

CANADIAN CENTRE^{FOR} **CYBER** SECURITY

Nuhad Zoght
Partenariats - Infrastructure Essentielle
Canadienne

27 Février 2020

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



LE MONDE À L'ÈRE
NUMÉRIQUE

anonymat
perturbation
censure
connectivité omniprésente
vol informatique
cybercriminalité
vulnérabilités omniprésentes
guerre électronique asymétrique
code malveillant
maisons piratables
Internet des objets
pertes d'emploi
non-imputabilité
fausses nouvelles
risques constants
systèmes de contrôle vulnérables
réseaux de zombies
capables de se reproduire
Protection insuffisante des données
transport piratable

Les 10 principales priorités des DPIs

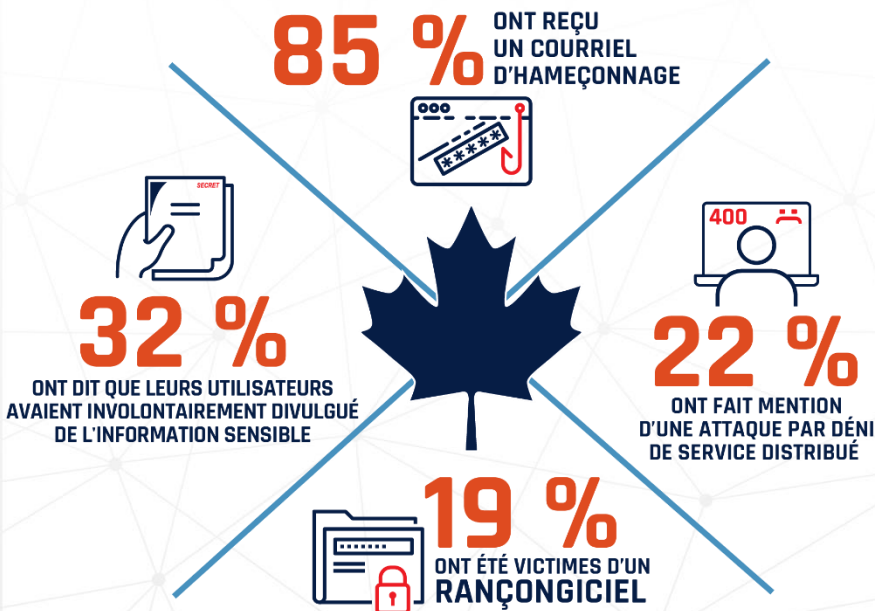
L'étude de 2020

Révèle que...

- 1 Cybersécurité et gestion des risques
- 2 Gouvernement numérique
- 3 Services infonuagiques
- 4 Consolidation/optimisation
- 5 Gestion de la relation client
- 6 Budget, contrôle des coûts, gestion financière
- 7 Modernisation des systèmes en place
- 8 Gestion et analyse des données
- 9 Connectivité à large bande/sans fil
- 10 Innovation et transformation par la technologie

Source: NASCIO.org

Contexte canadien - cybersécurité



75% des petites entreprises conservent des données confidentielles sur des services d'hébergement web externes comparativement à 48% chez les grandes entreprises.

21% des entreprises canadiennes ont rapportées avoir interrompu leurs opérations suite à un

66% des entreprises canadiennes ont des employés qui utilisent leurs appareils personnels pour travailler.

76% des cyber incidents perpétrés par un auteur externe sont motivés par les gains financiers.

Entre 80% et 90% des entreprises ont une couverture d'assurance en cas de pertes directes liées à des cyber attaques ou à des cyber intrusions.

La Stratégie nationale de cybersécurité de 2018, *Vision du Canada*
pour
la sécurité et la prospérité dans l'ère numérique, présente la nouvelle

La nouvelle Stratégie nationale de cybersécurité

Systèmes canadiens sécurisés et résilients

Protéger les Canadiens contre la cybercriminalité, contrer les menaces en évolution et défendre les systèmes essentiels du gouvernement et du secteur privé



Un écosystème du cyberspace novateur et adaptable

En appuyant les recherches avancées, en encourageant l'innovation numérique, en développant les compétences et en améliorant la sensibilisation



Leadership, gouvernance et collaboration efficaces

En étroite collaboration avec les provinces, les territoires, le secteur privé et les alliés internationaux, le gouvernement fédéral exercera un leadership pour améliorer la cybersécurité au Canada.



