Étude sur la cybersécurité et les opportunités offertes par l'accès aux données au Québec

Version finale – 9 novembre 2021

FCCQ
Fédération des chambres de commerce du Québec

Fédération des chambres de commerce du Québec

Grâce à son vaste réseau de 130 chambres de commerce et 1 100 membres corporatifs, la Fédération des chambres de commerce du Québec (FCCQ) représente plus de 50 000 entreprises exerçant leurs activités dans tous les secteurs de l'économie et sur l'ensemble du territoire québécois. Plus important réseau de gens d'affaires et d'entreprises du Québec, la FCCQ est à la fois une fédération de chambres de commerce et une chambre de commerce provinciale. Ses membres, qu'ils soient chambres ou entreprises, poursuivent tous le même but : favoriser un environnement d'affaires innovant, concurrentiel et durable.

Charles Milliard
Président-directeur général – FCCQ

Philippe Noël
Vice-président, Affaires publiques et économiques – FCCQ

Mathieu Lavigne
Directeur, Affaires publiques et économiques – FCCQ

Charles Vaillancourt
Économiste - FCCQ

RESPONSABLES DE L'ÉTUDE

Jean-Pierre Lessard
Associé

Kathy Megyery
Associée-conseil

RECHERCHE, ANALYSE ET RÉDACTION

Mathieu Paquet
Directeur

Jean-François Landry
Directeur

Nastasia Faivre
Analyste

Sommaire

Sommaire

Une prise de conscience sur la cybersécurité et l'importance de la valorisation des données

Des données au volume vertigineux qui représentent à la fois risques et occasions

À travers le monde, le volume de données corporatives générées a été multiplié par 18 au cours de la dernière décennie. Le nombre d'appareils intelligents, la facilité de l'accès à Internet, la baisse des coûts d'entreposage des données, l'émergence d'outils d'analyse de plus en plus puissants, et l'essor du commerce en ligne sont autant de facteurs qui ont contribué au développement des données massives. Du reste, on estime que 82% de ces données ne sont pas structurées alors que 87% des chefs de direction au Canada se disent préoccupés par les cybermenaces.

Il était donc à-propos que la FCCQ fasse le point quant à l'état des connaissances sur les menaces auxquelles sont confrontées les entreprises en matière de cybersécurité et sur les occasions liées à la valorisation des données.

Les cybermenaces s'intensifient de plus en plus

L'avènement de notre ère numérique et la crise sanitaire de la COVID-19 contribuent grandement à l'intensification des cybermenaces. L'informatique quantique et la popularité croissante de la 5G et de l'Internet des objets contribueront à accroître encore davantage les risques.

Ère numérique	– Profusion des données – Sophistication et démocratisation de la cybercriminalité – Montée des cryptomonnaies – Mutation des guerres froides – Infonuagique
Crise sanitaire	– Décentralisation des réseaux – Explosion du commerce en ligne – Hausse des visioconférences – Intérêt des réseaux de santé – Pratiques défaillantes en sécurité

Les menaces en matière de cybersécurité peuvent prendre plusieurs formes

Les diverses techniques mises parfois sur des failles informatiques alors que dans d'autres cas, c'est la vulnérabilité humaine qui est mise à profit. Les effets sont multiples : divulgation d'informations sensibles, espionnage, sabotage, dégradation de l'image, vol d'identité et de propriétés intellectuelles, fraude, etc.

Ordinateur zombie	Rançongiciel	Injection SQL	Ver informatique
Cheval de Troie	Hameçonnage	Logiciel espion	Virus informatique

41%

Pourcentage des entreprises au Québec qui pensent avoir été la cible d'une ou plusieurs cyberattaques

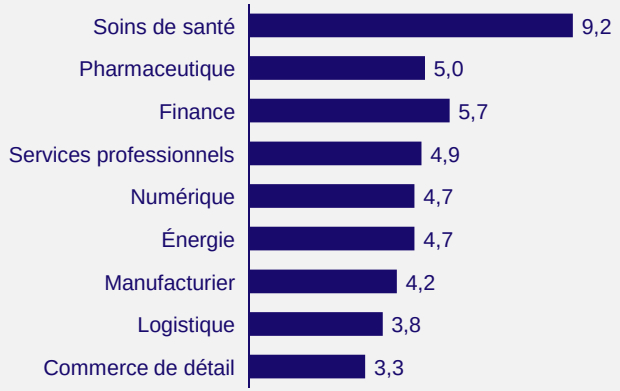
Les cyberattaques ont des impacts majeurs

Une proportion de 40% des entreprises sondées craint le plus les dommages financiers directs liés par exemple à une demande de rançon ou le dommage aux équipements. À 27%, c'est la rupture des opérations qui inquiètent le plus.

Une cyberattaque coûte cher aux entreprises

Si le coût moyen d'une seule attaque atteint les 4,2 M$ au Canada, c'est la perte cumulée de la rupture des activités, de la diminution de la clientèle et des dommages réputationnels qui constituent, à 38%, la composante la plus importante. Les coûts varient toutefois selon les différents secteurs économiques

Coût moyen d'une violation de données par secteur
2021, en $US



« La hausse des cyberattaques est fulgurante. L'enjeu est de déployer les mesures plus rapidement dans en environnement ou les ressources humaines spécialisées manquent. […] De plus, il faut rehausser le niveau de sécurité des partenaires et tierces parties. Dans le futur, l'objectif ne sera pas seulement monétaire mais plus politique et stratégique (ex. attaquer des hôpitaux, des infrastructures publiques) »

Le message final de notre sommaire est de prouver que nous, humains, sommes tous et sans

Sommaire

Des stratégies existent afin de limiter les probabilités d'occurrence et les impacts d'une cyberattaque

Les entreprises doivent perdre leur naïveté

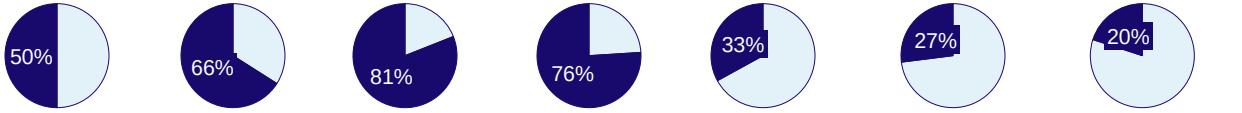
En matière de cybermenaces, le risque zéro n'existe pas. Il importe d'être proactif et de soutenir dans le temps diverses mesures. La formation, l'authentification robuste, les contrôles d'accès, la conservation de copies de sauvegarde chiffrées, la tenue d'audit de sécurité, et la mise en place d'un chef de la sécurité sont autant de mesures qui contribueront à diminuer les chances d'être l'objet d'une attaque.

