CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 5, Num. 3
2025

Mesurer la cybercriminalité: Canada, Australie, Royaume-Uni

Maya Dubord, candidate à la maîtrise en criminologie

Introduction

De nombreuses études portant sur la cybercriminalité au Canada et à l'international sont publiées chaque année, permettant de mettre en lumière **les tendances et les mesures de prévention mises en œuvre par les gouvernements et entreprises**. Toutefois, le taux de déclaration à la police des incidents de cybercriminalité et les distorsions qui y sont associées ont un impact important sur la qualité des analyses produites dans ces études [1]. En effet, **il est possible que des incidents ne puissent être qualifiés comme étant des cybercrimes par les organisations policières, malgré les conséquences importantes qu'ils peuvent avoir sur les victimes**, que des erreurs d'enregistrements telles que la présence de valeurs manquantes ou de doublons viennent invalider les sources de données, et que certains services de police n'enregistrent qu'un seul crime par victime d'un incident afin de limiter les risques de doublons. Ces limites aux données de source policière rendent difficile l'établissement d'un portrait global de la cybercriminalité, notamment en incluant les expériences de victimisation multiple [1].

Les données policières ne sont pas les seules statistiques portant sur la cybercriminalité disponible publiquement. Différents ministères et organisations publiques en publient régulièrement, ce qui dans chaque cas s'accompagne d'avantages et de lacunes. Il est donc nécessaire de comprendre la diversité des rapports statistiques portant sur la cybercriminalité et d'analyser leurs avantages et inconvénients [2]. Cette note de synthèse présente plusieurs rapports portant sur la cybercriminalité au Canada, en Australie et au Royaume-Uni. Une attention particulière est portée aux méthodes d'échantillonnage et d'analyse de chaque étude.

Canada

La prochaine sous-section présente les rapports sur la cybercriminalité au Canada.

<u>Programme de déclaration uniforme de la criminalité (DUC)</u>

Statistique Canada publie plusieurs rapports annuels qui diffusent des statistiques officielles portant sur la cybercriminalité trouvant leur source dans le **Programme de déclaration uniforme de la criminalité (DUC)** [2]. La DUC mesure **la fréquence des crimes au Canada à partir des signalements déclarés par les services de police partout au pays**. Ce programme a été mis en place en 1962 et est parrainé par le *Centre canadien de la statistique juridique sur les actes criminels déclarés par la police* (CCSJSC). La DUC ne représente pas l'ensemble des crimes commis sur le sol canadien puisqu'**elle ne recense que les infractions qui ont été déclarées à la poli-**

-**ce**. Depuis 2022, la Police militaire des Forces canadiennes s'est jointe au reste des services de police canadiens qui ont l'obligation de partager les données qu'ils collectent. Ce sont donc **plus de 150 services de police** qui participent au programme dont le **taux de réponse frôle les 100 %**.

Malgré un processus de vérification des doublons et des valeurs manquantes par le CCSJSC, **aucune vérification de l'exhaustivité ou de l'exactitude des données enregistrées n'est effectuée par un organisme externe aux services de police.** Il se peut donc que certaines informations ne soient pas collectées rigoureusement. De plus, en raison du processus d'enregistrement des incidents au sein de la DUC, **les crimes les moins graves tendent à être statistiquement sous-représentés** dans les bases de données.

Des rapports et des jeux de données tirant leurs informations de la DUC sont produits périodiquement par Statistique Canada. Les principaux résultats démontrent notamment la présence d'**une hausse de la cybercriminalité depuis cinq ans**. En 2019, le nombre d'affaires de cybercrime déclarées par la police s'élevait à 43 318 incidents. En 2023, il s'élevait plutôt à 93 068 incidents, soit **une hausse de 114,85%** [3]. Pour le Québec, en 2023, le taux de cybercrime déclaré par la police par 100 000 habitants était de 115,7 alors que le taux national se situait à 233,1 [3]. Pour la même année, **24 % des incidents de fraude déclarés ont été classés comme étant un cybercrime** [4].

Évaluation des cybermenaces nationales 2023-2024 (2022)

L'évaluation des cybermenaces nationales 2023-2024 est un rapport publié en 2022 par le Centre canadien pour la cybersécurité (CCC) et don l'objectif du rapport est de **prédire les tendances des cybermenaces contre les individus et organisations canadiennes** à partir des statistiques provenant de documents classifiés et publics [5].

