COVID-19 Monthly Update – February 18, 2022 / COVID-19 - Mise à jour du mois – le 18 février 2022

***** Le français suit *****

Hello,

We would like to send you a few updates regarding COVID-19 and ask you to share this information in your networks. Please continue to consult the **AAFC website** regularly for updates. Please note that we have included an additional section with general information about the agriculture and agri-food sector.

Please be reassured that AAFC will send updated information as soon as it becomes available.

INFORMATION ON COVID-19

1. **Switch Health Introduces Corporate Accounts for the Temporary Foreign Worker Program**
   On February 26, 2022, Switch Health will be incorporating the Temporary Foreign Worker (TFW) Program into its corporate platform. Corporate ASMO (Switch Health's proprietary patient portal) will allow those involved with the management of TFWs in your organization to easily access, oversee, and store workers' results in one secure account, using a unique Corporate Code as your identifier.

   All employers **must** contact a Switch Health Account Manager **before February 25, 2022, at 2:00 p.m. EST** to receive a **Corporate Code,** and unique login link to **Corporate ASMO**. Corporate ASMO is the reconstructed ASMO experience for corporate use. Account Managers can be reached at: tfw-canada@switchhealth.ca. **For more details, please consult the attached document.**
2. **Government of Canada lightens border measures as part of transition of the pandemic response**
   On February 15, 2022, the Government of Canada announced a series of adjustments to the current border measures, representing the beginning of a phased easing of travel restrictions. The ability of the country to transition to a new phase at the border is a result of the actions of tens of millions of Canadians across the country who followed public health measures, including getting themselves and their families vaccinated.
3. **Results of the Labour Shortages and Supply Chain Challenges survey**
   Public Safety Canada conducted a brief survey between January 30 and February 3, 2022, which received responses from 419 individuals. The survey was shared directly with over 700 Critical Infrastructure (CI) owners and operators, Provincial and Territorial governments, and national CI related associations.
   The responses to the survey were provided by CI stakeholders, and are meant to provide a snapshot in time of the labour shortages and supply chain challenges facing industry during that date range. The results represent the input from participants and do not provide a complete picture of the actual labour shortages and supply chain challenges in Canada. **You will find attached an overview of all CI sectors results and a presentation made at the Multi-Sectoral Network (MSN).**
4. **Ransomware Toolkit and presentation from the Canadian Centre for Cyber Security**
   Attached please find a presentation on a Ransomware toolkit that the Canadian Centre for Cyber Security has prepared. **For more details, consult the attached toolkit and presentation.**

If you want to have a presentation made to your members on this toolkit please contact Lindsay.macdonald@cyber.gc.ca.

5. **Canadian Centre for Occupational Health and Safety (CCOHS) COVID-19 Resources**

Throughout this pandemic, CCOHS, in partnership with the Public Health Agency of Canada, has developed a variety of products/services to help provide high-level COVID-19 related guidance in relation to public health, infection prevention, occupational safety guidance, training, and knowledge transformation to support a wide range of employment sectors and organizations across Canada, including the agriculture and agri-food sector.

CCOHS : Coronavirus (COVID-19) – Tips :

- Reducing Return Anxiety - Returning to the workplace after working remotely during the COVID-19
- Return to Work During COVID-19: Considerations for a Hybrid Workplace
- CCOHS: Get the Facts on Masks

All CCOHS COVID-19 Health and Safety Resources are available here and on the CCOHS Safe Work App for FREE in both English and French.

6. **Information on Coronavirus disease (COVID-19) from the Public Health Agency of Canada**

There are a number of updated resources available on the Public Health Agency of Canada website for the public including an Outbreak Update and the COVID-19 Virtual Assistant: Coronavirus disease (COVID-19). Your organization may also be interested in:

General information:

- **Update**: National Advisory Committee on Immunization (NACI): Meetings
- **Update**: Reducing COVID-19 risk in community settings: A tool for operators
- **Update**: Statement on COVID-19 and International Travel
- **Update**: Public health management of cases and contacts associated with COVID-19
- **Update**: Vaccines for COVID-19: How to get vaccinated
- **Update**: Vaccination and pregnancy: COVID-19

Coronavirus disease (COVID-19): Travel restrictions, exemptions and advice

Coronavirus disease (COVID-19): Awareness resources

For any questions: **phac.hpoc.stakeholders-partiesprenantes.cops.aspc@canada.ca**

We encourage you to share your comments and questions in writing through the AAFC Roundtable account (aafc.roundtable-tableronde.aac@agr.gc.ca).

Industry Engagement Division
Agriculture and Agri-Food Canada
Government of Canada

****

Bonjour,

Nous souhaitons vous faire part de quelques mises à jour concernant la COVID-19 et vous demandons de diffuser ces renseignements dans vos réseaux. Veuillez continuer à consulter régulièrement le **site Web d'AAC** pour les mises à jours les plus récentes. **Veuillez noter que nous avons inclus une section supplémentaire avec des informations générales se rapportant au secteur de l'agriculture et de l'agroalimentaire.**

Soyez assuré qu'AAC enverra des informations actualisées dès qu'elles seront disponibles.

INFORMATION SUR LA COVID-19

1. **Switch Health instaure des comptes d'entreprise pour le Programme des travailleurs étrangers temporaires**
   Le 26 février 2022, Switch Health intégrera le Programme des travailleurs étrangers temporaires dans sa plateforme pour entreprises. Le portail ASMO (le portail propriétaire des patients de Switch Health) pour entreprises permettra aux personnes impliquées dans la gestion des TET dans votre organisation d'accéder facilement aux résultats des travailleurs, de les superviser et de les enregistrer dans un compte sécurisé, à l'aide d'un code d'entreprise unique comme identifiant.

   Tous les employeurs **doivent** contacter un gestionnaire de comptes de Switch Health avant le 25 février 2022 à 14 h 00 (heure de l'Est) pour recevoir un **code d'entreprise** et un lien de connexion unique vers le portail **ASMO pour entreprises**. Le portail ASMO pour entreprises est la version repensée de l'expérience ASMO destinée aux entreprises. Les gestionnaires de comptes peuvent être contactés à l'adresse suivante: tfw-canada@switchhealth.ca. **Pour plus de détails, veuillez consulter le document ci-joint.**

2. **Le gouvernement du Canada assouplit les mesures frontalières pour la transition de la réponse à la pandémie**
   Le 15 février 2022, e gouvernement du Canada a annoncé une série de modifications aux mesures frontalières ce qui signale le début des allègements des restrictions en matière de voyage. La capacité du pays à entamer une nouvelle phase à la frontière est attribuable aux gestes de dizaines de millions de Canadiens partout au pays qui ont respecté les mesures de santé publique, y compris de se faire vacciner et de faire vacciner leur famille.
3. **Résultats du sondage sur les pénuries de main-d'œuvre et la chaîne d'approvisionnement**
   Sécurité publique Canada a mené un bref sondage entre le 30 janvier et le 3 février 2022, auquel ont répondu 419 personnes. Le sondage a été partagé directement avec plus de 700 propriétaires et exploitants d'infrastructures essentielles (IE), gouvernements provinciaux et territoriaux et associations nationales liées aux IE.

   Les réponses au sondage ont été fournies par les intervenants du secteur des IE et visent à donner un aperçu des pénuries de main-d'œuvre et des problèmes de chaîne d'approvisionnement auxquels l'industrie sera confrontée à cette date. Les résultats représentent l'apport des participants et ne donnent pas une image complète des pénuries de main-d'œuvre et des défis de la chaîne d'approvisionnement au Canada. **Vous trouverez ci-joint un aperçu des résultats de tous les secteurs des IE et une présentation faite au Réseau multisectoriel (RM).**

4. **Boîte à outils sur les rançongiciels et présentation du Centre canadien pour la cybersécurité**

Vous trouverez ci-joint une présentation sur une boîte à outils sur les rançongiciels que le Centre canadien de cybersécurité a préparée. **Pour plus de détails, consultez la boîte à outils et la présentation ci-jointes.**

Si vous souhaitez faire une présentation à vos membres sur cette boîte à outils, veuillez contacter Lindsay.macdonald@cyber.gc.ca

5. **Ressources relatives à la COVID-19 du Centre canadien d'hygiène et de sécurité au travail (CCHST)**
Pendant la pandémie, le CCHST, en partenariat avec l'Agence de la santé publique du Canada, a élaboré une variété de produits et de services pour aider à assurer une orientation de haut niveau liée à la COVID-19 en ce qui concerne la santé publique, la prévention des infections, les lignes directrices en matière de sécurité au travail, la formation et la transformation des connaissances afin d'appuyer un large éventail de secteurs d'emploi et d'organisations partout au Canada, y compris le secteur de l'agriculture et de l'agroalimentaire.

CCHST: Coronavirus (COVID-19) - Conseils :

- Réduire l'anxiété de déconfinement - retour sur le lieu de travail après avoir travaillé à distance pendant la pandémie de COVID-19
- Retour au travail pendant la COVID-19 : Considérations liées au milieu de travail hybride
- CCHST : Obtiens les faits sur les masques

Toutes les ressources du CCHST sur la santé et la sécurité du COVID-19 sont disponibles ici et sur l'application CCHST - Sécurité au travail GRATUITEMENT en anglais et en français.

6. **Informations sur les maladies à coronavirus (COVID-19) de l'Agence de la santé publique du Canada**
Il y a un certain nombre de ressources mises à jour disponibles sur le site Web de l'Agence de santé publique du Canada pour le public, ainsi que pour les professionnels de la santé, y compris notre **Mise à jour sur l'éclosion** et la **assistant virtuel COVID-19** : Maladie à coronavirus (COVID-19).

Informations générales:

- **Mise à jour** : Comité consultatif national de l'immunisation (CCNI) : Réunions
- **Mise à jour** : Réduire le risque de COVID-19 en milieu communautaire : Un outil pour les exploitants
- **Mise à jour** : Déclaration sur les voyages internationaux relativement à la COVID-19
- **Mise à jour** : Prise en charge par la santé publique des cas de COVID-19 et des contacts qui y sont associés
- **Mise à jour** : Vaccination contre la COVID-19 : Manière de se faire vacciner
- **Mise à jour** : Vaccination et grossesse : COVID-19

Maladie à coronavirus (COVID-19): Restrictions, exemptions et conseils en matière de voyages

Maladie à coronavirus (COVID-19): Ressources de sensibilisation

Pour toutes questions: **phac.hpoc.stakeholders-partiesprenantes.cops.aspc@canada.ca**

Nous vous encourageons à nous faire part de vos commentaires et questions par écrit via le compte de la table ronde d'AAC (aafc.roundtable-tableronde.aac@agr.gc.ca).