Méthodes les plus efficaces pour réduire les coûts liés aux violations de données
– Encryptage de données
– Équipe dédiée aux attaques
– **Politique de gouvernance des données**
– **Formation des employés**

Au Québec, les entreprises sont majoritairement de petite taille
L'absence de sensibilité et d'expertise chez ces entreprises accentuent davantage les risques

Il y a des écarts importants entre les bonnes pratiques et ce que font en réalité les entreprises du Québec

L'installation de logiciels de sécurité et les dispositifs de sauvegarde constituent les mesures les plus implantées au Québec. Il reste que près du quart des entreprises sondées n'ont pas de processus de sauvegarde. Le tiers des entreprises offrent de la formation alors qu'on estime que 40% des infractions relatives aux données résultent du comportement des employés. Le fait que la moitié des entreprises jugent leurs mesures suffisantes suggèrent une certaine méconnaissance des risques. De même, il semble paradoxal que 66% des entreprises affirment dédier des ressources pour connaître les risques mais que seulement 20% disent avoir mis un plan de gestion à la suite d'une cyberattaque.



jugent que leurs mesures de cybersécurité sont adéquates et suffisantes	dédient des ressources pour connaître ses vulnérabilités et les risques	utilisent des logiciels de sécurité	ont un processus de sauvegarde des données	offrent de la formation aux employés	ont souscrit à une assurance visant à se protéger contre les cyber-risques	ont un plan de gestion en cas d'occurrence

Les assurances sont importantes mais ne suffisent pas

Les experts s'attendent à ce que les primes d'assurance augmentent en raison de la hausse des risques. L'étendue des couvertures pourraient aussi diminuer. La réelle valeur de l'assurance est dans la facilitation du rétablissement des activités après une cyberattaque.

40% **Croissance des professionnels en cybersécurité au Canada au cours des cinq dernières années. La rareté de main-d'œuvre affectera le secteur.**

Recommandations relatives à la cybersécurité

FCCQ

1. Continuer de sensibiliser et former les entreprises aux risques relatifs à la cybersécurité	**2. Appliquer les pratiques exemplaires en matière de cybersécurité**	**3. Mettre en place une fonction dédiée à la cybersécurité**	**4. Former de manière continue les employés sur les risques relatifs à la cybersécurité**	**5. Renforcer l'écosystème d'expertises et constituer un réseau de veille préventive**	**6. Accélérer le projet de mise en place du portefeuille numérique du gouvernement du Québec**	**7. Apprendre de nos leçons récentes**	**8. Interdire le paiement de rançons**

Peu importe la taille de l'entreprise, ce n'est plus une question de savoir si une elle sera l'objet d'une cyberattaque, mais bien de quand elle sera attaquée

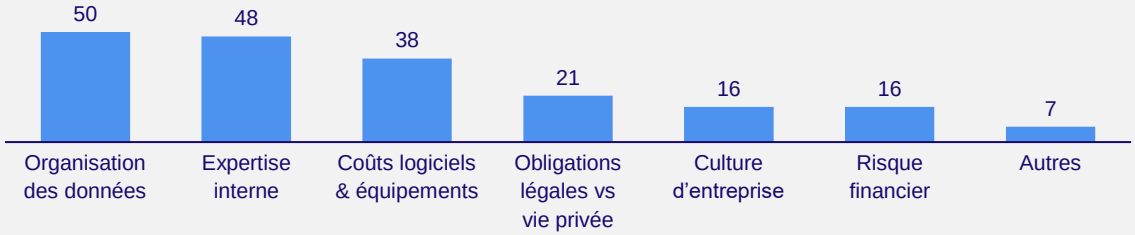
FCCQ

L’abondance des données et l’importance des bénéfices de leur valorisation

Un actif intangible qui requiert des investissements

Les données sont de plus en plus perçues comme une ressource clé, un atout stratégique. Leur ampleur actuelle permet de les qualifier dans plusieurs cas de « massives » et ont comme grandes caractéristiques leur fort volume, leur vélocité, leur véracité et leur variété. L’exploitation de ces données massives demeure un enjeu pour les entreprises québécoises alors qu’elles ont identifiés de nombreux freins qui les empêchent d’en tirer des bénéfices. C’est ainsi que l’organisation des données et l’expertise interne constituent les principales limites.

Principaux freins à la valorisation des données
2021, Membres de la FCCQ, en %



D’importants bénéfices issus de la valorisation

On peut identifier deux grands vecteurs stratégiques pour lesquels les données peuvent contribuer à générer de la valeur, soit **l’analyse prédictive et l’accroissement des connaissances** des clientèles. Ces vecteurs contribueront en définitive à l’augmentation de l’efficacité des entreprises

5% **Gains de productivité**

6% **Gains de rentabilité**

L’analyse prédictive devient un incontournable

L’analyse prédictive vise à reconnaître des patterns dans les données pour obtenir la probabilité d’un événement. Elle s’appuie sur une collecte de données minimale alliée à des techniques statistiques, principalement l’analyse de régression. Plus récemment, combinée à du data mining et parfois du machine learning, l’analyse prédictive est parvenue à considérer des facteurs d’influence dans un éventail beaucoup plus large qu’auparavant. Ses bénéfices sont multiples.

–	–	–	–
Gains d’efficacité	Hausse de productivité	Qualité des services	Baisse des accidents

De nombreux secteurs peuvent y recourir

Une étude révélait que les entreprises du secteur de l’énergie ayant mis en place des programmes de maintenance prédictive ont réussi à éliminer pas moins de 75% des pannes sur leurs équipements. Il s’agit d’un exemple parmi d’autres. Le manufacturier, la finance, les assurances, la santé, et le commerce de détail sont autant d’autres secteurs à fort potentiel.

La relation client bénéficie des données valorisées

La mise en valeur des données permet de mieux connaître ses marchés et ses canaux et alimentent l’efficacité de l’entreprise.