Centralisation de l'expertise en Cybersécurité



Nous représentons la seule source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour le gouvernement, le secteur privé, les Canadiens ainsi que les propriétaires et exploitants d'infrastructures essentielles.

Les nouveaux locaux



- Les locaux du Centre pour la cybersécurité est situés au 1625, promenade Vanier.
- Des locaux distincts, ouverts, accessibles et axés sur la collaboration.
- Ils favorisent l'innovation avec les partenaires de l'industrie.

Loi sur le CST : Pouvoirs et capacités du CST

« Il n'y a pas d'obligation plus importante que celle d'assurer la sécurité des Canadiens au pays et à l'étranger. Le projet de loi C-59 accorderait au CST les pouvoirs et les outils nécessaires pour adhérer aux normes les plus rigoureuses en matière tant de sécurité que de reddition de comptes et de transparence. »

—L'honorable Harjit Singh Sajjan,
MINISTRE DE LA DÉFENSE NATIONALE

RENSEIGNEMENT ÉLECTROMAGNÉTIQUE ÉTRANGER



**MAINTENIR LA CAPACITÉ DU CST
DE RECUEILLIR DU RENSEIGNEMENT
ÉLECTROMAGNÉTIQUE ÉTRANGER**

Utiliser des techniques avancées pour accéder à des réseaux étrangers afin de recueillir du renseignement étranger à l'appui des priorités du gouvernement

CYBERSÉCURITÉ ET ASSURANCE DE L'INFORMATION



**DÉFENDRE LES RÉSEAUX NON
GOUVERNEMENTAUX IMPORTANTS**

Déployer sur demande les outils de cybersécurité du CST dans les systèmes non gouvernementaux

Éliminer les obstacles juridiques à l'échange d'information sur les cybermenaces et de conseils d'atténuation

ASSISTANCE AUX PARTENAIRES FÉDÉRAUX DE LA COLLECTIVITÉ DE LA SÉCURITÉ ET DU RENSEIGNEMENT



**PRÊTER ASSISTANCE AU MDN ET AUX FAC,
Y COMPRIS MENER DES CYBEROPÉRATIONS
DANS LE CONTEXTE DE MISSIONS MILITAIRES
AUTORISÉES PAR LE GOUVERNEMENT**

Utiliser des techniques avancées pour appuyer les compagnies militaires et protéger le personnel militaire

CYBEROPÉRATIONS ÉTRANGÈRES

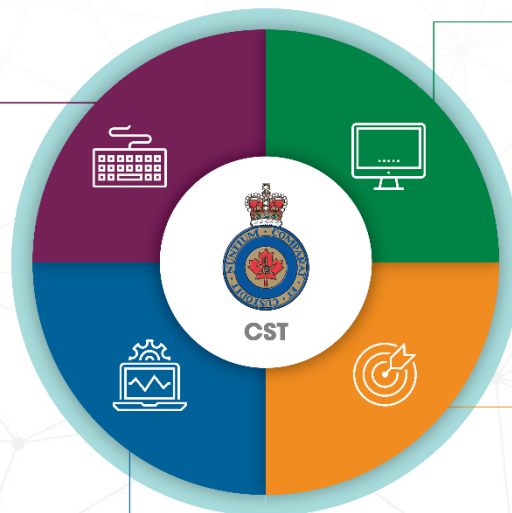


CYBEROPÉRATIONS DÉFENSIVES

Contenir les cybermenaces étrangères visant les réseaux canadiens importants

CYBEROPÉRATIONS ACTIVES

Entraver les activités étrangères en ligne qui menacent le Canada



MESURES ACCRUES DE REDDITION DE COMPTES

Une portée de services élargie

*Loi sur la
défense
nationale*

Le CST pouvait fournir des conseils, avis et services aidant à protéger l'infrastructure essentielle pour le gouvernement canadien.

**La loi sur le
CST**

Le CST peut maintenant offrir un service de cyberdéfense plus robuste par l'utilisation d'outils de cyberdéfense sur des réseaux critiques non-gouvernementaux désignés comme étant d'importance pour le Canada.