Division de la consultation du secteur
Agriculture et Agroalimentaire Canada
Gouvernement du Canada

Switch Health Introduces Corporate Accounts for the Temporary Foreign Worker Program

On February 26, 2022, Switch Health will be incorporating the Temporary Foreign Worker Program into its corporate platform. Corporate ASMO will allow those involved with the management of TFWs in your organization to easily access, oversee, and store workers' results in one secure account, using a unique Corporate Code as your identifier. Even if your email address or phone number changes, this code will remain the same, ensuring your workers' results are always posted under the correct account.

All employers **must** contact a Switch Health Account Manager before February 25, 2022, at 2:00pm EST to receive a **Corporate Code,** and unique login link to **Corporate ASMO**. Corporate ASMO is the reconstructed ASMO experience for corporate use. Account Managers can be reached at tfw-canada@switchhealth.ca

Until February 25, 2022, there will be no changes to the existing system. **On February 26, 2022, all employers must start using their Corporate Accounts** as Switch Health will now be assigning Corporate Codes to all incoming workers upon their arrival at Pearson International Airport. While you may still request a Corporate Account and Corporate Code at any moment, failure to do so before February 25, 2022, at 2:00pm EST will result in delays receiving your worker's results.

A complete guide to the revised process will be distributed in the upcoming days.

Account Managers will be responsible for creating a Corporate ASMO Account for your operation and providing you with all registration and login instructions.

1. Please email tfw-canada@switchhealth.ca to request your Corporate Account and provide the following information:
    - ✓ Name of your Operation
    - ✓ First Names and Last Names
    - ✓ Emails
    - ✓ Cell Phone Numbers

    *Provide **up to 3 complete names, emails, and cell phone numbers. Corporate ASMO allows for 3 members of your operation to manage the account. Clearly indicate which of the 3 individuals is the Operation Lead.**

    * If your organization has several Operations, but the same management staff, they will only need 1 Corporate Account under the umbrella name of your organization.

    *If your organization has several Operations, each with their own management staff, you will need to request a Corporate Account/Corporate Code for each Operation and their respective staff.

2. An Account Manager will create your Corporate ASMO account based on the information you provide. The 3 individuals will each receive separate emails with their temporary password,

within 15-20 minutes of the account setup. They will also receive emails with the Corporate Code and an attachment with instructions to register into the account. Requests for Corporate Accounts will be responded to within 24 hours (Monday-Friday).

3. You will receive a confirmation email with a unique link to your corporate account.
4. Complete registration to your newly created Corporate ASMO account using the link and password provided.

Keeping Canadians and visiting workers safe during COVID-19 is our top priority.

Switch Health instaure des comptes d'entreprise pour le Programme des travailleurs étrangers temporaires

Le 26 février 2022, Switch Health intégrera le Programme des travailleurs étrangers temporaires dans sa plateforme pour entreprises. Le portail ASMO pour entreprises permettra aux personnes impliquées dans la gestion des TET dans votre organisation d'accéder facilement aux résultats des travailleurs, de les superviser et de les enregistrer dans un compte sécurisé, à l'aide d'un code d'entreprise unique comme identifiant. Même si votre adresse courriel ou votre numéro de téléphone changent, ce code restera le même, ce qui garantit que les résultats de vos travailleurs seront toujours affichés sous le bon compte.

Tous les employeurs **doivent** contacter un gestionnaire de comptes de Switch Health avant le 25 février 2022 à 14 h 00 (heure de l'Est) pour recevoir un **code d'entreprise** et un lien de connexion unique vers le portail **ASMO pour entreprises**. Le portail ASMO pour entreprises est la version repensée de l'expérience ASMO destinée aux entreprises. Les gestionnaires de comptes peuvent être contactés à l'adresse suivante : tfw-canada@switchhealth.ca.

Jusqu'au 25 février 2022, il n'y aura aucun changement au système existant. Le 26 février 2022, tous les employeurs doivent commencer à utiliser leurs comptes d'entreprise, car Switch Health attribuera désormais des codes d'entreprise à tous les travailleurs entrants à leur arrivée à l'aéroport international Pearson. Bien que vous puissiez toujours demander un compte d'entreprise et un code d'entreprise à tout moment, si vous ne le faites pas avant le 25 février 2022 à 14 h 00 (heure de l'Est), la réception des résultats de votre travailleur sera retardée.

Un guide complet du processus révisé sera distribué dans les prochains jours.

Les gestionnaires de comptes seront chargés de créer un compte ASMO d'entreprise pour votre exploitation agricole ou entreprise et de vous fournir toutes les instructions d'inscription et de connexion.

1. Veuillez envoyer un courriel à tfw-canada@switchhealth.ca pour demander votre compte d'entreprise et fournir les renseignements suivants :
    a. Nom de l'exploitation agricole ou de l'entreprise
    b. Prénoms et noms de famille
    c. Addresses courriel
    d. Numéros de téléphone cellulaire

*Fournissez **jusqu'à 3 noms complets, adresses courriel et numéros de téléphone cellulaire. Le portail ASMO pour entreprise permet à 3 membres de votre exploitation de gérer le compte.** Indiquez clairement laquelle de ces 3 personnes est le responsable des opérations.

* Si votre entreprise a plusieurs exploitations, mais le même personnel de gestion, vous n'aurez besoin que d'un seul compte d'entreprise sous le nom général de votre entreprise.

*Si votre organisation a plusieurs exploitations, chacune avec son propre personnel de gestion, vous devrez demander un compte d'entreprise/code d'entreprise pour chaque exploitation et son personnel respectif.

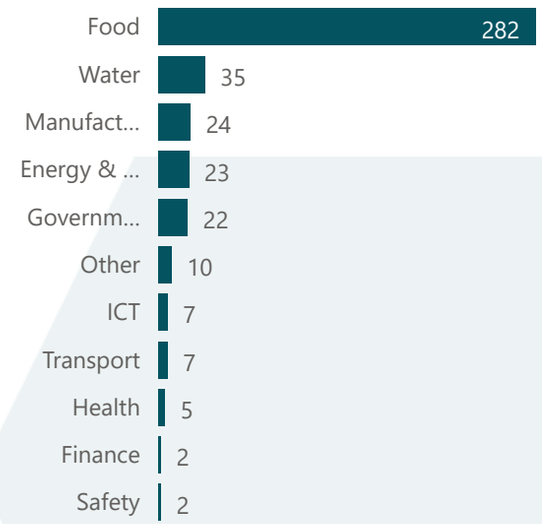
2. Un gestionnaire de compte créera votre compte ASMO d'entreprise sur la base des renseignements que vous aurez fournis. Les 3 personnes recevront chacune un courriel séparé avec leur mot de passe temporaire, dans les 15-20 minutes suivant la création du compte. Elles recevront également un courriel avec le code d'entreprise et une pièce jointe avec les instructions pour s'inscrire au compte. Les demandes de compte d'entreprise seront traitées dans un délai de 24 heures (du lundi au vendredi).

3. Vous recevrez un courriel de confirmation contenant un lien unique vers votre compte d'entreprise.
4. Complétez l'inscription au compte ASMO d'entreprise que vous venez de créer en utilisant le lien et le mot de passe fournis.

Assurer la sécurité des Canadiens et des travailleurs étrangers temporaires pendant la COVID-19 est notre priorité absolue.

Context of Respondents

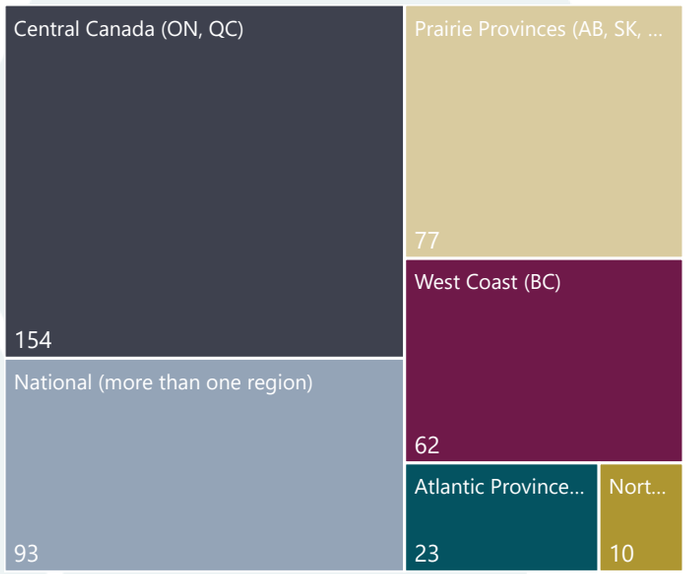
Count of respondents by CI sector



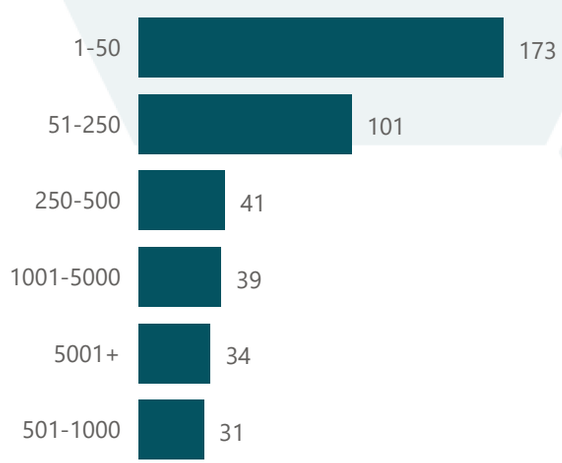
Breakdown by CI sector and subsector

Sectors	Count
Food	**282**
Food and beverage processing and manufacturing	85
Crop production (including grains, oilseeds, fruit and vegetables)	58
Livestock production (including beef, pork, poultry, sheep/lamb, goat, eggs, dairy)	56
Grain processing and handling	22
Agricultural inputs (fertilizer, extraction, processing, potash)	19
Meat and dairy processing	16
Fish and seafood production and processing (including aquaculture, marine harvesting)	14
Food and beverage distribution	9
Food and beverage retailers	3
Water	**35**
Potable or drinking water supply (storage, treatment, distribution)	22
Water supply (distribution, treatment, storage)	8
Wastewater removal	5
Total	**419**