Efficacité commerciale	– Génération de contenu – Ciblage plus fin – Développement des recommandations – Tarification individualisée	Maximisation des revenus
Efficacité opérationnelle	– Baisse des coûts d’acquisition & de fidélisation des clients – Automatisation des processus – Arrimage marketing- ventes – Performance des campagnes marketing	Réduction des coûts
Efficacité relationnelle	– Parcours clients selon le cycle de vie – Expérience de marque cohérente, personnalisée et mémorable – Segmentation de la clientèle en temps réel	Rehaussement de l’expérience client

En autorisant la collecte de leurs données, les clients attendent des gains parlants
– 80 % des clients sont plus susceptibles d’acheter si l’offre est personnalisée
– 60% des entreprises voient l’expérience-client comme la principale source de différenciation par rapport à la concurrence

Tirer un avantage concurrentiel

Les objectifs de la valorisation peuvent varier selon chaque organisation, outre les gains en efficacité. Si la facilitation et l’accélération de la prise de décision sont plus évidents comme finalité, une entreprise pourrait aussi vouloir améliorer ses produits, en développer de nouveaux, renforcer ses connaissances sur sa clientèle, ou encore vendre les données.

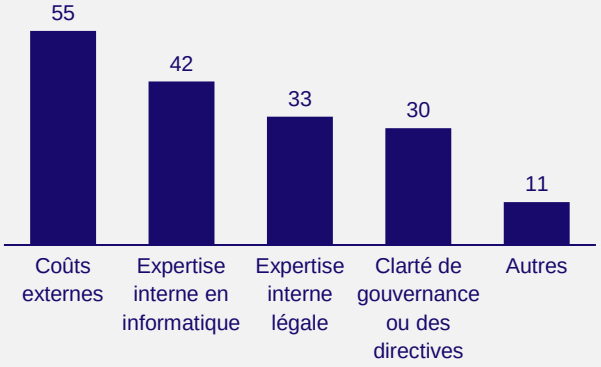
Sommaire

Le Québec entrepreneurial doit intégrer une culture dynamique et à l'avant-garde de la donnée

Des enjeux certains à relever

La confidentialité et la protection des données personnelles constituent des enjeux fondamentaux lorsqu'il est question de mise en valeur des données. À cela s'ajoute la question de l'expertise qui peut manquer à l'interne dans une organisation. C'est d'ailleurs le deuxième enjeu (42%) le plus important selon les entreprises sondées, derrière les coûts externes liés soit à leur organisation, soit à leur traitement (55%).

Principaux enjeux relatifs à la protection légale des données
2021, Membres de la FCCQ, en %



Des approches simples peuvent aider

La fiducie de données est un modèle de partage de données qui offre un équilibre entre la juste valorisation et la protection des données et de la vie personnelle. Elle permet de mettre en commun des données et d'impliquer tous les acteurs économiques et sociaux.

Certaines organisations créent un poste de « traducteur de données » qui fait le pont entre les technologies et les impératifs d'affaires, donc entre les moyens et les résultats.

Les méthodes statistiques d'aujourd'hui permettent de rendre anonymes les différents contenus, donc de rendre extrêmement difficile l'identification d'un individu. Elles favorisent dès lors l'acceptabilité sociale en vue d'une utilisation commerciale.

Des réponses concrètes à l'enjeu de la sensibilité des données

- **Fiducie de données**
- **Traducteur de données**
- **Anonymisation**

Des exemples inspirants

Le rapport propose une série de pratiques inspirantes en matière de cybersécurité et de valorisation de données.

Le gouvernement français a mis en place une plateforme de signalement (PHAROS) des comportements illicites sur Internet, donc les cyberattaques

Israël mise depuis plusieurs années sur les incubateurs. Le secteur de la cybersécurité y a recours alors que les entreprises ont connu une croissance de 70% de leur financement en 2020

Une chaîne hôtelière a construit un modèle pour prédire les vols annulés. En anticipant les réservations de dernière minute, son chiffre d'affaires a crû de 10%

Une chaîne de restaurants au Japon réussit à prédire à 85% le nombre de clients. Les établissements sont plus efficaces dans la planification du travail

Les données en santé offrent de grands bénéfices

- Accélérer l'innovation
- Développer une culture de la donnée
- Mieux évaluer la performance
- Optimiser l'utilisation de médicaments
- Assurer une gestion plus efficace
- Améliorer la pratique médicale

Le système de recommandations personnalisées d'Amazon serait responsable d'environ 35% des ventes annuelles. Grâce aux données massives, l'entreprise parviendrait à diminuer ses coûts de transport de 10% à 40%

Recommandations relatives à la cybersécurité

FCCQ

9. Développer une capacité transversale à générer et gérer les données	**10. Prévoir des règles internes établissant les politiques d'accès sur l'ensemble du cycle de vie des données**	**11. Adapter la disponibilité et la présentation de l'information pour répondre à différents besoins**	**12. Intégrer l'apport d'un « traducteur de données » et mieux faire connaître les ressources externes**	**13. Soutenir la création de modèles collaboratifs et de partenariats entre entreprises**	**14. Accroître les budgets de l'Institut de la statistique du Québec**	**15. Ouvrir de manière anonymisée les données publiques en santé**

La valorisation des données est indissociable de la numérisation et des systèmes d'information. Il est indispensable de considérer la donnée comme un actif fondamental dans lequel il est payant investir.

FCCQ

Table des matières

FCCQ
Fédération des chambres de commerce du Québec

Introduction

Cybersécurité et accès aux données

La quantité de données disponibles est en croissance

La quantification du volume des données disponibles se heurte à des enjeux méthodologiques, mais il est estimé que le taux de croissance annuelle implicite serait autour de 40%

Les principaux facteurs contribuant à la croissance et au développement des données massives sont :

1. **L'augmentation du nombre d'appareils intelligents**
2. **La baisse des coûts d'accès à Internet**
3. **La diminution des coûts d'entreposage des données**
4. **Des outils d'analyse de plus en plus puissants et sophistiqués**
5. **La hausse des utilisateurs d'internet et l'essor du commerce en ligne**

La prolifération des données génère à la fois des enjeux de cybersécurité mais représente également des opportunités pour les entreprises et les gouvernements reliées à la valorisation des données massives.

