de données administratives et d'enquêtes.
- L'EFC fournit un large éventail de bases de données permettant aux utilisateurs d'analyser les caractéristiques des entreprises canadiennes à travers de nombreuses variables sans imposer de charge de réponse supplémentaire aux entreprises.
- La participation au EFC est volontaire, de sorte que toutes les enquêtes de Statistique Canada auprès des entreprises n'y sont pas disponibles. Cependant, le ECCC est disponible.
- Étant donné que de nombreuses enquêtes incluses dans le EFC, y compris la ECCC, sont des enquêtes transversale par échantillon, certaines variables du EFC ne seront pas disponibles pour toutes les entreprises.
- Les chercheurs intéressés doivent indiquer dans leur proposition de projet les extractions prévues dans le cadre du EFC.



PRINCIPAUX CRITÈRES D'ÉVALUATION DU CDR

L'analyse est-elle axée sur une modélisation complexe des données, et pas uniquement sur des résultats descriptifs ou tabulaires ? Les chercheurs doivent justifier pourquoi les données agrégées sont insuffisantes pour ce qu'ils essaient de faire.

Les chercheurs doivent également fournir les dimensions des tableaux de données pour les résultats descriptifs/tabulaires et justifier comment ces tableaux soutiennent les résultats de la modélisation.

Les ensembles de données demandés sont-ils appropriés pour l'analyse proposée ?

Les chercheurs doivent fournir une liste spécifique des variables d'enquête qui seront examinées pour répondre aux questions de recherche, et fournir une explication des variables dépendantes/indépendantes dans la modélisation.

Les données contiennent-elles suffisamment d'observations pour protéger la confidentialité des personnes interrogées ? Les chercheurs doivent indiquer quelles sous-populations seront examinées, le cas échéant, afin que Statistique Canada puisse déterminer si la taille de l'échantillon est suffisante pour permettre la publication des données.



LISTE DES TABLEAUX DE DONNÉES ACTUELLEMENT DISPONIBLES

.....

# de tableau	Titre du tableau
22-10-0001-01	Mesures de cybersécurité mises en place par les entreprises par industrie et taille de l'entreprise
22-10-0056-01	Principales raisons pour lesquelles les entreprises consacrent du temps ou de l'argent à la cybersécurité par industrie et taille de l'entreprise
22-10-0076-01	Types d'incidents de cybersécurité touchant les entreprises par industrie et taille de l'entreprise
22-10-0078-01	Signalement des incidents de cybersécurité à un service de police par industrie et taille de l'entreprise
22-10-0129-01	Nombre d'employés qui accomplissent des tâches liées à la cybersécurité, par industrie et taille de l'entreprise
22-10-0131-01	Coût moyen de la prévention ou de la détection des incidents de cybersécurité par industrie et taille de l'entreprise
22-10-0132-01	Coût moyen pour se remettre d'incidents de cybersécurité par industrie et taille de l'entreprise
22-10-0133-01	Répercussions des incidents de cybersécurité sur les entreprises par industrie et taille de l'entreprise
22-10-0130-01	Utilisation des dispositions en matière de gestion des risques par industrie et taille de l'entreprise
22-10-0128-01	Utilisation de dispositifs personnels pour mener des activités commerciales, par industrie et taille de l'entreprise



LIENS POUR LA DÉMONSTRATION

Tableaux de données de Statistique Canada :

<https://www150.statcan.gc.ca/n1/fr/type/donnees>

**Page du Programme des centres de données de
recherche de Statistique Canada :**

<https://www.statcan.gc.ca/fr/microdonnees/centres-donnees>

Pour plus d'informations concernant le ECCC :

https://www23.statcan.gc.ca/imdb/p2SV_f.pl?Function=getSurvey&SDDS=5244



Statistics
Canada

Statistique
Canada



Statistics
Canada

Statistique
Canada

Canada



MERCI!

Bana Ammba

Economiste

Division de l'organisation et finances de l'industrie

Statistique Canada

bana.ammba@statcan.gc.ca



Statistics
Canada

Statistique
Canada

Canada