CYBERSÉCURITÉ ET ASSURANCE DE L'INFORMATION



**DÉFENDRE LES RÉSEAUX NON
GOUVERNEMENTAUX IMPORTANTS**
Déployer sur demande les outils de cybersécurité
du CST dans les systèmes non gouvernementaux
Éliminer les obstacles juridiques à l'échange
d'information sur les cybermenaces
et de conseils d'atténuation



Nous représentons la seule source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour le gouvernement, le secteur privé, les Canadiens ainsi que les propriétaires et exploitants d'infrastructures essentielles.



Résultats nationaux

Information et
systèmes d'information
importants

Complément des
capacités publiques et
commerciales

À qui s'adressent nos services

Nous **développons** les partenariats visant à créer un cyberspace canadien fort et résilient. Nous offrons des espaces polyvalents et non classifiés que peuvent employer conjointement le gouvernement, l'industrie privée et le milieu universitaire.

Gouvernement

- Nous sommes une ressource centralisée qui agit à titre d'interlocuteur pour les hauts dirigeants du gouvernement pour tout ce qui touche à la cybersécurité

Partenaires
externes

- Nous représentons le point de contact principal du gouvernement fédéral en matière de cybersécurité pour les partenaires externes, notamment dans le cadre de la coordination et de l'intervention en cas d'incident.

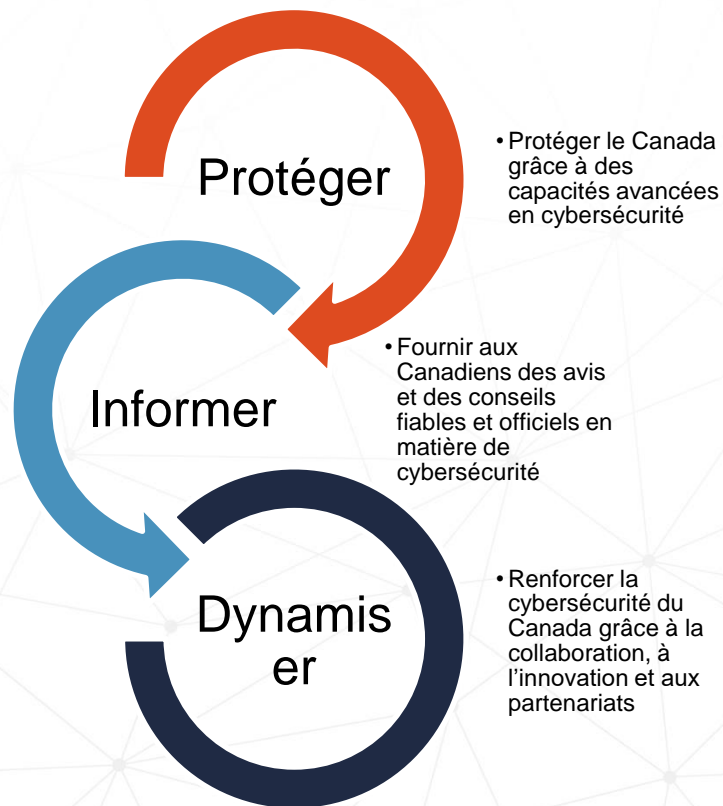
Application de la loi

- Nous sommes la seule source autorisée à fournir de l'expertise technique en matière de cybersécurité qui vient appuyer les organismes responsables dans le cadre de leurs fonctions policières et de leurs activités de sécurité et de renseignement.