Sources : Banque Mondiale; Hajirahimova et Aliyeva 2017; McKinsey 2011; General Électric 2012, Wang et al. 2018

La cybersécurité s’avère une préoccupation grandissante pour les entreprises

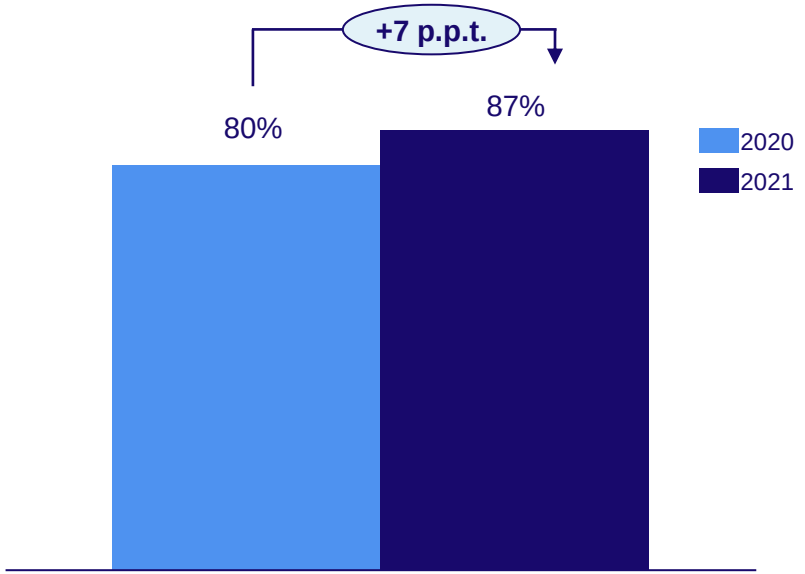
Au cours des dernières années, les incidents majeurs de cybersécurité se sont multipliés et devenus monnaie courante. En 2020, 445 millions cyberattaques ont été répertoriées à travers le monde, le double de ce qui avait été enregistré en 2019. En plus d’être plus courantes, les cyberattaques deviennent de plus en plus sophistiquées.

Dans l'économie numérisée d'aujourd'hui, toutes les entreprises ont recours à la technologie dans leurs opérations. La protection des données, de l'infrastructure numérique, des opérations, des clients voire des tiers contre une cyberattaque constitue un défi grandissant.

Comme pour bien d’autres phénomènes émergents, la pandémie de la COVID-19 et l’adoption du télétravail n’aura qu’exacerbé les risques de cybermenace et placé les entreprises dans une position encore plus vulnérable. Aujourd’hui, ce sont 87 % des chefs d’entreprise canadiens qui s’avouent anxieux face aux effets négatifs des cybermenaces sur la croissance de leur organisation, en hausse par rapport au 80 % de 2020.

Niveau de préoccupation des chefs de direction quant aux cybermenaces

Canada; 2020-2021; en %



Les chefs de direction canadiens sont plus préoccupés des effets négatifs des enjeux de cybersécurité sur leurs entreprises

Sources : PwC Canada, Aviseo Conseil 2021.

Les cyberattaques contre les institutions publiques sont également plus courantes et sophistiquées

Les risques croissants liés à la cybersécurité sont illustrés par une série d'attaques perpétrées auprès d'entités publiques et théoriquement munis des ressources pour s'en protéger. Or, il s'avère qu'aucune organisation n'est à l'abris des cyberpirates, qui ont su adapter et sophistiquer leurs techniques.

Les cybercriminels cherchent à exploiter les points faibles des systèmes informatiques, ce qui semble d'ailleurs s'avérer une stratégie efficace lorsqu'on analyse la série d'attaques recensées au cours des dernières années contre des entités publiques au Québec et au Canada.

Le gouvernement du Québec a récemment déclaré que des États internationaux financent des attaques contre ses systèmes informatiques, en précisant que ces États pourraient ainsi tenter d'accéder aux banques de données du gouvernement dans de multiples domaines tels que les services de santé ou encore des données territoriales.

Organisations	Attaques
Centre de services scolaire des Appalaches Québec	En 2016, une attaque par rançongiciel envers la Commission scolaire des Appalaches a paralysé 95 % de son réseau et a coûté 275 000$ en équipement et heures supplémentaires des informaticiens.
Revenu Québec	En 2016, Revenu Québec est victime d'une attaque par rançongiciel. Bien que l'attaque ait été commise via un courriel générique ouvert par un employé, qu'elle ne visait pas directement Revenu Québec et qu'aucune donnée n'ait été perdue ou rançon payée, cette attaque a démontré une certaine vulnérabilité du gouvernement
Culture et Communications Québec	Entre 2017 et 2018, le ministère a été la proie de dix cyberattaques, incluant des tentatives d'extorsion, et des courriels contenant des pièces infectées.
Centre de services partagés Québec	Peu avant les élections d'octobre 2018, le Centre de services partagés du Gouvernement du Québec a été la cible d'une attaque par déni de service. Plusieurs sites web du gouvernement ont cessé d'être accessible pendant une certaine période de temps.
Gouvernement du Canada	En 2019, le Gouvernement du Canada rapporte qu'il est victime de 50 cyberattaques par semaine.
stm	En octobre 2020, la Société de Transport de Montréal a été la cible d'une variante hautement sophistiquée du virus informatique « RansomExx » qui a touché 1 000 serveurs et provoqué des dommages de 2 M$ en équipement et services.

Sources : Vumetric 2020, Société de Transport de Montréal, La Presse +, Le Journal de Québec, La Presse, 1er octobre, 2021, Aviseo Conseil 2021

Les entreprises (et gouvernements) doivent également se pencher sur les opportunités liées à la valorisation des données

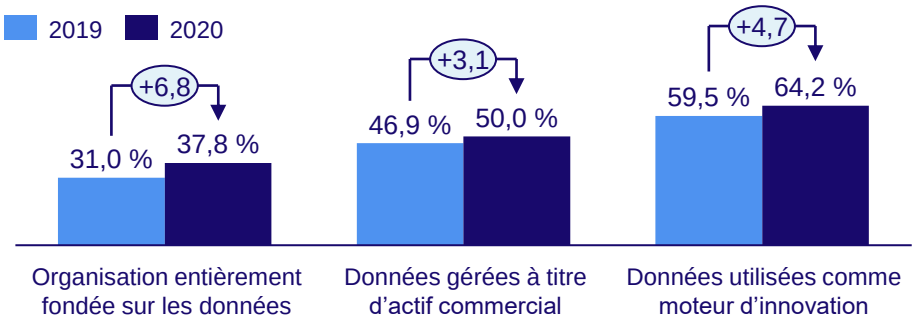
La montée en puissance des grandes entreprises technologiques américaines au cours de la dernière décennie aura montré tout le potentiel de création de valeur latent au sein de bases de données.