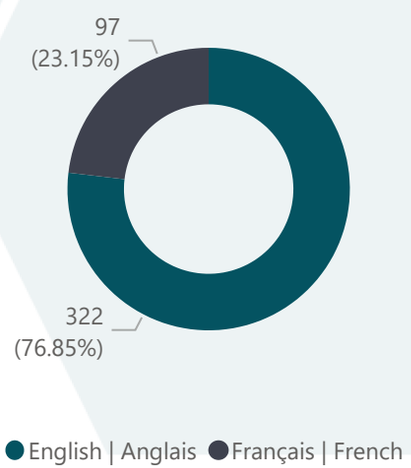
Breakdown by region of operation



Count by size of workforce



Language of respondents



Impacts by Sector

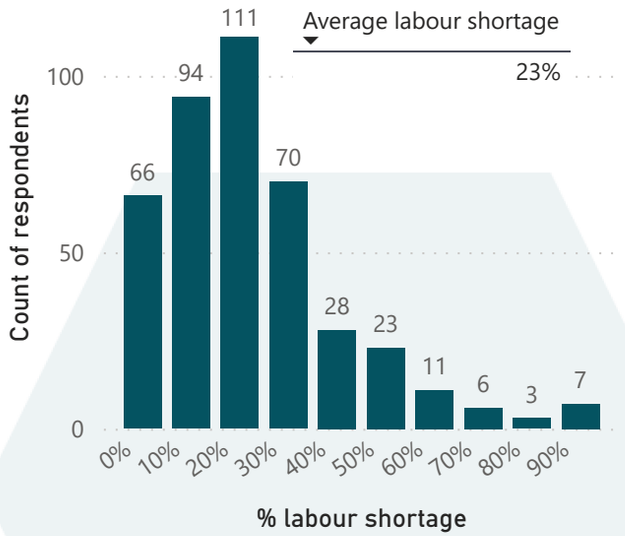
Degree of impacts by type of factors (0 = no disturbance, 5 = maximum disturbance)

CI sectors	Absenteeism	Labour shortages	Access to inputs/supplies	Transport delays	Changes in demand	Public health measures	Access to rapid test kits	Access to transport
Energy & Utilities	2.43	2.35	3.09	3.22	2.33	2.74	2.52	1.87
Finance	3.00	3.00	1.00	1.00	1.00	2.50	2.50	1.00
Food	2.89	3.29	3.48	3.67	2.92	2.95	2.50	2.87
Government	2.52	2.55	3.10	2.90	2.61	2.81	2.83	2.33
Health	3.40	3.20	3.40	3.75	4.00	4.00	2.50	2.50
ICT	2.29	2.14	2.83	2.67	2.71	2.71	2.50	1.60
Manufacturing	2.88	3.04	3.67	4.00	2.92	3.04	2.46	3.18
Other	2.80	3.00	3.50	3.80	3.10	3.33	2.56	2.90
Safety	3.00	3.00	2.00	2.50	2.50	2.00	3.00	2.50
Transport	2.43	3.00	2.43	3.57	2.86	2.86	1.86	2.80
Total	**2.77**	**3.05**	**3.36**	**3.55**	**2.80**	**2.91**	**2.46**	**2.69**

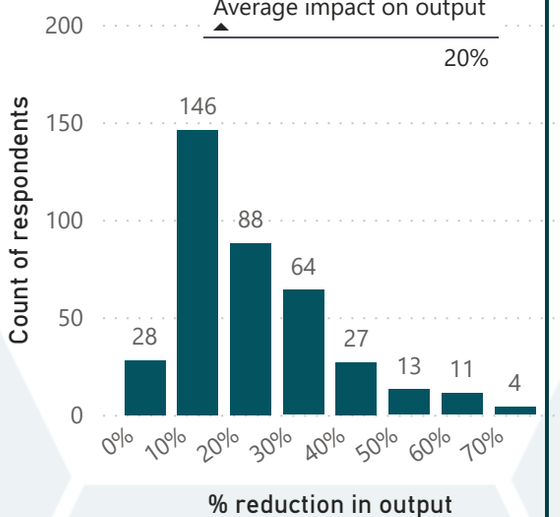
Canada

Labour Shortages and Associated Impacts

Labour shortage

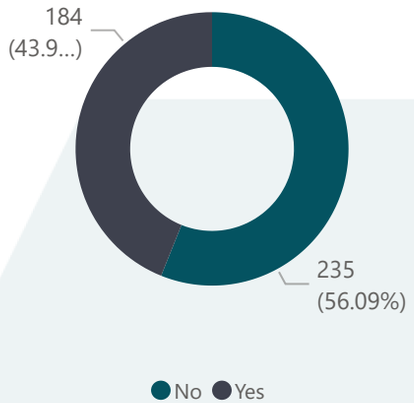


Reduction in output due to labour shortages



Distribution and Associated Challenges

Are you experiencing challenges distributing your products/services?

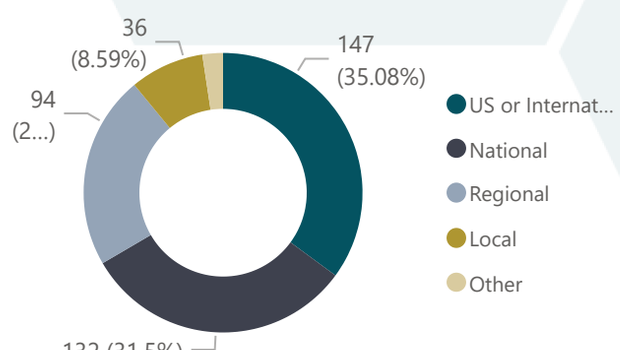


Degree to which factors are impacted in distribution challenges (1 = minimal impact, 5 = critical impact)

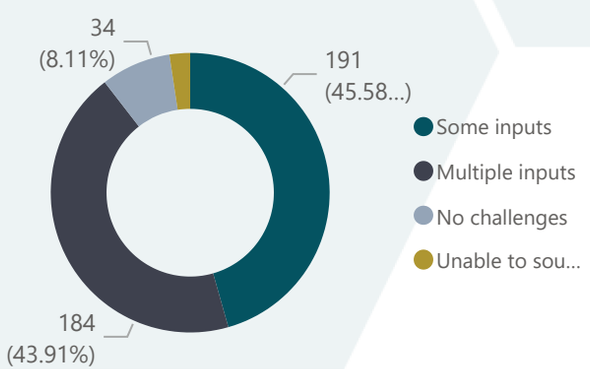
CI sectors	Loss of revenue	Cost of storage	Waste	Follow-on supply-chain impacts	Animal welfare
Energy & Utilities	2.60	2.00	1.80	3.80	1.00
Food	3.60	3.08	2.34	3.65	2.14
Manufacturing	3.33	3.00	1.75	3.00	1.43
Other	3.50	2.17	1.80	2.83	1.33
Transport	3.00	3.67	2.00	3.75	2.00
Water	2.80	1.83	1.60	2.20	1.00
Total	**3.51**	**2.98**	**2.25**	**3.54**	**2.00**

Sources of Input and Associated Challenges

From where are the majority of materials critical to your organization's production/distribution of goods and/or services sourced?



Are you experiencing challenges sourcing the materials and inputs you require to produce/distribute your goods and/or services?

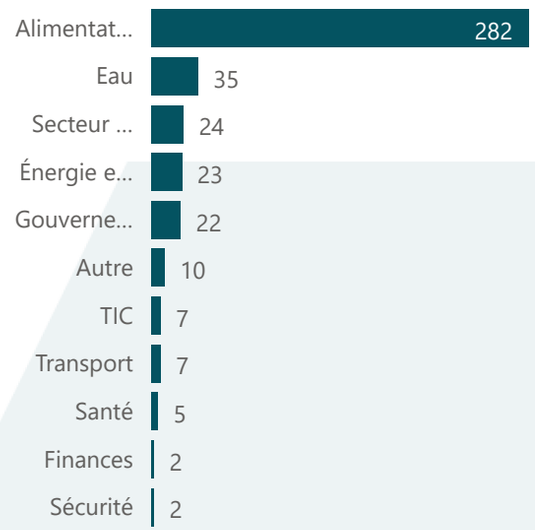


Degree to which factors are impacting ability to source materials (1 = minimal impact, 5 = critical impact)

CI sectors	Price inflation	Transport delays or cancellations	Suppliers have reduced supply (domestic)	Global supply chain issues
Energy & Utilities	2.86	3.45	3.41	3.48
Food	3.93	3.93	3.78	3.93
Government	3.25	3.82	3.63	3.81
Health	2.00	2.75	3.25	4.00
ICT	2.33	2.75	3.25	3.25
Manufacturing	3.55	4.41	3.86	4.36
Other	3.56	4.22	3.67	4.11
Safety	2.50	3.50	3.00	3.00
Transport	4.50	4.33	4.50	4.50
Water	3.17	3.50	3.33	3.47
Total	**3.72**	**3.87**	**3.7**	**3.9**

Aperçu des répondants·es

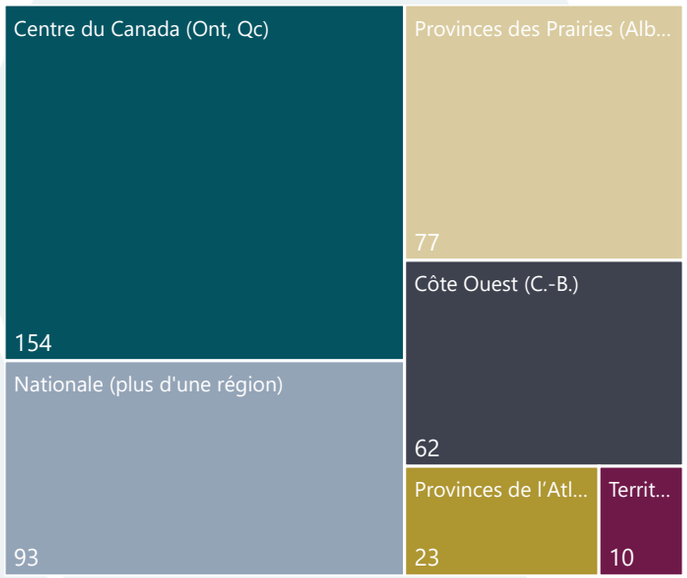
Nombre de répondants·es par secteur des IE



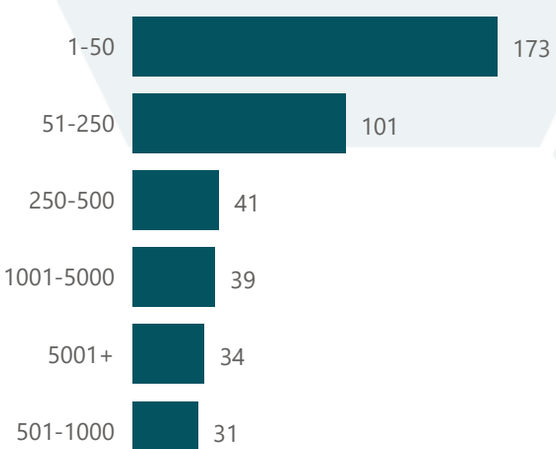
Répartition par secteur et sous-secteur des IE **

Secteur des IE	Compte
Alimentation	**282**
Transformation et fabrication d'aliments et de boissons	85
Cultures agricoles (y compris les grains, les oléagineux, les fruits et les légumes)	58
Production de bétail (y compris le bœuf, le porc, la volaille, le mouton et l'agneau, la chèvre, les œufs, troupeau)	56
Transformation des céréales et leur manipulation	22
Intrants agricoles (engrais, extraction, transformation, potasse)	19
Transformation de la viande et des produits laitiers	16
Production et transformation du poisson et des fruits de mer (y compris l'aquaculture, les récoltes marines)	14
Distribution d'aliments et de boissons	9
Détaillants en aliments et boissons	3
Eau	**35**
Approvisionnement en eau potable (stockage, traitement, distribution)	22
Total	**419**