Canadiens

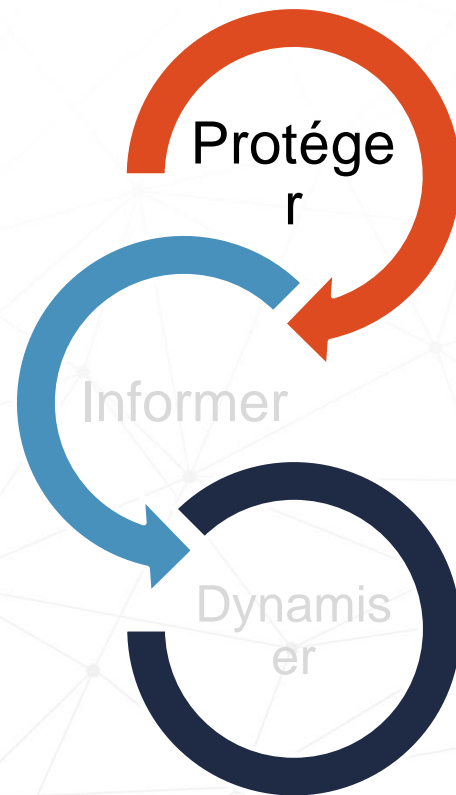
- Nous informons et sensibilisons les Canadiens sur les enjeux de cybersécurité, et nous communiquons avec eux à ce sujet, en leur fournissant des conseils clairs et des pratiques qui sont appuyés par une expertise et des renseignements uniques.

Assurer la cybersécurité des activités numériques au Canada



Protéger

- Programmes d'atténuation des risques
- Soutien des activités de gestion des incidents
- Services d'échange d'information automatisé
- Défense des réseaux
- Services cryptographiques
- Projets collaboratifs de cyberdéfense



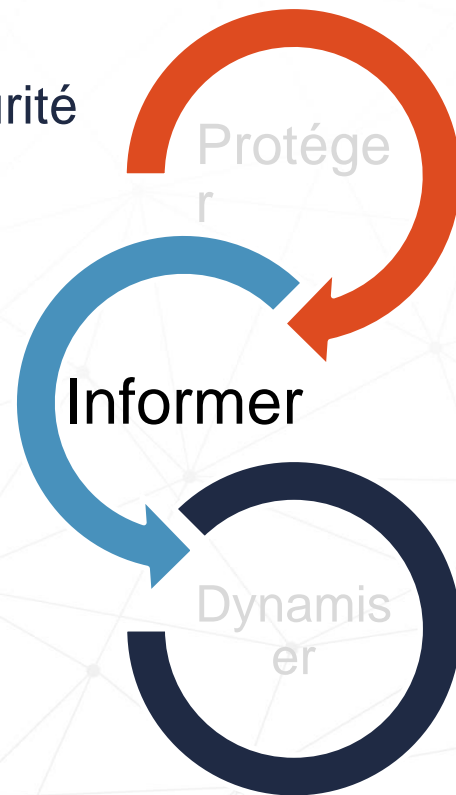
Protection des réseaux du gouvernement du Canada

- Nous avons détecté et confirmé une cyberintrusion perpétrée au moyen de méthodes hautement sophistiquées par une entité parrainée par le gouvernement de la Chine visant les systèmes informatiques du Conseil national de recherche du Canada (CNRC).
- Pour y arriver, nous avons collaboré avec le CNRC, SPC et d'autres partenaires en sécurité des TI du GC.
- Nous avons fait appel à de nombreuses méthodes de cyberdéfense pour assurer le suivi et l'atténuation de cette cyberintrusion.
 - Les leçons apprises dans le cadre de cet incident ont contribué à améliorer et à perfectionner nos outils et techniques.

Assemblyline est un outil de source ouverte du Centre pour la cybersécurité qui a été employé pour détecter et analyser le maliciel lors de la compromission.

Informer

- Campagne de sensibilisation Pensez cybersécurité
- Avis et conseils techniques
- Évaluations stratégiques des cybermenaces
- Cyberstabilité et rapports sur les tendances
- Rapports et notifications d'événements de cybersécurité



Campagne Pensez cybersécurité

À QUEL POINT ÊTES-VOUS CYBERSÉCURITAIRE?



Les Canadiens sont branchés à Internet en moyenne 6 heures par jour.

QUELS TYPES D'APPAREILS LES CANADIENS UTILISENT-ILS POUR ALLER EN LIGNE?



94 %
ORDINATEUR
DE BUREAU
OU PORTABLE



58 %
TABLETTE



25 %
TÉLÉVISEUR INTELLIGENT



74 %
TÉLÉPHONE
INTELLIGENT



25 %
CONSOLE DE JEUX

Les Canadiens protègent leurs ordinateurs contre les cybermenaces, mais **seulement 50 % connaissent** les risques liés aux autres appareils



PENSEZ  CYBERSECURITE

5 CONSEILS POUR DIRIGER UNE #ENTREPRISECYBERSÉCURITAIRE

Dans chaque entreprise, les employés représentent à la fois le plus grand risque ET la meilleure protection contre la cybercriminalité.