Parmi les grandes entreprises Fortune 1000, certaines sont entièrement fondées sur l'exploitation de données (37,8 %), alors que d'autres les gèrent à titre d'actif commercial (50 %) ou les utilisent pour stimuler l'innovation (64,2 %). Tous ces usages sont en hausse.

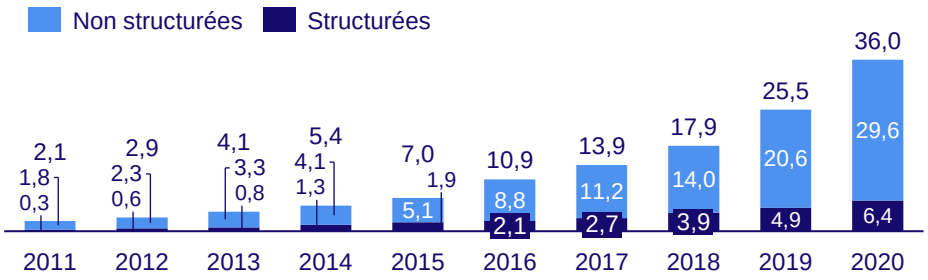
Malgré leur grande volonté, les entreprises font face à divers enjeux pour extraire le maximum de valeur des données : protection de la vie privée, infiltrations malveillantes et vols de données, conformité réglementaire, manque d'expertise, etc.

La désorganisation de l'information constitue également une barrière. En 2020, 82% des données corporatives générées dans le monde étaient non structurées, et devaient subir des manipulations préalablement à leur exploitation.

Exploitation des données dans les entreprises du Fortune 1000
États-Unis; 2019-2020; en %



Volume de données corporative généré annuellement, selon le type
Monde; 2011-2020; en exabytes



Sources : IDC, The Economist, NewVantage Partners : Big Data and AI Executive Survey 2021, Aviseo Conseil 2021.

Les gouvernements doivent trouver le juste équilibre entre la valorisation des données tout en se portant garant des droits civils

À titre d'entités propriétaires de données, les gouvernements peuvent stimuler l'adoption de pratiques novatrices en matière de prestation de services publics. La valorisation des données gouvernementales peut s'inscrire dans quatre vecteurs de création de valeur :

- L'optimisation de la prestation de services publics
- La conception de politiques publiques robustes
- La consolidation de la participation citoyenne aux débats publics
- La stimulation de l'innovation et de la prise de décision basées sur des données probantes.

Prestation des services

Comme les entreprises privées, les gouvernements peuvent avoir recours à l'analyse de données pour mesurer des corrélations, procéder à des inférences et dresser des constats afin d'ajuster leur prestation de services, d'améliorer leur efficience ou de lancer de nouveaux services, le tout au bénéfice du citoyen.

Élaboration des politiques

Le processus d'élaboration d'une politique publique débute par la réalisation d'une base de faits et d'un diagnostic robuste, permettant entre autres de cerner les enjeux à résoudre. Les données gouvernementales peuvent être mises à contribution à cet égard pour mesurer les effets des politiques.

Engagement civique

L'engagement du citoyen envers les politiques et les actions de son gouvernement peuvent être stimulés par le recours aux données. Des analyses probantes du contenu des médias sociaux qui peuvent rendre le gouvernement plus agile face aux préoccupations ou sentiments des citoyens.

Innovation accélérée

Les gouvernements recueillent d'importantes quantités de données qui, si elles sont structurées, protégées et partagées selon les meilleures pratiques, peuvent stimuler la recherche et le développement et ainsi devenir un vecteur d'innovation et de création de richesse. La valorisation des données génère ainsi des bénéfices économiques et sociétaux.

Sources : World Bank Group Big Data in action for governement, Aviseo Conseil 2021.

Une étude portant sur les enjeux de cybersécurité ainsi que sur les opportunités liées à la valorisation des données

La Fédération des Chambres de Commerce du Québec (FCCQ), un réseau de 130 chambres de commerce et de 1 100 membres corporatifs qui représentent plus de 50 000 entreprises, a mandaté Aviseo Conseil, firme spécialisée en économie et en stratégie, pour mener une étude sur la cybersécurité et les occasions de valorisation des données.

L'étude poursuit quatre objectifs principaux, lesquels sont énoncés ci-contre. Principalement, le but est d'approfondir les connaissances quant aux menaces auxquelles sont confrontées les entreprises en matière de cybersécurité, d'évaluer la façon dont elles ont évolué récemment et de les hiérarchiser en fonction du degré d'attention qu'on devrait leur porter. L'étude s'attarde aussi aux mesures d'atténuation disponibles, et analyse l'écart entre la situation actuelle et optimale en vertu de laquelle les risques seraient minimisés. Finalement, une revue des occasions liées à la valorisation des données est effectuée.

Objectifs de l'étude

1. **Recenser et évaluer l'impact des principales menaces envers les entreprises en matière de cybersécurité**
2. **Analyser l'efficacité des mesures d'atténuation disponibles**
3. **Offrir des pistes d'action pour renforcer la cybersécurité**
4. **Identifier les principales occasions à saisir en matière de valorisation des données**

FCCQ

Sources : FCCQ, Aviseo Conseil 2021.

Une approche structurée fondée sur l'analyse de données de qualité colligées auprès de sources primaires et secondaires

Une démarche en trois étapes

L'approche d'Aviseo est basée sur la collecte de données et une analyse rigoureuse visant à extraire les enseignements pertinents sur lesquels s'appuiera la formulation des recommandations. Le présent document étaye les résultats de cette démarche et est structuré en trois principales sections :

- État des lieux en matière de cybersécurité : recensement des principales menaces, positionnement en fonction de leur impact potentiel, revue sectorielle, identification des mesures d'atténuation existantes et analyse de leur efficacité
- Valorisation des données: recensement des enjeux pour les entreprises et gouvernements, analyse des occasions et revue de quelques pratiques inspirantes sur la scène internationale
- Recommandations: formulation des pistes d'action pour renforcer la cybersécurité des entreprises et saisir les occasions relatives à la valorisation des données.