Selon les résultats des analyses, **les rançongiciels resteraient une menace persistante, notamment pour les infrastructures essentielles**, car, depuis 2020, on note une augmentation des risques d'extorsion par rançongiciel. Le rapport met également en avant **une augmentation de la diffusion de contenu de désinformation** qui pourrait être attribuée à l'utilisation de l'intelligence artificielle, des algorithmes et de la technologie de l'hypertrucage (*deep fake*) par les acteurs malveillants. Un volet du rapport est aussi consacré aux prédictions **des impacts des développements sur les ordinateurs quantiques et les risques que présente la cryptographie moderne**.

Ce rapport présente plusieurs avantages, notamment son **utilisation de statistiques provenant de plusieurs agences gouvernementales et d'une échelle d'interprétation des probabilités qu'un événement survienne** (p. ex. très probable vs presque certainement). En revanche, **la méthodologie employée reste opaque**, peu de pistes de solutions pour atténuer les risques des cybermenaces sont proposées et peu d'informations portant sur les risques en fonction des secteurs d'activités économiques y sont présentées.

Rapport annuel du Centre de la sécurité des télécommunications 2023-2024 (2024)

Ce rapport annuel, dont le dernier a été publié en 2024, consiste en un état des lieux des activités stratégiques du Centre de la sécurité des télécommunications (CST) [6]. Les données collectées proviennent de rapports sommaires non classifiés portant sur les activités du CST pour l'année fiscale 2023-2024. Plusieurs thématiques s'y retrouvent telles que **le renseignement étranger**, **la cybersécurité**, **la cybercriminalité et la sécurité des communications**. Ce rapport présente certaines des mesures de sécurité mise en place par le CST tel que l'apprentissage machine (*machine Learning* [ML]), employé pour détecter des anomalies sur certaines infrastructu-

res numériques. Environ 6,6 milliards de signaux potentiellement malveillants ont été bloqués quotidiennement par cette technologie. Peu d'informations sur les cybercrimes et les cyberattaques sont présentées dans le rapport. **La sensibilité et les risques pour la sécurité nationale que pourrait engendrer le partage d'informations classifiées limitent évidemment la transparence des informations** présentées dans le rapport.

Ce document permet d'avoir une idée générale des **activités et des priorités stratégiques du CST**, par exemple **le fait d'avoir averti 250 entreprises canadiennes de l'imminence d'une attaque par rançongiciel contre leurs systèmes**. En revanche, **aucune information n'est disponible sur la prévalence des incidents de cybersécurité**. Seules des données sur la réponse du CST face à ces incidents sont présentées ce qui limite grandement le potentiel informatif du document, mais se justifie en regard des impacts potentiels sur les institutions et la population canadienne.

Perception et attitudes des organisations canadiennes vis-à-vis de la cybersécurité

Le sondage *Perception and Attitudes of Canadian Organizations Toward Cybersecurity* a été publié par le *Canadian Internet Registration Authority (CIRA)* [7] en 2022. Il tente d'établir **un portrait de la cybervictimisation, des comportements en matière de cybersécurité et de la perception des risques de cybermenaces des organisations canadiennes**. Au total, 500 employés et propriétaires d'entreprises canadiennes ont été sondés. Seules les organisations, dont au moins 50 employés, utilisent un ordinateur ou un appareil mobile dans 20 % de leurs tâches et les entreprises de moins de 1000 employés ont été sélectionnées. Des statistiques ont ensuite été produites tant pour le secteur privé que pour le secteur public. Puisque le rapport est produit ponctuellement, des comparaisons statistiques entre plusieurs années sont présentées.

Les principaux résultats du rapport démontrent que **41 % des organisations sondées ont été victimes d'une cyberattaque en 2022 et que leurs conséquences principales sont les coûts directs** (p. ex. perte de revenu) **et les coûts de récupération**. Pour les organisations ayant accepté de payer une rançon à la suite d'une attaque par rançongiciel, le montant moyen payé était de 25 000 $. **75 % des organisations se disent prêtes à soutenir une législation interdisant le paiement des rançons**. Les plus gros risques perçus par les organisations sont l'accès non autorisé ou le vol de données, les logiciels malveillants et la fraude. **68 % des entreprises se disent inquiètes de l'utilisation potentielle de l'intelligence artificielle dans des cyberattaques**, notamment en raison des informations collectées et leur potentiel d'utilisation pour améliorer les courriels d'hameçonnage.