Les connaissances et la formation peuvent faire toute la différence.



Protégez-vous et signalez les escroqueries

Pensez cybersécurité vous offre des conseils pour vous protéger contre les cybermenaces. Mais que devez-vous faire si vous êtes victime d'un cyberincident? Les mesures à prendre dépendront de sa nature



5 façons de protéger votre vie privée sur un nouvel appareil intelligent

Les appareils qui se connectent à Internet (aussi appelés « appareils intelligents ») sont amusants et nous simplifient la vie, mais ils peuvent aussi permettre aux pirates informatiques d'accéder à des renseignements personnels ou confidentiels. Suivez ces conseils pour assurer votre protection et celle de votre entourage.



Trois éléments à considérer avant d'acheter un appareil intelligent

Les assistants intelligents, les casques de réalité virtuelle et les montres intelligentes sont parmi les cadeaux les plus convoités en cette période des fêtes. Avant d'acheter un appareil qui se connecte à Internet, renseignez-vous afin de vous protéger, vous et le destinataire de votre cadeau, des cybercriminels.

Les 10 mesures du CST

- Ensemble complet de mesures visant à atténuer les cybermenaces et s'appliquant à tous les types d'organisation
- Mesures fondées sur l'analyse des tendances en matière de cybermenaces en vue de contrer les cybermenaces les plus récentes



Contrôles recommandés

Élaborer un plan d'intervention en cas d'incident

Fournir de la formation pour sensibiliser les employés

Mis en œuvre des contrôles d'accès et autorisation

Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications

Établir un périmètre de défense de base

Infonuagique sécurisée et services de TI externalisés

Activer les logiciels de sécurité

Utiliser un authentification forte

Services mobiles sécurisés

Services mobiles sécurisés

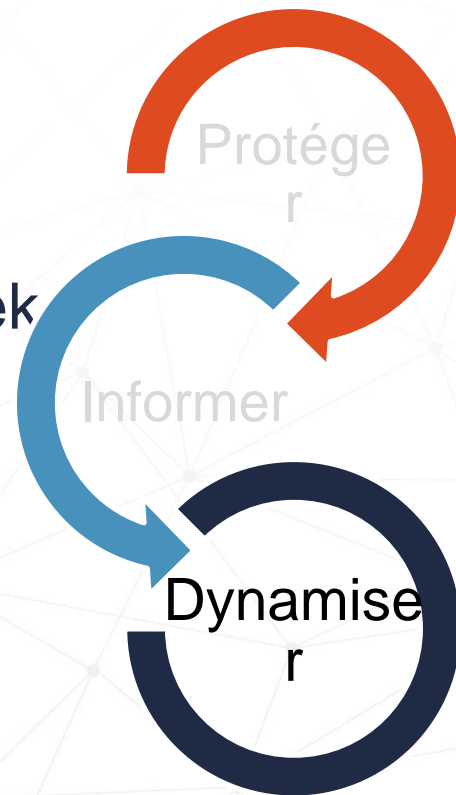
Sauvegarde et chiffrement des données

Supports amovibles sécurisés

Sites web sécurisés

Dynamiser

- Partenariats
- Carrefour de l'apprentissage
- Événement de collaboration : GeekWeek
- Relations avec le milieu universitaire
- Recherche et développement



CARREFOUR DE L'APPRENTISSAGE DU CENTRE POUR LA CYBERSÉCURITÉ



FAVORISER L'EXCELLENCE DANS LE DOMAINE DE LA CYBERSÉCURITÉ

○ Livraison électronique (gratuite), y compris :

- 601-Introduction à la gestion de la sécurité des TI
- 604-Survol de la gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie - Résumé
- 606-Rudiments de la sécurité des TI à l'intention des professionnels des TI

○ Salle de classe, y compris:

- 104 - La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
- 105 - Information System Security Implementation Process (ISSIP)
- 107 - Cybersécurité au gouvernement du Canada (pour les employés non-TI)
- 109 - Cybersécurité pour les praticiens de la sécurité
- 110 - Cybersécurité dans le GC et la visibilité en ligne
- 111 - La cybersécurité dans le GC pour la maison et le télétravail
- 115 - Une introduction à l'infonuagique au sein du Gouvernement du Canada
- 345 - Cyber sécurité pour les communications sans-fil
- 701 - Gestion des risques liés à la sécurité des TI et profils de contrôles de sécurité

○ Sessions de WebEx sont disponibles (25 max.)