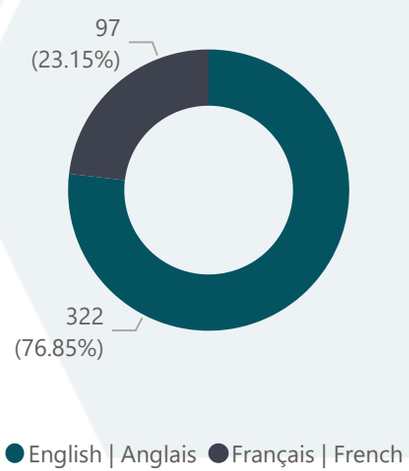
Répartition par région d'activité



Décompte selon la taille de la main-d'œuvre



Langue des répondants·es



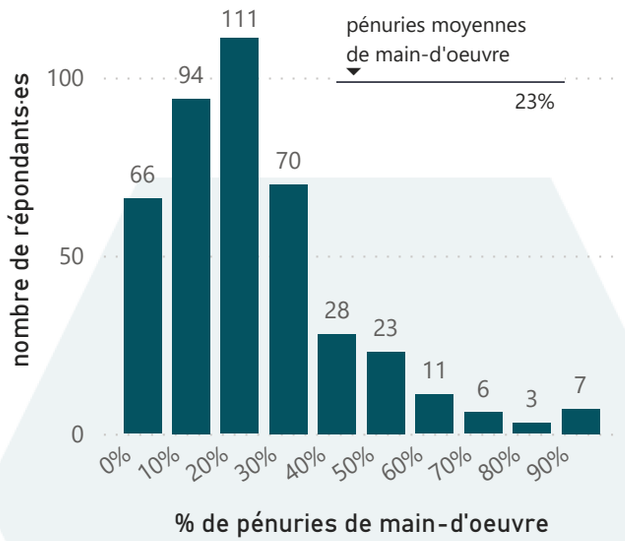
Impacts par secteur

Degré des impacts par type de facteurs (0 = aucune perturbation, 5 = perturbation maximale)

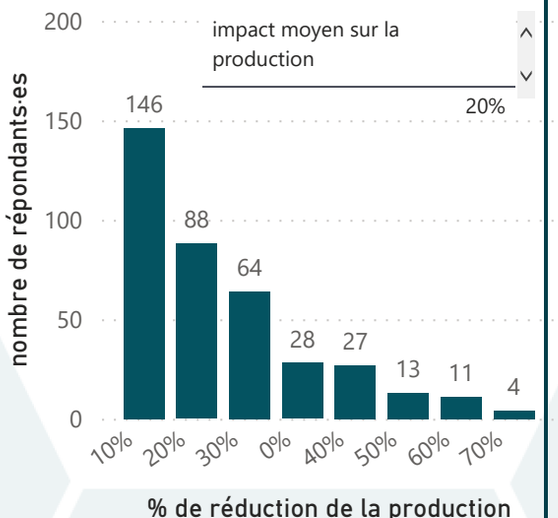
Critical Infrastructure sector	Absentéisme	Pénurie de main-d'œuvre	Accès aux sources d'apport / matériel	Retards dans les transports	Changements dans la demande	Mesures de santé publique	Accès aux kits de test rapide	Accès aux transports
Secteur Manufacturier	2.88	3.04	3.67	4.00	2.92	3.04	2.46	3.18
Autre	2.80	3.00	3.50	3.80	3.10	3.33	2.56	2.90
Alimentation	2.89	3.29	3.48	3.67	2.92	2.95	2.50	2.87
Santé	3.40	3.20	3.40	3.75	4.00	4.00	2.50	2.50
Gouvernement	2.52	2.55	3.10	2.90	2.61	2.81	2.83	2.33
Énergie et services publics	2.43	2.35	3.09	3.22	2.33	2.74	2.52	1.87
Eau	2.20	2.17	2.94	3.09	1.94	2.53	1.90	1.77
TIC	2.29	2.14	2.83	2.67	2.71	2.71	2.50	1.60
Transport	2.43	3.00	2.43	3.57	2.86	2.86	1.86	2.80
Sécurité	3.00	3.00	2.00	2.50	2.50	2.00	3.00	2.50
Total	**2.77**	**3.05**	**3.36**	**3.55**	**2.80**	**2.91**	**2.46**	**2.69**

Pénuries de main-d'œuvre et impacts associés

Pénuries de main-d'oeuvre

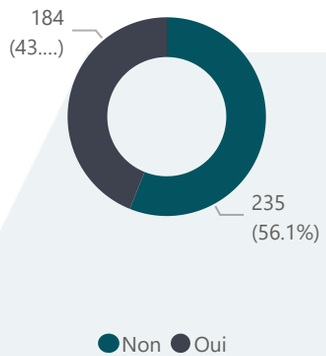


Réduction de la production en raison d'une pénurie de main-d'œuvre



Distribution et enjeux associés

Vous rencontrez des difficultés pour distribuer vos produits / services ?

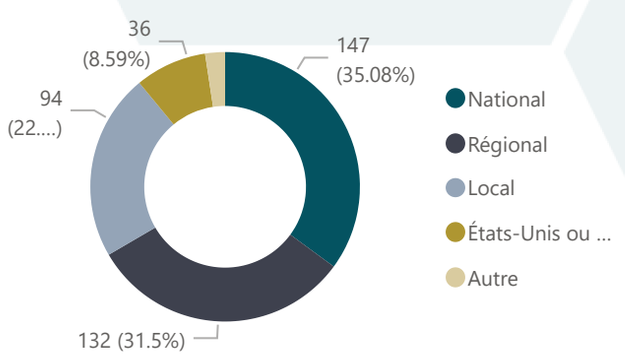


Degré d'impact des facteurs sur la distribution (1 = impact minimal, 5 = impact critique)

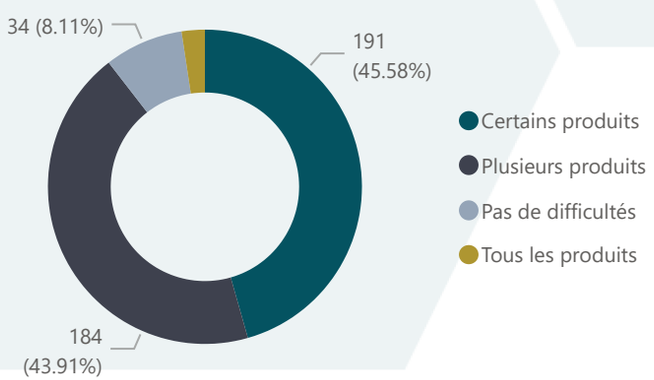
Secteur des IE	Perte de revenus	Frais de dépôt des marchandises	Gaspillage	Répercussions sur la chaîne d'approvision nement	Bien-être des animaux
Alimentation	3.60	3.08	2.34	3.65	2.14
Autre	3.50	2.17	1.80	2.83	1.33
Eau	2.80	1.83	1.60	2.20	1.00
Énergie et services publics	2.60	2.00	1.80	3.80	1.00
Secteur Manufacturier	3.33	3.00	1.75	3.00	1.43
Transport	3.00	3.67	2.00	3.75	2.00
Total	**3.51**	**2.98**	**2.25**	**3.54**	**2.00**

Sources d'apport et défis associés

D'où provient la majorité des matières indispensables à la production/distribution de biens et/ou de services de votre organisation?



Éprouvez-vous des difficultés à vous approvisionner en matériel et en matières premières pour la production / distribution de vos biens et/ou services?



Degré auquel les facteurs ont un impact sur la capacité à s'approvisionner en matériaux (1 = impact minimal, 5 = impact critique)

Secteur des IE	Inflation des prix	Retards ou annulations de services de transport	Fournisseurs ont limité leur approvisionnement (national)	Enjeux liés à la chaîne d'approvisionnement mondiale
Alimentation	3.93	3.93	3.78	3.93
Autre	3.56	4.22	3.67	4.11
Eau	3.17	3.50	3.33	3.47
Énergie et services publics	2.86	3.45	3.41	3.48
Gouvernement	3.25	3.82	3.63	3.81
Santé	2.00	2.75	3.25	4.00
Secteur Manufacturier	3.55	4.41	3.86	4.36
Sécurité	2.50	3.50	3.00	3.00
TIC	2.33	2.75	3.25	3.25
Transport	4.50	4.33	4.50	4.50
Total	**3.72**	**3.87**	**3.71**	

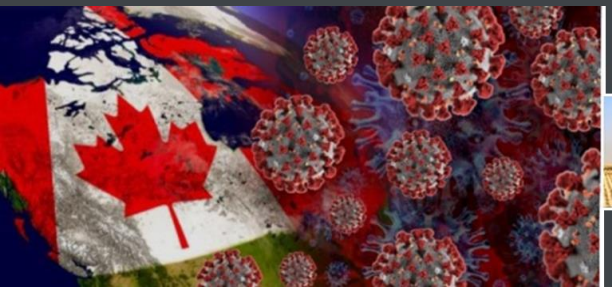
Multi-Sector Network (MSN) Labour Shortages and Supply Chain Challenges to Critical Infrastructure | Feb 2022 Survey Results

The Labour Shortages and Supply Chain Challenges survey collected responses **between Jan. 31 – Feb. 3, 2022**.

The responses to the survey were provided by Critical Infrastructure (CI) stakeholders, and are meant to provide a snapshot in time of the labour shortages and supply chain challenges facing industry during that date range. The results represent the input from participants and do not provide a complete picture of the actual labour shortages and supply chain challenges in Canada.

There were a total of **419 participants** from all CI Sectors.

Public Safety Canada
National and Cyber Security Branch
Critical Infrastructure Directorate
(00360-20)



Introduction

On January 12, 2022, a Multi-Sector Network (MSN) meeting was held with critical infrastructure (CI) stakeholders from across the 10 CI sectors, focused on the impacts of the Omicron variant on critical infrastructure. At the forefront of discussions were labour shortages and supply chain disruptions being experienced by CI stakeholders.

For the purpose of further capturing the impacts being experienced by critical infrastructure, Public Safety Canada then launched a brief survey, which received responses from **419 individuals** between **January 30 and February 3, 2022**. The survey was shared directly with over 700 CI owners and operators, Provincial and Territorial governments, and national CI related associations, and email recipients were also encouraged to share the survey link freely within their sectors. Highlights from the information gathered though the survey have been compiled in this report, and further detail can be obtained by accessing the Power BI tool.