Ce rapport présente de nombreux avantages. Il a été produit par un organisme à but non lucratif, **la démarche méthodologique est clairement expliquée** et **les caractéristiques de l'échantillon employé sont disponibles en annexe du rapport**. De nombreuses statistiques et de graphiques sont disponibles, tant sur les expériences que sur les perceptions des organisations en matière de cybersécurité. Toutefois, **l'échantillon choisi est trop petit pour être représentatif** et le rapport entier n'est disponible qu'en anglais. Il contient par ailleurs peu d'analyses, qui sont disponibles dans une publication séparée alors qu'elles auraient pu être intégrées au rapport.

Enquête canadienne sur la cybersécurité et le cybercrime (2023)

L'*Enquête canadienne sur la cybersécurité et le cybercrime (ECCC) 2023* [8] a été publiée en octobre 2024 par la Division de l'organisation industrielle et des finances (DOIF) de Statistique Canada, le tout parrainé par Sécurité publique Canada. Ce sondage est mené **tous les deux ans**, ce qui permet de suivre **l'évolution des tendances de la cybercriminalité et de la cy-**

-bersécurité depuis 2017.

Son objectif est d'**établir un portrait des mesures de cybersécurité, des types d'incidents et des coûts associés à la prévention et au rétablissement des opérations à la suite de cyberattaques contre les entreprises canadiennes**. L'échantillon analysé est constitué de **12 462 entreprises canadiennes de 10 employés ou plus** dans presque tous les secteurs, ce qui constitue un échantillon représentatif des entreprises canadiennes. Un processus de vérification et de validation des données a été effectué et les réponses jugées comme étant plus fiables ou de meilleure qualité se sont vu accorder une plus grande pondération dans les analyses.

Les entreprises canadiennes effectuent de plus en plus de vente en ligne et/ou de télétravail créant des risques importants quant à la confidentialité et la préservation des données. **L'erreur humaine reste la source la plus importante d'incidents majeurs**. En 2023, alors que **les dépenses engagées pour le rétablissement des activités à la suite d'incidents de cybersécurité a doublé comparativement à 2021** (passant de 600 millions de dollars à 1,2 milliards), **la dépense moyenne des entreprises en matière de prévention et de détection des incidents a peu augmenté** (de 9,7 milliards de dollars en 2021 à 11 milliards en 2023). De plus, la proportion d'entreprises ayant dépensé en prévention et détection a baissé de 61% en 2021 à 56% en 2023. En terme d'incidents, **le vol d'identité (36%) et la fraude (50%) représentent la majorité des incidents subis**.

L'approche méthodologique du rapport est claire et inclut un processus exhaustif de validation des données. La taille de l'échantillon est appropriée pour les analyses effectuées. De nombreux graphiques aident à la compréhension des statistiques. Le choix de développer un indicateur de la qualité des réponses est intéressant, mais aurait pu être plus expliqué. Les microdonnées sont disponibles à la communauté universitaire et aux organisations gouvernementales qui en font la demande, et seule une présentation résumant les points les plus importants est disponible pour le grand public. Bien que **plusieurs secteurs d'activités soient représentés au sein de l'échantillon, les données publiées ne permettent pas de les différencier**.

Le **tableau 1** présente une comparaison des principaux résultats du sondage de CIRA et celui de l'Enquête canadienne sur la cybersécurité et le cybercrime.

Rapport annuel 2022 du Centre antifraude du Canada (2023)

Le *Rapport annuel 2022* [9] du Centre antifraude du Canada (CAFC) brosse **un portrait des signalements et tendances en matière de la fraude au Canada**. Il présente aussi **une vue d'ensemble des mesures de prévention mises en place et des interventions effectuées par le CAFC**. Les données collectées comprennent tous les signalements reçus de particuliers et vérifiés par le CAFC entre le 1er janvier et le 31 décembre 2022. Certains signalements ont dû être omis à cause d'un manque d'informations sur les circonstances de l'incident. Il s'agit de la deuxième édition du rapport.

Les principaux résultats du rapport démontrent **une hausse de signalements de fraude traditionnelle et de cyberfraude**, atteignant un sommet de 91 000 signalements. **Les pertes financières encourues par ces fraudes s'élèvent à 530,4 millions de dollars canadiens dont 97 millions de dollars ont été perdus à la suite de fraude à l'investissement lié aux cryptomonnaies**, qui représentent d'ailleurs le deuxième mode de paiement le plus fréquemment employé dans les fraudes avec 125,9 millions de dollars de perte enregistrés. La perte moyenne par individu pour la fraude à l'investissement s'élève à 72 000 $, soit environ dix fois plus que pour les fraudes en ligne plus classique. Les fraudes par hameçonnage ont engendré des pertes de 58,1 millions de dollars.