Ce que nous faisons

Guichet de
services
unique



Carrefour de
l'apprentissag
e inclusif



Réponse
aux
incidents
coordonné
e



Conseils et
avis
d'experts



Programme de
collaboration
avec
l'infrastructure
essentielle



Évaluation des
équipements de
cryptographie
commerciaux et
gouvernementau



Défense des
systèmes et réseaux
du gouvernement
contre les cyber
menaces



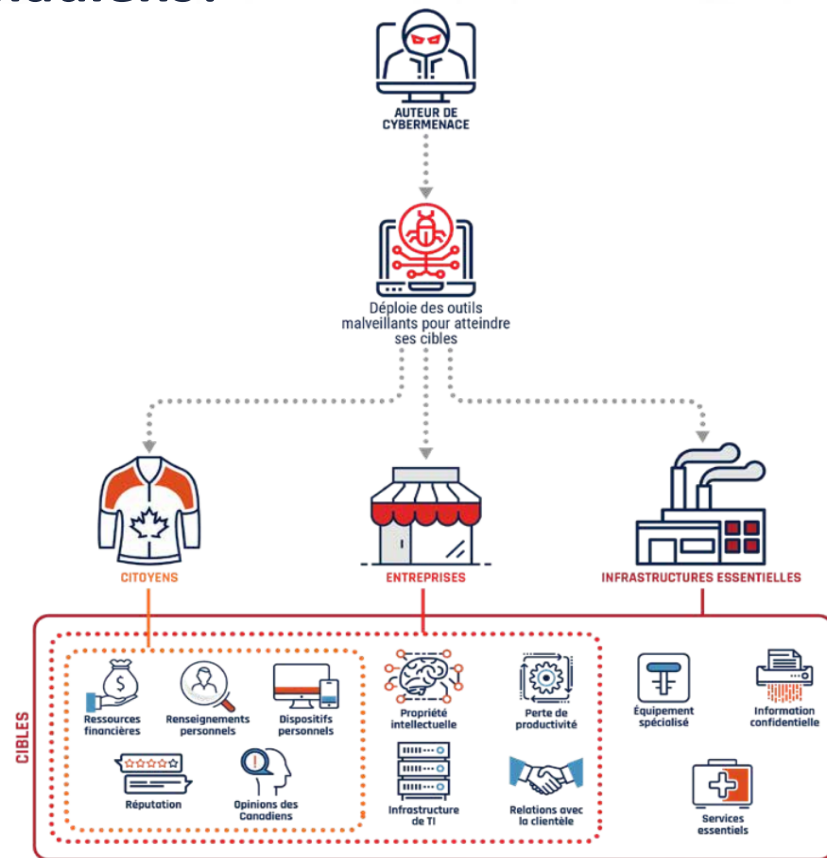
Partage de
l'information et des
technologies avec le
secteur privé

Les services PTM mis à profit aujourd'hui

Quels acteurs ciblent les réseaux canadiens?