Key Findings

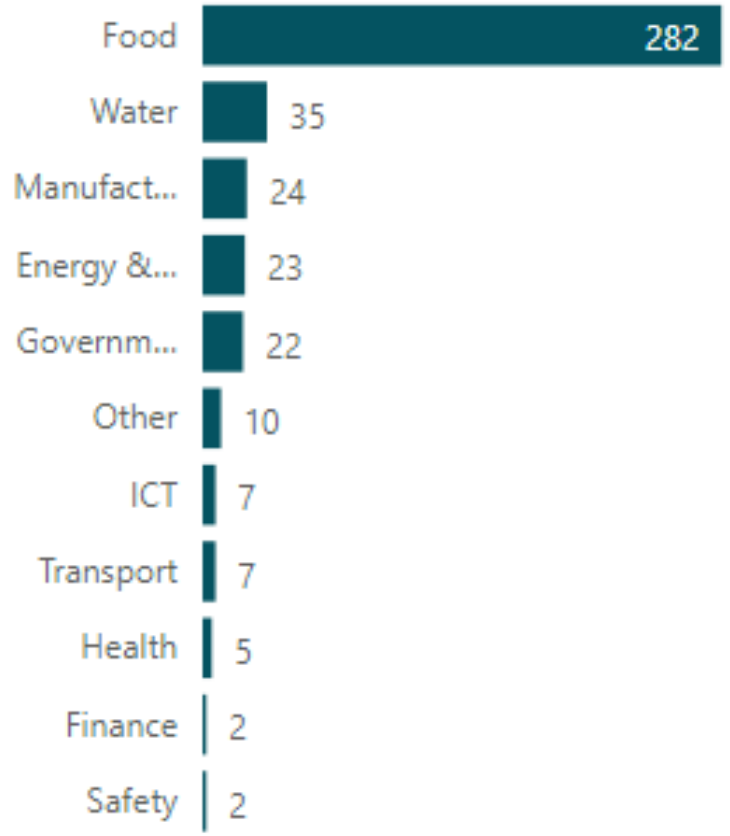
- Across all sectors, the **average labour shortage was reported to be 23%**, with an **average reduction of output of 20%**
  - The **highest rates of labour shortages** were reported in the **Food, Finance,** and **Safety sectors**

- **92%** of respondents indicated that that they were experiencing **challenges sourcing some or all of the materials and inputs required** to produce and/or distribute their goods and/or services
  - Transportation disruptions are having a significant impact on CI production of goods as the majority of inputs are sourced nationally or internationally (including from the US)
  - Three CI sectors (**Food, Health,** and **Manufacturing**) indicated that the factor impacting them most severely was **labour shortages**

Number of Respondents by CI Sector

The survey received a total of **419 responses**, with the three highest level of respondents from the Food (282), Water (35), and Manufacturing sectors (24).

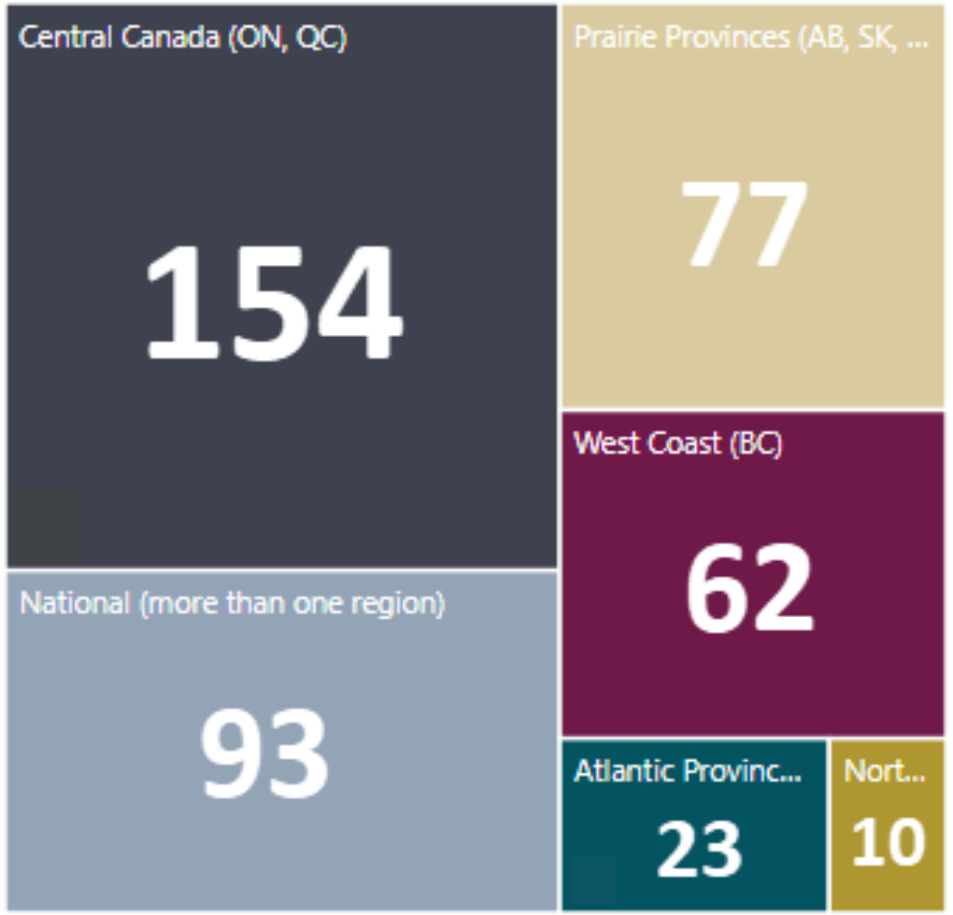
Given the high number of Food sector respondents, it should be noted that the analysis may be biased towards the issues faced by this particular CI sector.



Breakdown by Region of Operation

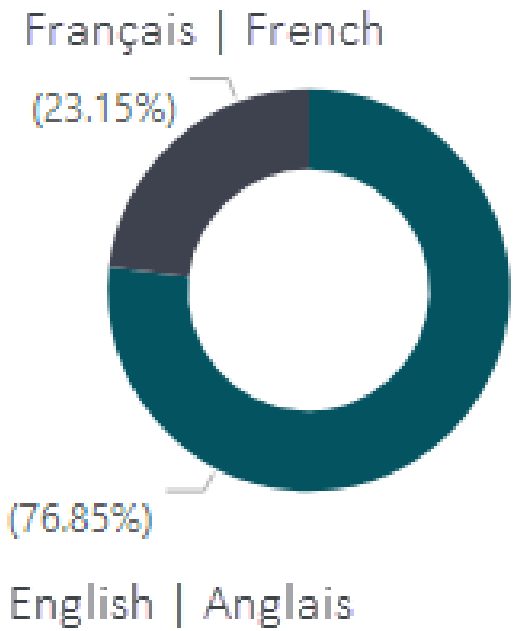
Respondents were located in:

- **Central Canada** (QC, ON) (154 surveys)
- **Nationally** (in more than one region) (93 surveys)
- **Prairies** (AB, SK, MB) (77 surveys).
- **West Coast** (BC) (62 surveys),
- **Atlantic** (NS, NB, NL, PE) (23 surveys)
- **Northern Territories** (NU, NT, YT) (10 surveys).



Language of Respondents

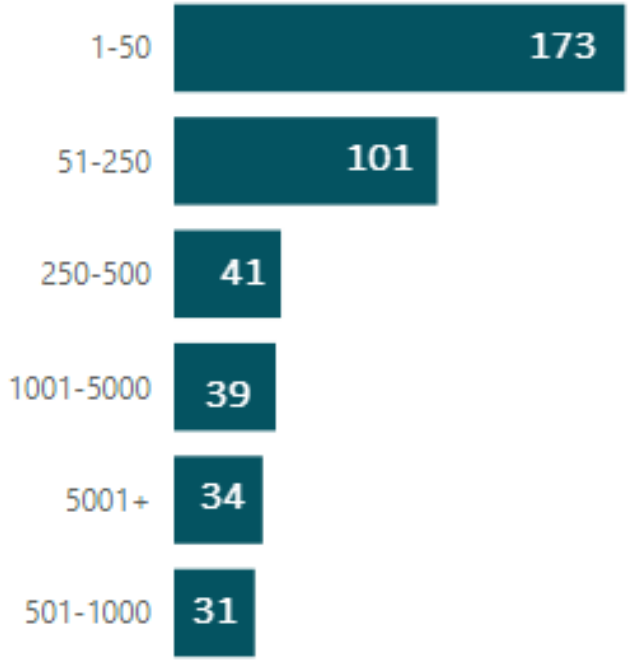
77% of respondents completed the survey in English and 23% in French. The respondents who completed the survey in French were overwhelmingly operating in Atlantic Provinces and Central Canada, or Nationally.



Size of Workforce

Small and medium sized enterprises and organizations represented the majority of respondents.

65% of responding organizations **had fewer than 250 employees**.



Canada

Impacts by Sector

Respondents were asked to indicate to what degree certain factors are currently affecting the organization's operational capacity, where 1 = no disturbance, and 5 = maximum disturbance. The responses revealed that the two factors most impacting CI sectors, with the exception of the Finance sector, are **transportation delays** and challenges with **access to inputs/supplies**.

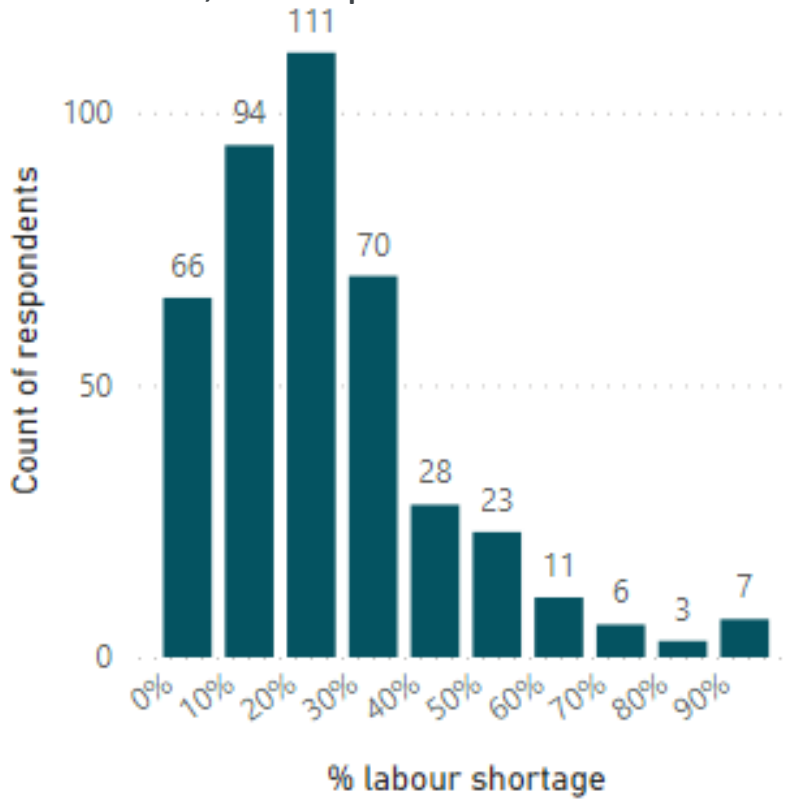
- Three CI sectors (**Food, Health**, and **Manufacturing**) indicated that the factor impacting them most severely was **labour shortages**