Tableau 1. Comparaison des principaux résultats du sondage de CIRA et celui de l'Enquête canadienne sur la cybersécurité et le cybercrime

	***Perception and Attitudes of Canadian Organizations Toward Cybersecurity* [6]**	***Enquête canadienne sur la cybersécurité et le cybercrime* [8]**
Organisation responsable	Canadian Internet Registration Authority	Statistique Canada
Victime	Entreprise	Entreprise
Échantillon	500 entreprises	12 158 entreprises
Représentativité	Non	Oui
Méthodologie	Sondage	Sondage
Victimisation (%)	41	18
Menace la plus importante	Accès non autorisé à un ordinateur	Erreur humaine
Attaque la plus fréquente	N/D	Arnaque ou fraude
Montant moyen perdu par incident ($)	N/D	19 000
Conséquence principale victimisation	Incapacité à poursuivre le travail	N/D
Montant moyen en prévention par entreprise ($)	N/D	52 000

Malgré tout, **2,9 millions de dollars ont pu être récupérés et restitués aux victimes**.

Ce rapport présente plusieurs mesures de prévention pouvant être utiles pour se protéger de la fraude traditionnelle et de la fraude en ligne. Une bonne partie du rapport est consacrée aux cryptomonnaies et à des vignettes de cas réels de fraudes. Des tableaux présentent **les types de fraudes les plus fréquents en fonction de l'âge des victimes ainsi que leurs conséquences financières**. Les risques liés à l'intelligence artificielle, les logiciels d'accès à distance et une grande variété de types de fraudes y sont présentés et analysés. Certaines sections du rapport peuvent être occasionnellement répétitives et **peu d'informations sont incluses sur les motifs d'exclusion des signalements**.

Enquête canadienne sur l'utilisation d'Internet 2022 (ECUI) (2023)

L'*Enquête canadienne sur l'utilisation de l'Internet 2022 (ECUI)* [10] a été publiée par Statistique Canada en 2023 et a été parrainée par Innovation, Sciences et Développement Économique Canada (ISDE). Le rapport existe sous sa forme actuelle depuis 2005 et est produit aux deux ans. L'Enquête met en lumière **comment les technologies numériques influencent les manières de travailler, de se divertir et d'interagir des citoyens canadiens**. Pour y arriver, **des données ont été collectées auprès d'individus âgés de plus de 15 ans et provenant de toutes les provinces canadiennes**. Les individus résidant au sein d'une institution à temps plein ou habitant dans un territoire ont été exclus. Près de 55 700 ménages ont répondu à un sondage grâce à un questionnaire électronique ou une entrevue téléphonique assistée par ordinateur. Une technique d'échantillonnage stratifiée a été employée et la qualité des données a été validée par un processus de vérification statistique.

Comme dans bien des cas, les microdonnées du sondage ne sont pas entièrement disponibles. Pour y avoir accès, u**ne demande doit être effectuée auprès de Statistique Canada**, ce qui peut prendre plusieurs mois. En revanche, **plusieurs produits connexes présentant des analyses partielles du jeu de données sont disponibles sur le site de l'organisation**. Différentes thématiques y sont abordées, notamment **l'utilisation des services bancaires en ligne au Canada** [11, 12], **l'utilisation des services et technologies de l'Internet** [13] et **la protection des appareils contre les cyberattaques** [14].

Les principaux résultats de ces rapports démontrent que **l'utilisation des services bancaires en ligne est en hausse et que les résidents de l'Alberta et du Québec étaient les plus susceptibles d'employer ces services** [11]. Le niveau de confiance des individus envers leur institution financière et leur capacité à protéger les renseignements personnels exerce une influence sur le choix d'employer les services en ligne [12]. **43,4 % des Canadiens se disent inquiet lors de l'utilisation de technologies numériques pour faire des achats en ligne**. **24,9 % se disent extrêmement ou très inquiet lors de leur utilisation** [13]. De plus, l'Enquête révèle que **les incidents de cybersécurité touchant les citoyens canadiens sont en constante augmentation**, ce qui concorde avec l'augmentation des crimes rapportés au services de police présentés dans la DUC. En effet, **70% des Canadiens ont été victimes d'un incident de cybersécurité** en 2022 selon l'Enquête.