- Les États étrangers
- Les hacktivistes
- Les criminels
- Les terroristes

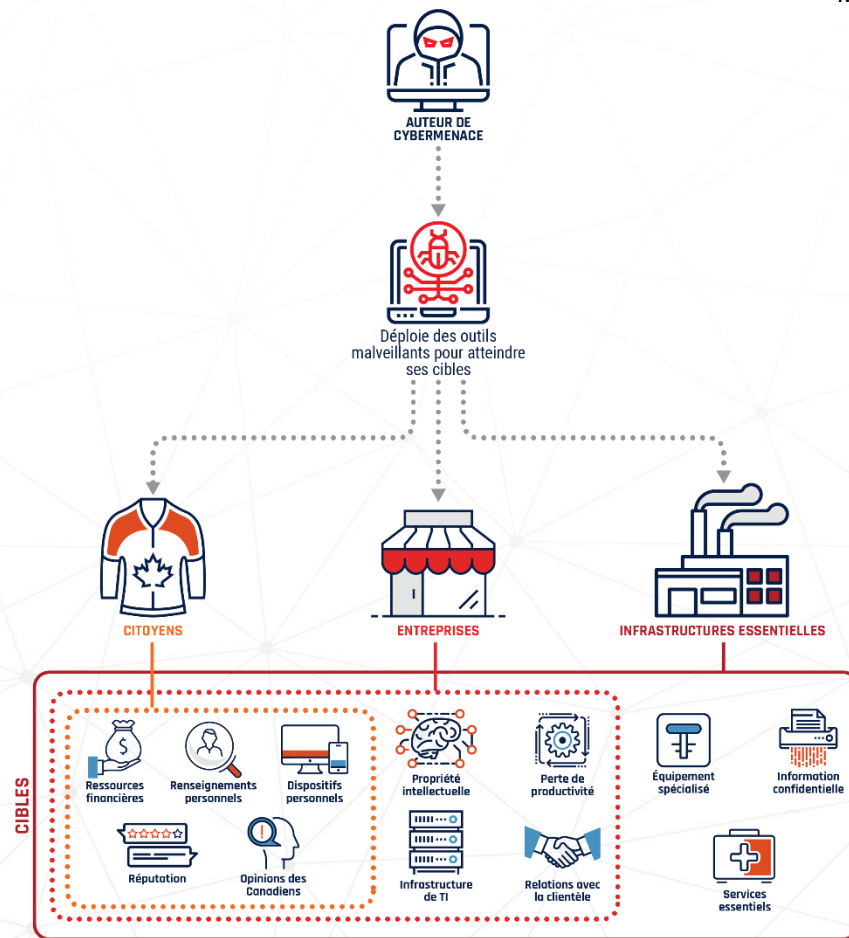
Une fois l'accès obtenu, les auteurs de menace peuvent voler ou altérer l'information, corrompre les opérations ou programmer les ordinateurs pour exploiter d'autres ordinateurs ou systèmes auxquels ils sont connectés.



Les cibles des cyber acteurs

Ils ciblent ce qui a de la valeur:

- Pour les gens
- Pour les organismes
- Pour le gouvernement



Les États-nations

- Les États nations soutiennent des auteurs de cybermenace qui vont continuer de faire du cyber espionnage contre les entreprises canadiennes et les infrastructures essentielles afin d'avancer leurs avantages stratégiques nationaux.
- De plus en plus d'États-nations développent des outils pour faire du cyber espionnage.
- Les États-nations vont utiliser les outils et techniques qui fonctionnent.
- Il est difficile d'attribuer les cyber attaques à des auteurs spécifiques.



Cybermenaces contre les entreprises canadiennes

Faits saillants

- Chaque maillon d'une chaîne d'approvisionnement mondiale peut constituer une menace pour la cybersécurité
- Plus une menace se produit tôt dans le cycle de vie du développement, plus l'impact potentiel
- Les faiblesses de la chaîne d'approvisionnement sont un moyen précieux pour les activités malveillantes pour les acteurs de la cybermenace

NORMES
ET EXIGENCES
DE L'INDUSTRIE

Profiter de l'influence du marché

CONCEPTION

Mauvaises pratiques en matière de qualité conceptuelle

PRODUCTION

Trafiage

LIVRAISON
ET DÉPLOIEMENT

Pratiques inadéquates en matière de cybersécurité

OPÉRATION

Exploitation des vulnérabilités

MAINTENANCE

Compromission du fournisseur de services

Statistiques sur les rançongiciels. (Deloitte, 2019)

- Les paiements de rançon moyens sont de 50,000\$
- Une entreprise est ciblée toutes les 40 secondes à travers le monde
- Plus de 50% des infections d'hameçonnage proviennent de la vulnérabilité du bureau à distance de Microsoft
- 40% des entreprises canadiennes ciblées ont payé la rançon
- 80% des entreprises affectées ont rétabli leurs