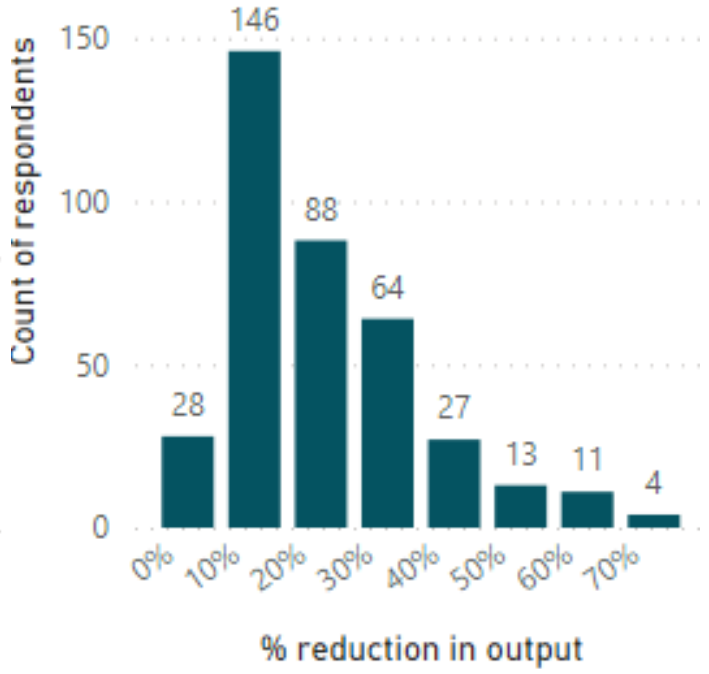
CI sectors	Absenteeism	Labour shortages	Access to inputs/supplies	Transport delays	Changes in demand	Public health measures	Access to rapid test kits	Access to transport
Energy & Utilities	2.43	2.35	3.09	3.22	2.33	2.74	2.52	1.87
Finance	3.00	3.00	1.00	1.00	1.00	2.50	2.50	1.00
Food	2.89	3.29	3.48	3.67	2.92	2.95	2.50	2.87
Government	2.52	2.55	3.10	2.90	2.61	2.81	2.83	2.33
Health	3.40	3.20	3.40	3.75	4.00	4.00	2.50	2.50
ICT	2.29	2.14	2.83	2.67	2.71	2.71	2.50	1.60
Manufacturing	2.88	3.04	3.67	4.00	2.92	3.04	2.46	3.18
Other	2.80	3.00	3.50	3.80	3.10	3.33	2.56	2.90
Safety	3.00	3.00	2.00	2.50	2.50	2.00	3.00	2.50
Transport	2.43	3.00	2.43	3.57	2.86	2.86	1.86	2.80
Water	2.20	2.17	2.94	3.09	1.94	2.53	1.90	1.77
Total	**2.77**	**3.05**	**3.36**	**3.55**	**2.80**	**2.91**	**2.46**	**2.69**

Labour Shortages and Associated Impacts

The **labour shortage average was reported to be 23%**, with an **average reduction of output due to labour shortage of 20%**.

- However, 16 respondents indicated that the labour shortage in their organization was at 70% or higher.





The impact of labour shortage on outputs is not directly linear.

- For example, the respondents who indicated that they had a higher than average labour shortage (60-90%) reported a higher than average reduction of outputs (37.75%), but not at the same rate as the labour shortage.

Canada

Distribution & Associated Challenges

44% of respondents indicated that they were experiencing **challenges distributing their products or services**

The three factors most impacted by a CI sector's inability to efficiently distribute their products and/or services were:

- **follow-on supply chain impacts** (3.54)
- **loss of revenue** (3.51); and,
- **cost of storage** (2.98).

Are you experiencing challenges distributing your products/services?

Degree to which factors are impacted in distribution challenges

CI sectors	Loss of revenue	Cost of storage	Waste	Follow-on supply-chain	Animal welfare
Food	3.60	3.08	2.34	3.65	2.14
Transport	3.00	3.67	2.00	3.75	2.00
Energy & Utilities	2.60	2.00	1.80	3.80	1.00
Other	3.50	2.17	1.80	2.83	1.33
Manufacturing	3.33	3.00	1.75	3.00	1.43
Water	2.80	1.83	1.60	2.20	1.00
Total	**3.51**	**2.98**	**2.25**	**3.54**	**2.00**

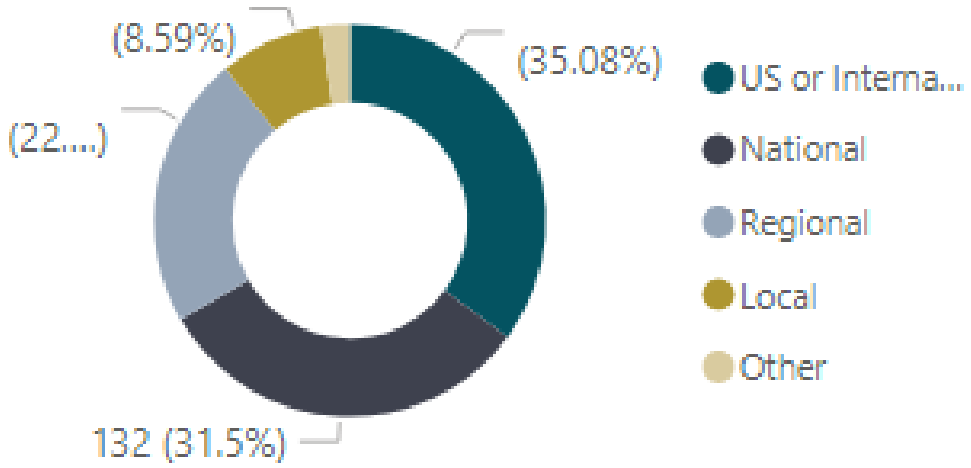
(1=minimal impact, 5= critical impact)

Canada

Sources of Input and Associated Challenges

- 35% of respondents identified that they source the majority of their critical inputs from the **United States or Internationally**.

From where are the majority of materials critical to your organization's production/distribution of goods and/or services sourced?



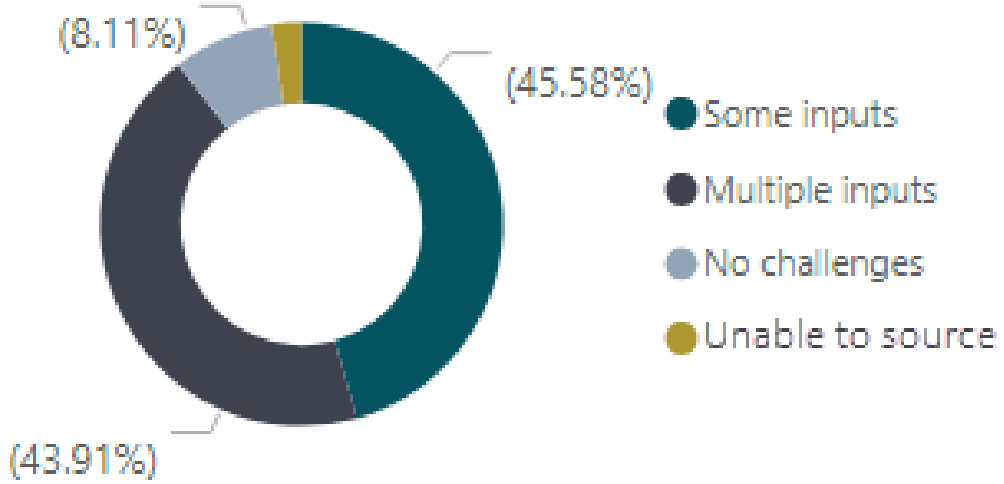
Sources of Input and Associated Challenges (continued)

92% of respondents indicated that that they were experiencing **challenges sourcing some or all of the materials and inputs required** to produce and/or distribute their goods and/or services.

These challenges are related to a number of factors, including:

- Price inflation
- Transportation delays/cancellations
- Reduced supplies of specific goods
- Global supply chain disruptions / delays

Are you experiencing challenges sourcing the materials and inputs you require to produce/distribute your goods and/or services?



Word Cloud Generated from the Survey's Comments Field

Further analysis

Short comments in text fields in the survey were added to a word cloud generator to provide a visual of the words that appeared in higher frequency. Supply, delays, transport, costs, labour and materials were mentioned most frequently in the text fields.

For a more detailed breakdown by CI sector, subsector, region, size of workforce, or other contextual indicator, please view the results in Power BI.

Canada

CANADIAN CENTRE FOR CYBER SECURITY

Ransomware Toolkit
Food Sector Network Meeting – Feb 8 2022

1 Publications

1.1 Ransomware

Ransomware is the most common cyber threat Canadians face and it is on the rise. This link offers resources from the Cyber Centre to help organizations understand the ransomware threat and take action to protect themselves.

Ransomware Playbook
Ransomware: How to prevent and recover
Ransomware: How to recover and get back on track

1.2 How to protect your networks from ransomware

Looking for steps you can take to protect your organization's networks and information from cyber threats? To get you started, we have summarized 13 security controls. By implementing these controls, you can reduce your risks and improve your ability to respond to security incidents. While it isn't always necessary to implement all of the controls, we encourage you to adopt as many as possible to enhance your cyber security.

Top measures to enhance cyber security for small / medium businesses

1.3 How to avoid phishing attacks

Phishing is the most common method for threat actors to deploy ransomware these days. The following publications will help you recognize and avoid a phishing attack.

Don't Take the Bait: Recognize and Avoid Phishing Attacks

The 7 red flags of Phishing

Spotting Malicious Email Messages

2 Cybersecurity Posture Assessment

2.1 Canadian Cyber Security Tool (CCST)

The Canadian Cyber Security Tool (CCST) is a free, virtual self-assessment tool developed by Public Safety Canada (PS) in collaboration with the Cyber Centre. The tool provides the participant with an overview of their organization's operational resilience and cyber security posture, as well as comparative results across their sector.

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-en.aspx

3 On- line Cybersecurity Training

3.1 CyberSecure Canada

CyberSecure Canada is a Federal certification program for small and medium-sized organizations (SMOs). CyberSecure Canada offers a free eLearning series designed to support small and medium organizations (SMOs) to implement baseline cybersecurity controls and improve their cybersecurity posture.

https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00017.html

4 Reporting Cyber I ncidents

Report cybercrimes to the Cyber Centre's online portal to get support and advice on how to protect your organization from being targeted.