L'ECUI présente plusieurs avantages, notamment par **sa capacité à toucher à un large éventail de sujets liés à l'utilisation de l'Internet**. **Son échantillon diversifié permet de présenter des problématiques touchant des populations spécifiques**. Produite périodiquement, **l'Enquête permet de comparer les résultats sur plusieurs années et d'identifier les nouvelles tendances**. En revanche, **l'accès difficile aux données limite le potentiel d'utilisation par la communauté universitaire et scientifique**. Bien que plusieurs rapports

d'analyse soient disponibles sur le site de Statistique Canada, l'interface de la plateforme est difficile d'utilisation et complique l'accès à certains rapports qui pourraient intéresser les lecteurs.

Australie

La prochaine section présente plusieurs rapports officiels portant sur la cybercriminalité en Australie. Une attention particulière est portée à la méthodologie employée pour chacun des documents.

Targeting Scams Report (2024)

Le *Targeting Scams Report* [15] a été publié en avril 2024 par le *National Anti-Scam Centre (NASC)*, une organisation du gouvernement australien. Il vise à **brosser un portrait de la fraude signalée par la population australienne en 2023**. **Un volet est aussi consacré aux initiatives gouvernementales et privées en matière de prévention des incidents de fraude**. Il est publié annuellement depuis 2010 par d'autres organisations, mais repris en 2023 par le NASC depuis la création de ce dernier. Les données analysées proviennent de plusieurs organisations gouvernementales, notamment le *Australian Financial Crime Exchange (AFCX)*, *Scamwatch* et *ReportCyber**. **Plus de 601 000 rapports d'événements de fraude ont été analysés constituant un échantillon représentatif des incidents de fraude**. Bien que plusieurs partenaires aient accepté de partager leurs données pour contribuer au rapport, **peu de statistiques y sont réellement présentes**. Une importante partie du document est consacrée à la présentation d'initiative des différentes organisations en matière de prévention et d'intervention.

Plus de 2,74 milliards de dollars ont été perdus à la suite d'incidents liés à des activi-tés frauduleuses. Les pertes financières ont atteint un sommet au mois de mars et ont suivi une tendance à la baisse jusqu'à la fin de l'année. **Près de la moitié des pertes financières engendrées par des incidents de fraude auraient impliqué des cryptomonnaies** pour l'année fiscale 2022-2023. **À l'instar du Canada, les fraudes liées aux investissements auraient engendré le plus de pertes malgré une baisse de 7,8 %** (291,9 millions de dollars), **dépassant largement les pertes causées par les arnaques amoureuses** (34,3 millions de dollars).

Cybercrime in Australia 2023 (2023)

Le rapport *Cybercrime in Australia 2023* [16] a été publié par l'Institut australien de criminologie en 2023. **Il brosse un portrait de la prévalence de la victimisation par type de cyberattaque ainsi que les demandes d'assistance faites par la population australienne à la suite de ces cyberincidents**. 13 887 individus ont été sondés en plusieurs phases. D'abord, un sondage principal portant sur les caractéristiques sociodémographiques, les expériences de victimisation ainsi que l'aide obtenue a été effectué. Ensuite, une analyse longitudinale a été effectuée sur deux ans pour comparer l'évolution des tendances de la cybercriminalité. Finalement, des sondages périodiques de moindre ampleur ont été réalisés auprès des mêmes participants. Une grande attention est portée sur la création d'une méthodologie de qualité. La combinaison d'analyses qualitatives, quantitatives et la collecte de données longitudinale permettent de pallier plusieurs limites observées dans les études moins exhaustives. Certaines limites demeurent présentes, notamment quant à la non-représentativité de l'échantillon et la difficulté de catégoriser certaines cyberattaques.

Selon ce rapport, **les attaques par rançongiciels représenteraient 22 % des expériences de victimisation des individus sondés**. **Le vol d'identité et la fraude représenteraient respectivement 20 % et 8 % des incidents**. **79 % des victimes par rançongiciels auraient perdu moins de 1000 AUD après des efforts de**

* Pour en savoir plus sur le programme *ReportCyber*, visitez la page de l'Observatoire des programmes de prévention de la cybercriminalité.

recouvrement. Dans le cas des fraudes, il s'agirait plutôt de 75 %. Les cybercrimes auraient affecté négativement le quart des répondants du sondage.