Valeur monétaire pour les entreprises



Pertes financières



**Avancées en
innovation**



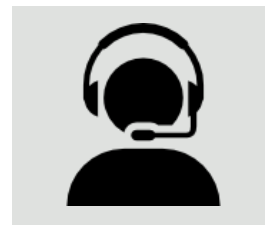
**Impacts sur la
réputation**



**Vol de propriété
intellectuelle**



**Disponibilité des
systèmes**



**Offre de
services**

Considérations pour votre organisation

○ Gouvernance interne

- Est-ce que la cybersécurité est mise en priorité de façon récurrente?

○ Investissements

- Combien de ressources investissons-nous en cybersécurité?

○ Résilience

- Sommes-nous prêts pour une cyberattaque?

○ Chaîne d'approvisionnement

- Est-ce que tous les composants de notre chaîne d'approvisionnement ont une bonne cybersécurité?

○ Collaboration

- Travaillons-nous avec des experts en cybersécurité, sommes-nous impliqués dans des efforts communs avec d'autres joueurs, utilisons-nous les services du gouvernement?

Comment rehausser notre cybersécurité?

- Porter attention aux éléments de base: planification, politiques, processus.
- Gérer l'information de grande valeur avec des précautions particulières.
- Intégrer la cybersécurité dans la gouvernance de votre organisation.
- Avoir un plan de rétablissement en cas de cyber incident.
- Développer la résilience de vos employés.

EN CYBERSÉCURITÉ LA COLLABORATION EST LA CLÉ DU SUCCÈS

Les nouveaux bureaux du Centre offriront l'opportunité pour les secteurs publics et privés de travailler côte-à-côte sur les problèmes les plus complexes au Canada

- ▶ Ouvert et accessible
- ▶ Grande quantité de travail non classifié
- ▶ Espaces innovatifs pour la collaboration
- ▶ Développement collaboratif

Comment le Centre pour la cybersécurité contribue

Que peut vous apporter le Centre pour la cybersécurité?

①



Rapports et alertes

Accès à du
renseignement
actionnable

②



**Outils de
cyberdéfense**

Renforcer votre
posture de
cyberdéfense

③



**Signalez une
menace au Centre**

Bénéficier de
l'expertise du Centre

④



**Créer une
communauté**

Avancer la
cybersécurité
ensemble

Qui contacter et Pour quelle raison?

Cyberaide.ca

- Exploitation juvénile, pornographie juvénile, sextorsion, etc.



Royal Canadian Mounted Police
Gendarmerie royale du Canada

- Cybercrime
- Rançongiciels, blanchiment d'argent, vol d'identité, cyberintimidation, etc.

Canadian Anti-Fraud Centre



CAFC

Centre antifraude du Canada

- Courriels personnalisés de hameçonnage, être ciblé par le télémarketing ou des fraudes d'impôts.

CANADIAN CENTRE FOR
CYBER SECURITY

- Pour des cyber incidents urgents, le partage de logiciel malicieux, avis et conseils généraux.

Tirez parti du Centre pour la cybersécurité

Inscrivez-vous
auprès du Centre
pour la cybersécurité
pour recevoir des
alertes et de
l'information.

Profitez de
l'**expertise** publique
et commerciale pour
améliorer vos
capacités et votre
résilience.

Contactez-nous

- Si vous êtes victime d'un cyberincident
- Si vous avez des questions de cybersécurité

Vous avez une idée
ou un projet dont
bénéficierait
grandement
l'écosystème?
Nous voulons en
savoir plus!

RESTEZ EN CONTACT AVEC NOUS



@CST_CSE



contact@cyber.gc.ca



www.cyber.gc.ca



@centrecyber_ca

Pour signaler une fraude :

Centre antifraude du Canada

1-888-495-8501

www.antifraudcentre-centreantifraude.ca

Pour signaler un cybercrime :

Service de police local ou

Gendarmerie royale du Canada

www.rcmp-grc.gc.ca

Pour signaler du pourriel :

Centre de notification des pourriels

pourriel@combattrelepourriel.gc.ca

www.antifraudcentre-centreantifraude.ca