Incident Reporting Portal

5 Cyber Centre Products

Interested in receiving threat intelligence, alerts and advisories from the Cyber Centre? Contact contact@cyber.gc.ca

CANADIAN CENTRE FOR CYBER SECURITY

Boîte à outils sur les rançongiciels
Réunion du réseau du secteur de l'alimentation – 8 février 2022

1 Publications

1.1 Rançongiciels

Les rançongiciels sont la cybermenace la plus courante avec laquelle les Canadiens doivent composer, et la tendance est à la hausse.
Ce lien propose des ressources du Centre pour la cybersécurité pour aider les organisations à comprendre la menace que représentent les rançongiciels et à prendre des mesures pour se protéger.

Guide sur les rançongiciels
Rançongiciels : Comment les prévenir et s'en remettre
Rançongiciel : Comment vous en remettre

1.2 Comment protéger vos réseaux contre les rançongiciels

Cherchez-vous des façons de protéger les réseaux et l'information de votre entreprise des cybermenaces? Le présent document résume les 13 catégories de contrôle de sécurité. Grâce à ces contrôles, vous réduirez votre exposition aux risques et serez plus apte à intervenir en cas d'incident de sécurité. Vous n'avez pas nécessairement besoin d'instaurer tous les contrôles, mais nous vous encourageons à en adopter le plus grand nombre possible pour optimiser votre cybersécurité.

Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises

1.3 Comment éviter les attaques par hameçonnage

Le hameçonnage est la méthode la plus utilisée par les auteurs de menaces pour déployer des rançongiciels de nos jours. Les publications suivantes vous aideront à reconnaître et à éviter une attaque d'hameçonnage.

Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage

Les 7 signaux d'alarme de l'hameçonnage

Reconnaître les courriels malveillants

2 Évaluation de la posture de cybersécurité

2.1 Outil canadien de cybersécurité (OCC)

L'Outil canadien de cybersécurité (OCC) est un outil virtuel d'auto-évaluation gratuit, conçu par Sécurité publique Canada (SP), en collaboration avec le Centre de la sécurité des télécommunications (CST) et le Centre canadien de cybersécurité (Centre pour la cybersécurité). L'outil offre au participant un aperçu de la résilience opérationnelle et de la situation en matière de cybersécurité de son organisation, ainsi que des résultats comparatifs dans l'ensemble de son secteur.

https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-scrt-tl/index-fr.aspx

3 Cours en ligne CyberSécuritaire

3.1 CyberSécuritaire Canada

CyberSécuritaire Canada est un programme fédéral de certification destiné aux petites et moyennes organisations (PMO). CyberSécuritaire Canada offre une série de cours en ligne gratuits, conçus pour aider les petites et moyennes organisations (PMO) à mettre en œuvre des contrôles de cybersécurité de base et à améliorer leur posture de cybersécurité.

https://www.ic.gc.ca/eic/site/137.nsf/fra/h_00017.html

4 Signaler un cyberincident

Signalez les cybercrimes sur le portail en ligne du Centre pour la cybersécurité pour obtenir du soutien et des conseils sur la meilleure façon de protéger votre organisation contre les attaques.

Portail de signalement des cyberincidents

5 Produits du Centre pour la cybersécurité

Aimeriez-vous recevoir des renseignements sur les menaces, ainsi que des alertes et des conseils du Centre pour la cybersécurité? Communiquez avec le Centre pour la cybersécurité, par courriel, à contact@cyber.gc.ca.

Centre canadien pour la cybersécurité

Réunion du réseau du secteur alimentaire

Février 2022

RÔLE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (CST) DANS LE DOMAINE DE LA CYBERSÉCURITÉ

- Leader en cybersécurité au Canada
- Accès à des renseignements étrangers uniques
- Au-delà des menaces émergentes
- Surveillance des systèmes gouvernementaux en tout temps
- Protection des renseignements les plus importants du Canada

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

PORTRAIT DE LA MENACE

ÉVALUATION DES CYBERMENACES NATIONALES – 2020

- Les cybercriminels représentent pour les Canadiens la cybermenace la plus envahissante.
  - Attaques aux rançongiciels et à l'hameçonnage
- Les auteurs de cybermenaces appuyés par un État disposent des capacités les plus élaborées.
  - Cyberespionnage, vol d'adresses IP, campagnes d'influence en ligne, cyberattaques perturbatrices

PORTRAIT DE LA MENACE

RÉPERCUSSIONS DE LA COVID-19 SUR LA CYBERMENACE

- Bulletin sur les cybermenaces : INCIDENCE DE LA COVID-19 SUR LA CYBERMENACE
  - Le cyberespionnage visant le Canada continuera à cibler le vol de la propriété intellectuelle canadienne concernant la recherche sur la vaccination contre la COVID-19 et le traitement de cette maladie.
  - **Les auteurs de cybermenaces sont identifiés comme des personnes travaillant à la maison et exploitant les technologies déployées en soutien aux effectifs en télétravail tels que les RVP.**
  - **Les auteurs de cybermenaces utilisent le thème de la COVID-19 comme appât dans leurs activités malveillantes.**

PORTRAIT DE LA MENACE

LA MENACE DES RANÇONGICIELS EN 2021

- Au cours de la première moitié de 2021, à l'échelle mondiale, les attaques par rançongiciel ont connu une hausse de 151 % par rapport aux chiffres de la première moitié de 2020 (alimentées par rançongiciel-service).
- L'année 2021 a été marquée par les rançons demandées et les rançons payées les plus élevées.
  - Au Canada, le coût moyen d'une fuite de données (incluant les données visées par un rançongiciel) était de 6,35 M$ CA.
  - Le coût moyen à l'échelle mondiale du rétablissement lié à un incident par rançongiciel (rançon payée/rétablissement du réseau compromis) a augmenté, passant de 970 000 $ CA en 2020 à 2,3 M$ CA en 2021.
- Le Centre pour la cybersécurité a répertorié 235 incidents par rançongiciel contre des victimes canadiennes entre le 1er janvier et le 16 novembre 2021.
- Une fois qu'elles ont été ciblées, les victimes d'attaque par rançongiciel sont souvent attaquées à nouveau plusieurs fois.

HAMEÇONNAGE

- L'hameçonnage est le principal vecteur d'introduction du rançongiciel.
  - Hameçonnage, hameçonnage par SMS, hameçonnage vocal, hameçonnage par code QR
  - Ne mordez pas à l'hameçon: Reconnaître et prévenir les attaques par hameçonnage
  - Les 7 signaux d'alarme de l'hameçonnage

MÉFIEZ-VOUS SI:

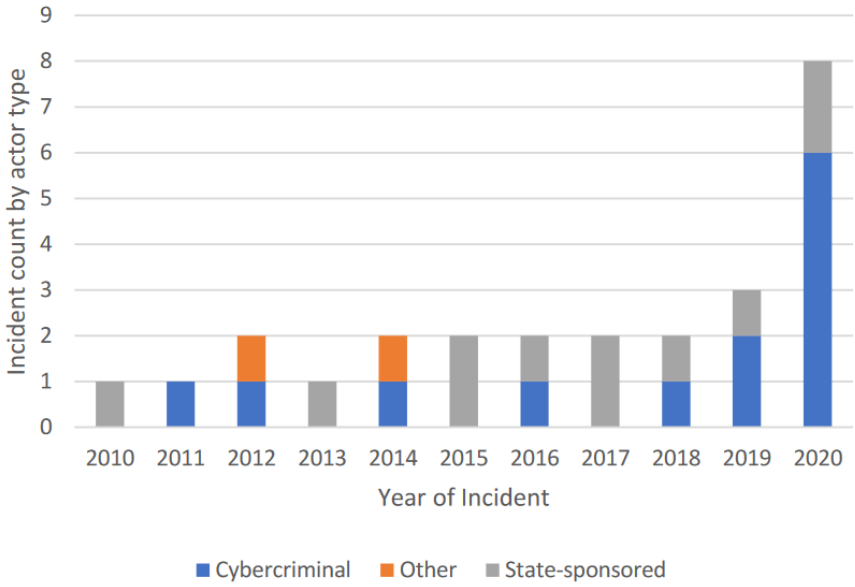
- Vous ne reconnaissez pas le nom de l'expéditeur, l'adresse électronique ou le numéro de téléphone (méthode de harponnage courante).
- Vous remarquez de nombreuses erreurs de grammaire et d'orthographe.
- L'expéditeur vous demande des renseignements personnels ou confidentiels.
- La demande de l'expéditeur est urgente et assortie d'une échéance.
- L'offre semble trop bonne pour être vraie.

PORTRAIT DE LA MENACE

LES CYBERMENACES VISANT LES TECHNOLOGIES OPÉRATIONNELLES

- La technologie opérationnelle (TO) joue un rôle essentiel dans la gestion des infrastructures essentielles du Canada.
- La transformation numérique de la TO fournit aux auteurs de cybermenaces de nouveaux débouchés pour accéder aux systèmes de TO et les perturber.
- L'année 2020 a connu un sommet dans les activités de cybermenaces visant les systèmes de TO partout dans le monde.

Figure 1. Publicly-reported cyber incidents targeting OT, by actor type.



PORTRAIT DE LA MENACE

ACTIVITÉS DE CYBERMENACE QUI SONT PARRAINÉES PAR LA RUSSIE

- Si la crise actuelle en Ukraine s'aggrave, la Russie attaquera très probablement les infrastructures essentielles de ceux qu'elle perçoit comme ses adversaires.
- Soyez préparé à isoler d'Internet les composantes et les services des infrastructures essentielles.
- Augmentez la surveillance de vos réseaux.
- Améliorez votre niveau de sécurité (systèmes de rustines, autorisations d'accès, etc.).

COMMENT PROTÉGER MON ORGANISATION?

Faites régulièrement des copies de sauvegarde de vos données et conservez les copies hors ligne. LIEN

Utilisez des mots de passe robustes et uniques, mettez en œuvre l'authentification à facteurs multiples. LIEN

Mettez vos systèmes à jour et appliquez les rustines disponibles.

Ayez un plan d'intervention en cas d'incident (et testez-le!). LIEN

Utilisez des outils de sécurité. LIEN

Contrôles de cybersécurité de base pour petites et moyennes organisations
du Centre pour la cybersécurité
Apprentissage en ligne sur la cybersécurité au Canada de l'ISDE

Publication du CCCS concernant les rançongiciels

Rançongiciels

- Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises
  - Les liens de la diapositive précédente sont tirés de cette publication.
- Reconnaître les courriels malveillants
- Rançongiciels : comment les prévenir et s'en remettre
- Rançongiciel : comment vous en remettre
- Avez-vous été victime de cybercriminalité?