ASD Cyber Threat Report 2022-2023 (2023)

Le *ASD Cyber Threat Report 2022–2023* [17] a été publié en 2023 par le *Australian Signals Directorate* du gouvernement australien, qui est l'agence de renseignement responsable de la collecte du renseignement électronique. Il présente **un portrait des cybermenaces en Australie**. **1 100 incidents de cybersécurité rapportés au *Australian Cyber Security Centre (ASCS)* et 94 000 incidents rapportés aux organisations policières australiennes ont été analysés**. La taille de l'échantillon analysé est l'une de ses forces principales. Cependant, puisqu'il s'agit d'incidents déclarés à la police, **il est possible que la prévalence de la cybercriminalité soit sous-estimée**. Aucune information disponible ne permet de détailler la méthodologie employée pour analyser les informations.

Les principaux résultats démontrent que **les brèches de données ainsi que les rançongiciels demeurent les menaces les plus importantes pour les entreprises**. L**es trois types de cyberattaques les plus fréquentes pour les individus sont la fraude à l'identité, la fraude bancaire en ligne et la fraude liée aux achats en ligne**.

The Commonwealth Cybersecurity Posture in 2023 (2023)

Le *Commonwealth Cybersecurity Posture in 2023* a été publié par le *Australian Signals Directorate* [18] du gouvernement australien en 2023. **Ce rapport tente d'informer le Parlement australien sur les menaces de cybersécurité les plus importantes** pour l'année fiscale 2022-2023 et **d'orienter l'implantation de mesures de prévention et développement de la cyberrésilience**. Les données provenant du ASD ont été employées ainsi que des données provenant du *Protective Security Policy Framework Assessment Report 2021–2022*. Ce rapport comporte les mêmes limites méthodologiques que celles présentées dans la section précédente.

Les résultats principaux démontrent qu'**entre 2022 et 2023, le nombre d'organisations gouvernementales employant le cryptage de sites web a augmenté tandis que le cryptage de courriels a diminué**. Plusieurs stratégies d'atténuation des risques de cybersécurité incluant le contrôle d'application, la restriction des privilèges administratifs et l'authentification à plusieurs facteurs sont efficaces pour diminuer les risques d'incidents.

Royaume-Uni

NCSC Annual Review 2023 (2023)

Le *NCSC Annual Review 2023* a été publié par le *National Cyber Security Centre* [19] du Royaume-Uni en 2023. **Il brosse un portrait des principaux événements cybercriminels ayant affecté le pays, ainsi que leurs impacts en matière de cybersécurité**. Les principales thématiques abordées sont les impacts de l'intelligence artificielle sur la cybersécurité, la protection des infrastructures critiques, la protection de la démocratie, le futur des services de cybersécurité, ainsi que les leçons apprises depuis l'invasion de l'Ukraine par la Russie. **Près de 2005 incidents collectés par le NCSC ont été analysés**, un nombre record pour l'organisation. Bien que l'échantillon étudié soit étendu, aucune description de ses caractéristiques n'est offerte. De plus, **peu d'informations sont disponibles sur les analyses qui en ont été faites**. Les analyses présentées sont principalement descriptives.

Selon le rapport, **les rançongiciels demeurent l'une des menaces les plus importantes contre les organisations du Royaume-Uni**. 297 rapports sur la présence d'activités suspectes liées à l'utilisation de ces maliciels ont été soumis

au NCSC. **La plupart des signalements provenaient du domaine universitaire, des industries de production et du secteur des technologies de l'information**. L'exfiltration et l'extorsion de données sont en hausse de 18,5 % par rapport à l'année précédente avec un total de 327 incidents.

Cyber Security Breaches Survey 2024 (2024)

Le *Cyber Security Breaches Survey 2024* [20, 21] a été publié par le Département des sciences, de l'innovation et des technologies du Royaume-Uni. Ce document est publié annuellement depuis 2017. **L'objectif du rapport est de comprendre les politiques d'approches en matière de cybersécurité tout en prenant en considération les vulnérabilités et réponses des institutions face aux cyberattaques**. 2000 entreprises, 1004 organisations à but non lucratif et 430 établissements scolaires ont participé à un sondage téléphonique entre septembre 2023 et janvier 2024. Ils ont été sélectionnés grâce à un échantillonnage probabiliste aléatoire. Un processus de repondération des données portant sur les entreprises et les organismes à but non lucratif a été effectué afin d'améliorer la représentativité de l'échantillon. De plus, 44 entrevues ont été effectuées dans le but de compléter les données qualitatives et quantitatives collectées par sondage. Seuls les incidents détectés par les organisations ont été collectés, sous-entendant une sous-représentation des cyberattaques réelles.