Appuyée par une collecte de données auprès de quatre principales sources

- Revue de la littérature sur les enjeux de cybersécurité, les impacts sectoriels, les mesures de mitigation ainsi que des pratiques inspirantes en matière de valorisation de données
- Enquête auprès des membres de la FCCQ entre le 31 août et le 23 septembre 2021. L'outil d'analyse l'Observatoire FCCQ aura été utilisé afin de recueillir les informations des 130 entreprises participantes.
- Consultations auprès de huit experts en gestion de données et en cybersécurité provenant de différents secteurs qui a eu lieu entre le 5 août et le 14 septembre 2021
- Consultation auprès des comités de travail de la FCCQ en date du 5 octobre 2021

FCCQ
Fédération des chambres de commerce du Québec

SECTION 1

LA CYBERSÉCURITÉ : De nouveaux défis pour les entreprises

État des lieux en matière de cybersécurité

Principales menaces et leurs impacts

FCCQ
Fédération des chambres de commerce du Québec

Plusieurs facteurs contribuent à l'intensification des cybermenaces 1/3

Ère numérique

Crise sanitaire

Développements futurs

Ère numérique

– **Profusion de données –** l'avènement de l'ère numérique a permis aux entreprises de recueillir et de stocker une quantité massive de données. La valeur qui y est rattachée accroît la portée des dommages causés par un vol ou une coupure d'accès aux systèmes et les récompenses potentielles tirées par les cybercriminels.

– **Sophistication et démocratisation de la cybercriminalité –** avec la hausse des gains potentiels liés à la cybercriminalité, les cyberpirates ont raffiné leurs connaissances et leur expertise, développant de façon continue de nouvelles techniques ingénieuses pour voler les données.

– **Avènement des cryptomonnaies –** elles représentent un outil précieux pour recueillir efficacement le fruit des activités illicites sans laisser de trace dans le système bancaire.

– **Mutation de la guerre froide –** L'intimidation et l'espionnage entre états concurrents s'expriment désormais dans l'espace numérique. La Chine et la Russie par exemple ciblent les pays occidentaux et leurs entreprises pour espionner les activités ou simplement rendre inopérants les systèmes.

– **Recours aux technologies d'informatique en nuage –** l'explosion du marché du *cloud computing* a fait converger les données sensibles de plusieurs entités vers une infrastructure commune qui permet les redondances de sécurité.

Le gouvernement fédéral canadien à lui seul subit chaque année près de 2 500 tentatives d'intrusions informatiques de la part d'acteurs étatiques étrangers.

FCCQ

Sources : Arkos Labs, Centre canadien pour la cybersécurité, 2020 ; Enquête canadienne sur la situation des entreprises 2020 : Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023, Chaire de recherche du Canada en sécurité et technologie 2012, Aviseo Conseil 2021; COVID-19 and E-commerce: A Global Review, Forbes, CNUCED.

Plusieurs facteurs contribuent à l'intensification des cybermenaces 2/3

Ère numérique

Crise sanitaire

Développements futurs

La Covid-19 et la crise sanitaire

- **Décentralisation des réseaux informatiques –** L'adoption de nouveaux outils informatiques dans le cadre du télétravail et hors du cadre protégé et sécurisé usuel de la firme a créé de nouvelles occasions de cyberattaques. Les organisations dont 60 % des employés ou plus travaillent à distance depuis la pandémie ont encouru un coût par violation de la sécurité des données plus élevé.
- **Explosion du commerce en ligne –** Alors que le confinement devenait la nouvelle normalité, les entreprises et les consommateurs se sont tournés de plus en plus vers le numérique. La part du commerce électronique dans le commerce de détail mondial est ainsi passée de 14 % en 2019 à environ 17 % en 2020.
- **Hausse du recours aux visioconférences –** La pandémie a conduit de nombreux travailleurs à recourir aux visioconférences, un outil pratique en cas de confinement mais qui comporte aussi des failles.
- **Les infrastructures numériques de la santé deviennent une cible particulièrement prisée –** Elles disposent d'informations précieuses et sensibles et les recherches sur les vaccins et sont particulièrement visés par le vol de données et le cyber-espionnage.
- **Des pratiques défaillantes en matière de sécurité informatique –** La pandémie a créé des brèches en matière de cybersécurité, du fait de pratiques informatiques des employés – de plus en plus en télétravail – ne respectant pas les standards ou politiques définis par les organisations.

63 % des entreprises canadiennes ont constaté une augmentation des cyberattaques ciblées depuis qu'elles se sont tournées vers le télétravail.

Sources : Arkos Labs, Centre canadien pour la cybersécurité, 2020 ; Enquête canadienne sur la situation des entreprises 2020 : Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023, Chaire de recherche du Canada en sécurité et technologie 2012, Aviseo Conseil 2021; COVID-19 and E-commerce: A Global Review, Forbes, CNUCED.

Plusieurs facteurs contribuent à l'intensification des cybermenaces 3/3

Ère numérique

Crise sanitaire

Développements futurs

Développements futurs

– **Informatique quantique –** cette technologie superpuissante révolutionnera la science informatique au cours des prochaines années, avec de profondes implications pour la cybersécurité. Elle améliorera l'efficacité de la cryptographie ainsi que l'intelligence artificielle permettant de détecter et bloquer les cyberattaques. Le revers de la médaille est que les cybercriminels auront accès à une technologie plus puissante pour décrypter les informations. Par exemple, des données financières ou de sécurité nationale encryptées et volées aujourd'hui pourraient être décryptées dans plusieurs années à l'aide de l'informatique quantique.

– **Montée de la 5G et de l'Internet des objets –** accroîtront la surface d'attaque et la vulnérabilité des entreprises. Les objets connectés sont réputés mal protégés et le recours à cette technologie dans les activités de production accroît le pouvoir de négociation des criminels en cas de rupture de services. La 5G ouvrira néanmoins de nouvelles possibilités en matière de surveillance.

Le marché mondial des produits et services liés à la cybercriminalité passera de 204 milliards dollars canadiens en 2018 à 334 milliards en 2023.

Sources : Arkos Labs, Centre canadien pour la cybersécurité, 2020 ; Enquête canadienne sur la situation des entreprises 2020 : Cybersecurity Market by Solution, Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region – Global Forecast to 2023, Chaire de recherche du Canada en sécurité et technologie 2012, Aviseo Conseil 2021; COVID-19 and E-commerce: A Global Review, Forbes, CNUCED.

Ce n’est plus une question de savoir si une entreprise sera l’objet d’une cyberattaque, mais bien de quand elle sera attaquée

Au Québec, près de la moitié des entreprises sont conscientes d’avoir fait l’objet d’une ou de plusieurs cyberattaques. Cependant, seulement deux tiers de ces entreprises ont consacré des ressources afin de connaître leurs vulnérabilités et leurs risques.