LE RÔLE DU CENTRE POUR LA CYBERSÉCURITÉ

Pour des services gratuits de cybersécurité, écrivez à contact@cyber.gc.ca

SOUTIEN À LA GESTION DES INCIDENTS

SOUTIEN EN TOUT TEMPS

contact@cyber.gc.ca

RENSEIGNEMENTS SUR LES MENACES

ACCÈS À DES RENSEIGNEMENTS EXPLOITABLES SUR LES CYBERMENACES

Alertes et avis

BÂTIR UNE COMMUNAUTÉ

ENSEMBLE POUR UNE CYBERSÉCURITÉ ACCRUE

CONSEILS ET ORIENTATION

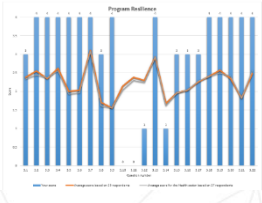
MISE À PROFIT DE L'EXPERTISE DU CENTRE POUR LA CYBERSÉCURITÉ

Publications

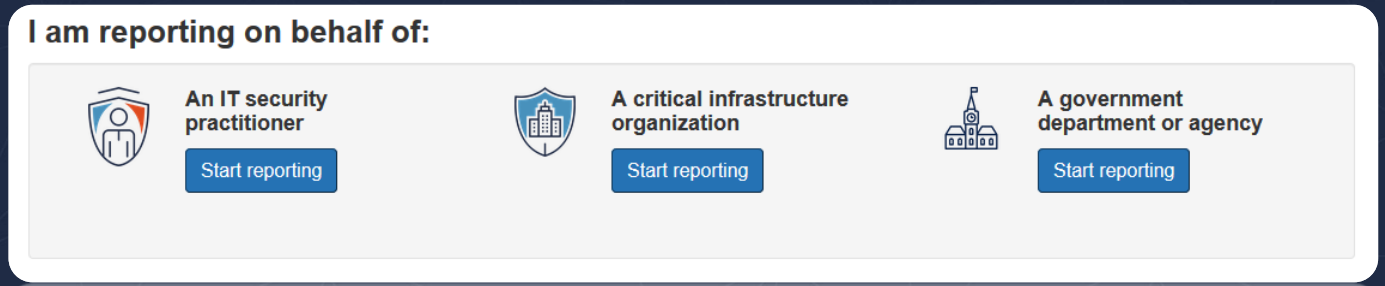
SERVICES DE CYBERDÉFENSE

RENFORCEMENT DE VOS CAPACITÉS DE DÉFENSE

Évaluations, avis de vulnérabilité, partage d'indicateurs de compromissions, etc.



VEUILLEZ SIGNALER TOUT INCIDENT DE CYBERSÉCURITÉ



Portail de signalement des incidents :
https://cyber.gc.ca/en/incident-management

cyberincident@cyber.gc.ca
contact@cyber.gc.ca

CANADIAN CENTRE FOR CYBER SECURITY

Food Sector Network Meeting

February 2022

COMMUNICATION SECURITY ESTABLISHMENT'SN (CSE) ROLE IN CYBER SECURITY

- CYBER SECURITY LEAD IN CANADA
- ACCESS TO UNIQUE FOREIGN INTELLIGENCE
- AHEAD OF EMERGING THREATS
- MONITOR GC SYSTEMS 24/7 FOR CYBER THREATS
- SAFEGUARDS CANADA'S MOST IMPORTANT INFORMATION

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

THE THREAT LANDSCAPE

National Cyber Threat Assessment – 2020

- Cybercriminals represent the most pervasive cyber threat to Canadians
  - Ransomware and Phishing attacks
- State sponsored cyber threat actors have most sophisticated capabilities
  - Cyber espionage, IP theft, online influence campaigns, disruptive cyber attacks

THE THREAT LANDSCAPE

IMPACT OF COVID-19 ON CYBER THREAT

- Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats
  - Cyber espionage directed at Canada will continue to attempt to steal Canadian intellectual property relating to COVID-19 vaccine and treatment research
  - **Cyber threat actors are identifying individuals working at home and exploiting technologies deployed in support of a remote workforce, such as VPNs**
  - **Cyber threat actors will leverage COVID-19 as a thematic lure for their malicious activities**

THE THREAT LANDSCAPE

THE RANSOMWARE THREAT IN 2021

- First half of 2021, global ransomware attacks increased by 151% when compared of the first half of 2020 (fueled by Ransomware-as-a-service)
- 2021 was marked by the highest ransoms and the highest payouts
  - In Canada, average cost of a data breach (includes ransomware) was $6.35M CAD
  - Global average cost of recovery from ransomware incident (paying ransom / remediating compromised network) increased from $970 000 CAD in 2020 to $2.3M CAD in 2021
- Cyber Center is aware of 235 ransomware incidents against Canadian victims from Jan 1 to Nov 16 2021
- Once targeted, ransomware victims are often attacked multiple times

PHISHING

- Phishing is the number one delivery vehicle for ransomware.
  - Phishing, SMiSing, Vishing, Quishing
  - Don’t Take the Bait: Recognize and Avoid Phishing Attacks
  - The 7 red flags of Phishing

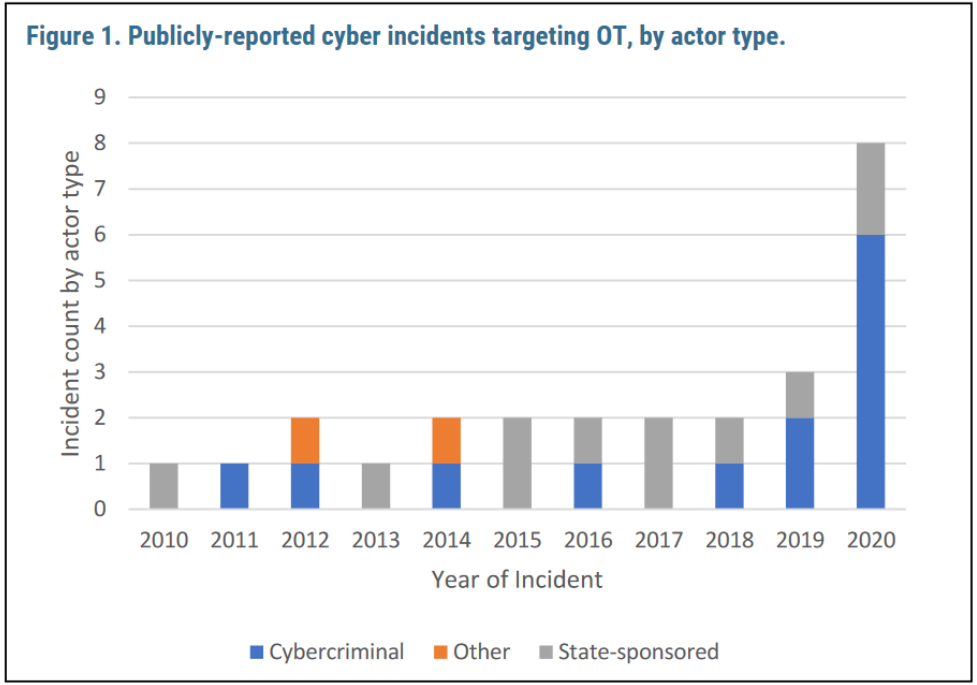
SOMETHING MAY BE PHISHY IF:

- You don’t recognize the sender’s name, email address, or phone number (e.g. very common for spear phishing)
- You notice a lot of spelling and grammar errors
- The sender requests your personal or confidential information
- The sender makes an urgent request with a deadline
- The offer sounds too good to be true

THE THREAT LANDSCAPE

CYBER THREAT TO OPERATIONAL TECHNOLOGY

- Operational Technology (OT) plays an essential role in the management of Canada's CI
- Digital transformation of OT is providing cyber threat actors new opportunities to access and disrupt OT systems
- 2020 saw a spike in cyber threat activity against OT systems around the world



THE THREAT LANDSCAPE

RUSSIAN-BACKED CYBER THREAT ACTIVITY

- Should the current Ukraine crisis escalate, Russia will very likely attack the CI of perceived adversaries
- Be prepared to isolate CI components and services from the Internet
- Increase monitoring of your networks
- Enhance security posture (patch systems, enable logging, etc.)

HOW CAN I PROTECT MY ORGANIZATION?

Regularly back up your data and store off-line. LINK

Use strong and unique passwords, implement MFA. LINK

Update and patch systems. LINK

Have an Incident Response Plan (and test it!) LINK

Use security tools. LINK

Cyber Center's Baseline Cyber Security Controls for SMO
ISED's CyberSecure Canada eLearning

CCCS Ransomware Publications

Ransomware Playbook

- Top Measures to Enhance CyberSecurity for SMO
  - Links from previous slide come from this Publication
- Spotting Malicious Email Messages
- Ransomware: How to prevent and recover
- Ransomware: How to recover and get back on track
- Have You Been A Victim of Cyber Crime?

THE ROLE OF THE CYBER CENTRE

For Free Cyber Center Services: contact@cyber.gc.ca

INCIDENT HANDLING SUPPORT

24/7 SUPPORT

contact@cyber.gc.ca

THREAT INTELLIGENCE

ACCESS TO ACTIONABLE CYBER THREAT INTELLIGENCE

Alerts, Advisories

COMMUNITY BUILDING

FURTHER CYBER SECURITY TOGETHER

ADVICE & GUIDANCE

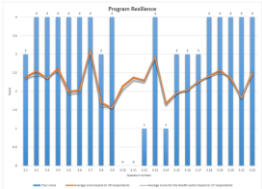
LEVERAGE THE CYBER CENTRE'S EXPERTISE

Publications

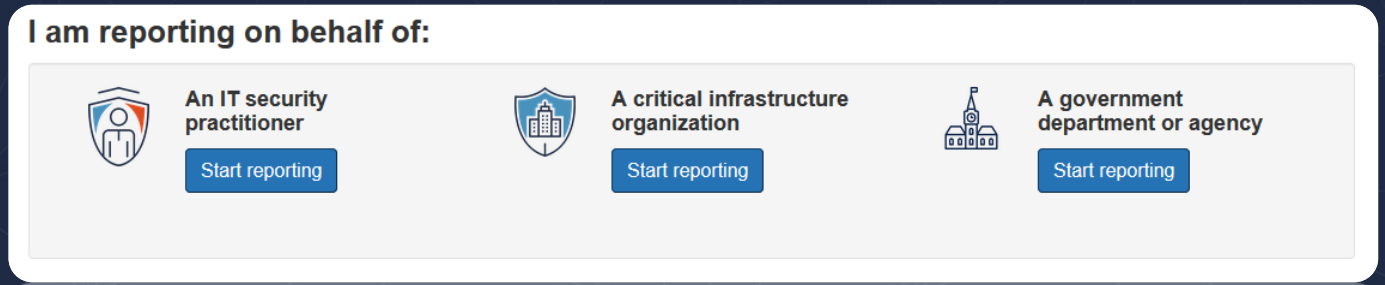
CYBER DEFENCE SERVICES

STRENGTHEN YOUR DEFENCE CAPABILITIES

Assessments, Vulnerability Notifications, Sharing IoCs, etc.



PLEASE REPORT A CYBER INCIDENT



Incident Reporting Portal:
https://cyber.gc.ca/en/incident-management

cyberincident@cyber.gc.ca
contact@cyber.gc.ca