41 % des organisations ayant répondu au sondage affirment avoir vécu une expérience de cybervictimisation dans la dernière année. **Près du quart (23 %) disent avoir été victime d'une attaque par rançongiciel** considérée comme étant réussie, et **70 % de celles-ci auraient payé la rançon demandée**. 53 % des entreprises auraient payé plus de 25 000 $ comme montant de rançon.

Nature of fraud and computer misuse in England and Wales: Year Ending March 2022 (2022)

Le *Nature of fraud and Computer Misuse in England and Wales* [22] a été publié par l'Office national de la Statistique du Royaume-Uni en 2022. Le rapport est parrainé par le Bureau national du renseignement sur la fraude. Une première édition portant sur les statistiques de 2019 est aussi disponible [23]. **Le rapport se fonde sur les données collectées annuellement dans le *Crime Survey for England and Wales (CSEW)* et le *Telephone-operated Crime Survey for England and Wales (TCSEW)***. Il est à noter que la méthodologie du CSEW a commencé à inclure les cybercrimes seulement à partir de 2015 [24]. **Ces études brossent un portrait du volume de fraude et de l'utilisation non autorisée d'ordinateurs pour effectuer des cyberattaques**. Des sondages et des entrevues ont permis de collecter les données. Les échantillons des deux études permettent d'avoir une bonne représentativité de la population du Royaume-Uni. Certaines manipulations statistiques ont été effectuées pour permettre la comparaison entre les résultats du CSEW et du TCSEW. Seuls les crimes contre les individus sont pris en considération.

Les résultats du rapport démontrent que **les incidents de fraude sont en hausse de 25 % par rapport à 2020 pour un total de 4,5 millions de délits**. **L'utilisation non autorisée d'un ordinateur a augmenté de 89 % pour la même période**. **Des pertes financières ont été subies dans 64 % des incidents**.

Cracking the Case: Uncovering the Cost of Small Business Crime (2023)

Le rapport *Cracking the Case: Uncovering the Cost of Small Business Crime* [25] a été publié par la Federation of Small Businesses (FSB) et met en lumière les expériences des micros et petites entreprises en lien avec la criminalité financière. Des entrevues, des sondages téléphoniques ainsi que des groupes de discussion ont été administrés par une firme externe pour collecter les données. Les incidents ayant eu lieu entre janvier 2021 et janvier 2023

ont été analysés. Ces derniers ont été catégorisés en trois dimensions : **crimes traditionnels**, **cybercrimes** et **fraude**. Des définitions de chacune de ces catégories sont présentées. Des vignettes de cas permettent d'exemplifier certains résultats d'analyse. **Il est possible que des entreprises sondées aient essayé de se présenter sous un angle positif ou aient eu de la difficulté à évaluer les impacts à long terme des différents incidents**. En revanche, des données officielles provenant entre autres du ministère des Affaires et du Commerce ou du National Business Crime Centre viennent soutenir certains résultats du rapport.

Annual Fraud Report 2024 (2024)

Le *Annual Fraud Report 2024* [26] a été publié par UK Finance en 2024. Cette organisation regroupe plus de 300 firmes du domaine de la finance. **L'objectif du rapport est de décrire le nombre de cas et les montants perdus à la suite d'incidents de fraude**. Les données présentées proviennent directement des organisations. Des formulaires standardisés sont remplis directement par les partenaires en fonction d'une définition précise des cybercrimes. Trois phases de validation des données sont ensuite effectuées par UK Finance pour en assurer la fiabilité. Les résultats démontrent que **les organisations sondées ont perdu 1,17 milliard de livres sterling (soit 2 100 716 046 dollars canadiens) à la suite d'incidents de fraude en 2023, ce qui correspondrait à une baisse de 4 % par rapport à 2022**. Toutefois, il est possible que **les firmes sondées aient tenté de surreprésenter les mesures de prévention qu'elles ont mises en place et de sous-estimer les coûts à long terme des incidents de fraude qu'elles ont vécus**. Il est aussi possible que les efforts de prévention mis en place par les organisations commencent à porter fruit. Il est donc nécessaire de continuer à porter une grande attention à l'évolution des statistiques dans les prochaines années.