Nombre d’entreprises qui pensent avoir été la cible d’une ou plusieurs cyberattaques
Membre FCCQ; 2021, en pourcentage

« Plus personne n’est à l’abri et ce ne sont pas seulement les grandes entreprises qui sont ciblées »

— Membre inter-comité FCCQ

« La nature des cyberattaques se diversifie de plus en plus et inclut maintenant des logiciels d’espion, des réseaux de zombies, et des vers informatiques »

— Expert en cybersécurité

Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021, Intercomité FCCQ le 5 octobre 2021, Aviseo Conseil 2021.

Les réseaux de zombies et les rançongiciels figurent parmi les techniques utilisées pour la perpétration de cyberattaques

Vecteur	Description	Menaces associées
Ordinateur zombie et réseau de zombies	Ce type d'attaque permet à un pirate de prendre le contrôle à distance d'un ordinateur ou d'un réseau d'ordinateurs sans le consentement et souvent sans la prise de conscience des victimes. Le logiciel malveillant est installé après une attaque ciblée, via une araignée* parcourant Internet ou non-intentionnellement par la victime après un clic sur un lien intégré dans un courriel, une publicité ou autre. Lorsque plusieurs ordinateurs sont infectés et connectés à l'ordinateur maître du pirate, celui-ci peut les contrôler de manière simultanée. Ce réseau de zombies peut regrouper des millions d'ordinateurs, de téléphones intelligents ou d'autres appareils numériques.	– **Pertes permanentes d'informations** – **Divulgation d'informations sensibles** – **Vol d'identité** – **Espionnage** – **Défiguration de sites web**
Rançongiciel	Le pirate installe un logiciel malveillant dans l'ordinateur ou le dispositif électronique pour bloquer l'accès à son contenu. Les rançongiciels sont installés après le clic de la victime sur un lien malveillant contenu dans un courriel, sur un réseau social ou un site web. Les rançongiciels peuvent également être installés par le maître ordinateur d'un réseau de zombies. Une fois fonctionnel, le rançongiciel peut encrypter les fichiers et les données, les rendant illisibles et inutilisables, afin que le pirate informatique exige une rançon à l'usager pour lui redonner l'accès.	– **Pertes permanentes d'informations** – **Divulgation d'informations sensibles** – **Vol d'identité** – **Espionnage** – **Exigence d'une rançon en cryptomonnaie en échange du rétablissement de l'accès à l'appareil et à ses fichiers** – **Dommages à l'équipement** – **Services techniques supplémentaires pour rétablir la fonctionnalité des systèmes**
Injection SQL	Il s'agit de l'intégration d'un code malveillant dans des applications web dans le but d'attaquer des sites web et collecter les données des utilisateurs. L'injection peut se faire via les données entrées, les modifications des cookies, des variables serveurs ou des outils de piratage automatisés.	– **Sabotage** – **Vol de données** – **Dégradation de l'image** – **Accès à d'autres parties de réseau interne**

Ressources additionnelles: *Dictionnaire de l'Office Québécois de la Langue Française en matière de cybersécurité*

FCCQ

** Partie du moteur de recherche qui surfe sur la toile, enregistre les URLs, classe les mots-clés et le texte de chaque page qu'il trouve*

Sources : Office de protection de la vie privée, McAfee, Norton, Aviseo Conseil 2021.

Les logiciels espions sont devenus particulièrement populaires depuis l'avènement des téléphones intelligents

Vecteur	Description	Menaces associées
Logiciel espion	Le pirate informatique installe un logiciel espion sur l'appareil électronique qui lui donne accès à distance au contenu et lui permet de suivre secrètement les activités. Les logiciels transmettent des informations en continu à l'auteur de l'attaque et sont généralement installés par la victime elle-même à la suite d'un clic sur un lien en apparence bénin. Le logiciel espion peut également être installé par une personne ayant accès physiquement à l'appareil.	– **Divulgation d'informations sensibles** – **Espionnage** – **Vol d'identité** – **Fraude bancaire**
Hameçonnage	L'hameçonnage, qu'on qualifie de piratage psychologique, n'est pas une technique qui fait appel à un logiciel malveillant ou à un code informatique, mais plutôt à la vulnérabilité humaine, comme la négligence ou la confiance aveugle. Le stratagème des pirates est de se camoufler derrière une entité fiable et d'inciter les victimes à dévoiler l'information les concernant, parfois sous peine de conséquences négatives. Le stratagème peut s'avérer plus ou moins sophistiqué, par exemple, un pirate peut utiliser le courriel d'un collègue de travail infiltré par une autre technique afin d'exiger des informations, ou simplement envoyer un courriel d'une boîte courriel qu'il a créé et dont l'adresse courriel comporte des similarités avec celle d'une entité fiable.	– **Pertes pécuniaires liées à une fraude** – **Vol d'identité** – **Espionnage** – **Divulgation d'informations sensibles**
Virus informatique	Le pirate attache le virus à un fichier, document ou programme exécutable téléchargé à partir d'un site web ou d'une pièce jointe à un courriel ou autre type de message, afin de l'installer sur l'appareil électronique de la victime. L'activation du programme, du fichier ou du document infecté lancera l'exécution du code informatique du virus qui se propagera dans le système et pourra infecter d'autres appareils d'un même réseau.	– **Corruption, suppression ou vol de données** – **Fraude bancaire** – **Espionnage** – **Divulgation d'informations sensibles** – **Pertes de temps liées au reformatage des systèmes et à la reprise du travail perdu**

Ressources additionnelles: *Dictionnaire de l'Office Québécois de la Langue Française en matière de cybersécurité*

Sources : Norton, gouvernement du Canada, McAfee, Aviseo Conseil 2021.