Conclusion

Cette note de synthèse a présenté plusieurs rapports portant sur la cybercriminalité au Canada, en Australie et au Royaume-Uni au cours des dernières années. Toutes ces études ne poursuivaient pas les mêmes objectifs et ne ciblaient pas les mêmes populations. Celles les plus robustes employaient des méthodes mixtes de collecte de données, parfois sur une longue période en reconduisant le même questionnaire sur une base annuelle ou bisannuelle, et tentaient d'être les plus représentatives des caractéristiques de leur population. Ce genre d'approche permet d'obtenir les chiffres les plus fidèles que possible de la cybercriminalité, ce qui constitue une condition indispensable à l'élaboration, à l'implantation et à l'évaluation de politiques et de programmes de prévention efficaces.

Références

[1] Correia, S. G. (2022). Making the most of cybercrime and fraud crime report data: A case study of UK Action Fraud. *International Journal of Population Data Science*, *7*(1), Article 1.

[2] Statistique Canada. (2024). *Programme de déclaration uniforme de la criminalité (DUC) (3302)*. Gouvernement du Canada.

[3] Statistique Canada. (2024). *Cybercrimes déclarés par la police, nombre d'affaires et taux pour 100 000 habitants, Canada, provinces, territoires, régions métropolitaines de recensement et Police militaire des Forces canadiennes [Tableau]*. Gouvernement du Canada.

[4] Statistique Canada. (2024). *Statistiques sur les crimes déclarés par la police au Canada, 2023*. Gouvernement du Canada.

[5] Centre canadien pour la cybersécurité. (2022). *Évaluation des cybermenaces nationales 2023–2024 (2816–9204; pp. 1–44)*. Centre de la sécurité des télécommunications Canada.

[6] Centre de la sécurité des télécommunications Canada. (2024). Rapport annuel du Centre de la sécurité des télécommunications 2023-2024 (2564-0488). Gouvernement du Canada.

[7] Canadian Internet Registration Authority. (2022). *2022 CIRA Survey: Perceptions and Attitudes of Canadian Organizations Toward Cybersecurity*. CIRA.

[8] Ammba, B. (2023). *Résultats de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2021*. Statistique Canada.

[9] Centre anti-fraude du Canada. (2023). *CAFC Rapport Annuel 2022 (PS61-46F-PDF)*. Gouvernement du Canada.

[10] Statistique Canada. (2023). *Enquête canadienne sur l'utilisation de l'Internet (ECUI) (4432)*. Gouvernement du Canada.

[11] Statistique Canada. (2024). *L'utilisation des services bancaires en ligne au Canada, 2022 (11-627-M)*. Gouvernement du Canada.

[12] Statistique Canada. (2024). *Tendances des activités bancaires et des achats en ligne (4432)*. Gouvernement du Canada.

[13] Statistique Canada. (2021). *Utilisation des services et technologies Internet par les Canadiens: Outil interactif*. Gouvernement du Canada.

[14] Statistique Canada. (2019). *Protection des appareils contre les incidents de cybersécurité*. Gouvernement du Canada.

[15] National Anti-Scam Centre. (2024). T*argeting scams: Report of the ACCC on scams activity 2023 (pp. 1–25)*. Australian Government.

[16] Voce, I., & Morgan, A. (2023). C*ybercrime in Australia 2023 (Statistical Report 43)*. Australian Institute of Criminology.

[17] Australian Signals Directorate. (2023). *ASD Cyber Threat Report 2022-2023*. Australian Cyber Security Centre.

[18] Australian Signals Directorate. (2023). *The Commonwealth Cyber Security Posture in 2023 | Cyber.gov.au*. Australian Cyber Security Centre.

[19] National Cyber SecurityCEnter. (2023). *NCSC Annual Review 2023*. Government Community Headquarters.

[20] Department for Science, Innovation and Technology, & Home Office. (2024). *Cyber Security Breaches Survey 2024 [Technical Report]*. Government of the United Kingdom.

[21] Department for Science, Innovation and Technology, & Home Office. (2024). *Cyber security breaches survey 2024: Technical report*. Government of the United Kingdom.

[22] Office for National Statistics. (2022). *Nature of fraud and computer misuse in England and Wales*. Government of the United Kingdom.

[23] Office for National Statistics. (2020). *Nature of fraud and computer misuse in England and Wales (pp. 1–29)*. Government of the United Kingdom.

[24] Office for National Statistics. (2015). *Update: Extending the Crime Survey for England and Wales (CSEW) to include fraud and cybercrime*. Government of the United Kingdom.

[25] The Federation of Small Businesses. (2023). *Cracking the Case: Uncovering the cost of small business crime*. FSB.

[26] UK Finance. (2024). *Annual Fraud Report 2024*. UK Finance.