Le ver informatique et le cheval de Troie s'infiltrent de manière différente dans les systèmes mais ont des conséquences similaires à celles des virus

Vecteur	Description	Menaces associées
Vers informatique	Les pirates propagent les vers informatiques via des vulnérabilités logicielles. Le ver informatique est une série de codes malveillants conçus pour exécuter des actions dommageables mais à la différence d'un virus, il peut se propager de manière autonome dans les systèmes sans recours à un fichier hôte ou à une interaction humaine. Par exemple, il peut infecter un appareil lors d'un simple accès à un site web, l'ouverture d'un courriel ou un téléchargement de logiciel. Une fois le ver installé dans l'appareil, il infecte l'ensemble du système, voire l'ensemble du réseau auquel le système est relié.	– **Pertes permanentes d'informations** – **Divulgation d'informations sensibles** – **Vol de données et d'identité** – **Espionnage**
Cheval de Troie	Le cheval de Troie permet d'infiltrer un ordinateur lors de son téléchargement par la victime. Il s'agit d'un code ou d'un programme malveillant déguisé en fichier légitime. Contrairement au virus informatique, il ne peut s'exécuter ou se répliquer de manière autonome, et nécessite l'intervention humaine pour se propager. Ainsi, après avoir fait passer le cheval de Troie pour un programme légitime et que celui-ci est installé sur l'appareil, le cyberpirate pourra supprimer, modifier et capturer des données, espionner les activités ou intégrer l'appareil dans un botnet.	– **Pertes permanentes d'informations** – **Divulgation d'informations sensibles** – **Vol d'identité** – **Espionnage**

Ressources additionnelles: Dictionnaire de l'Office Québécois de la Langue Française en matière de cybersécurité

« Botnet » vient de la contraction des termes « robot » et « network » (réseau). En prenant le contrôle de chacun des ordinateurs infectés, les cyber-criminels se trouvent à regrouper au sein d'un réseau des « bots » gérables à distance.

Sources : Office de protection de la vie privée, McAfee, Aviseo Conseil 2021.

Les impacts des cyberattaques peuvent être répertoriés en six grandes catégories

Le vol de données ou le blocage des accès oblige l'organisation à radier des actifs ayant une certaine valeur monétaire.

La divulgation non autorisée d'informations privilégiées donne un avantage aux concurrents s'ils accèdent à ces informations, affectant négativement la position concurrentielle de l'entreprise sur son marché.

L'image de marque de l'organisation peut être négativement affectée non seulement auprès des clients, mais de l'ensemble des consommateurs ou usagers potentiels.

La perte de confiance des clients dans la sécurité des systèmes informatiques et la protection de leurs données confidentielles peuvent les pousser à cesser de faire affaires avec l'entreprises, affectant ainsi ses revenus et ses profits.

Les cyberattaques peuvent générer des dommages financiers directs à la suite d'une fraude bancaire, une demande de rançon, au paiement d'honoraires d'experts pour le rétablissement des systèmes ou au remplacement d'équipements devenus obsolètes.

Lorsque la cyberattaque a pour objectif de d'affecter les systèmes et de faire dérailler les activités normales de l'entreprise, les impacts peuvent s'avérer importants sur les finances ou la sécurité des clients.

Sources : Cisel, S.Ghernaouti, Aviseo Conseil 2021.

Certaines menaces sont associées à des techniques précises

Impacts		Perte de savoir corporatif	Rupture des opérations	Perte de confiance de la clientèle	Dommages financiers directs	Mise en péril de l'avantage concurrentiel	Atteinte à l'image de marque
Menaces		– Pertes permanentes d'informations – Espionnage – Blocage d'accès – Vol de données	– Attaque de déni de service – Blocage d'accès – Sabotage	– Divulgation d'informations sensibles – Vol d'identité	– Vol d'identité – Fraude bancaire – Demande de rançon – Dommages aux équipements – Honoraires d'experts	– Espionnage – Vol de données	– Attaque de déni de services – Défiguration de site web – Vol d'identité – Sabotage
Vecteurs d'attaque	**Ordinateur zombie**						
	Rançongiciel						
	Injection SQL						
	Logiciel espion						
	Hameçonnage						
	Virus informatique						
	Ver informatique						
	Cheval de Troie						

Légende

Fréquence d'utilisation : Faible – Élevée

Sources : BPIFrance, Aviseo Conseil 2021.

Les coûts liés à une violation de la sécurité des données au Canada sont parmi les plus élevés au monde

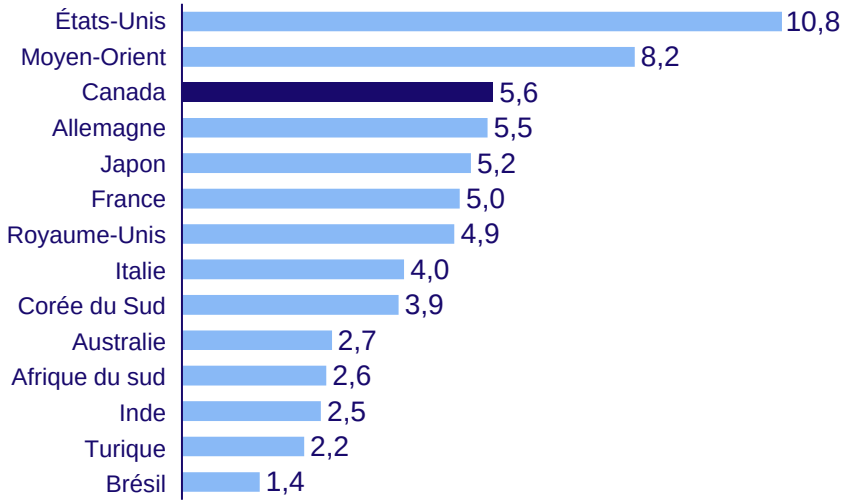
Le coût moyen d'une violation de données au Canada est estimé à 5,6 M$, ce qui lui confère le 3e rang mondial :

– Ces coûts incluent les services légaux et de conformité, les frais liés à l'expertise technique, les dommages à l'image de marque et à la perte de clients et de productivité.

– Ces coûts sont d'autant plus significatifs lorsqu'on considère que les 2/3 des petites et moyennes entreprises n'ont pas d'assurance contre les cyber-risques

– De plus, 60 % de leurs employés ne sont pas formés adéquatement pour repérer et atténuer les cybermenaces.

Coût moyen d'une violation de données, par pays
2020; en millions de dollars américains



Indicateurs de cybersécurité des petites et moyennes entreprises
2020; Canada

Thème	Indicateur (en moyenne)	
	59 heures	… durant lesquelles les activités de l'entreprise ont été interrompues
	12 000 $	… par employé pour se rétablir d'une atteinte
	1/3 des entreprises	… n'ont pas d'assurance contre les cyber-risques au Canada
	60 % des employés	… ne sont pas formés pour repérer et atténuer les cybermenaces

Sources : IBM, Scalar 2018, Statistique Canada, Ponemon Institute, In-Sec-M, Aviseo Conseil 2021.

La perte de revenus d'activités représente la catégorie de coûts la plus importante pour les entreprises ciblées par une cyberattaque

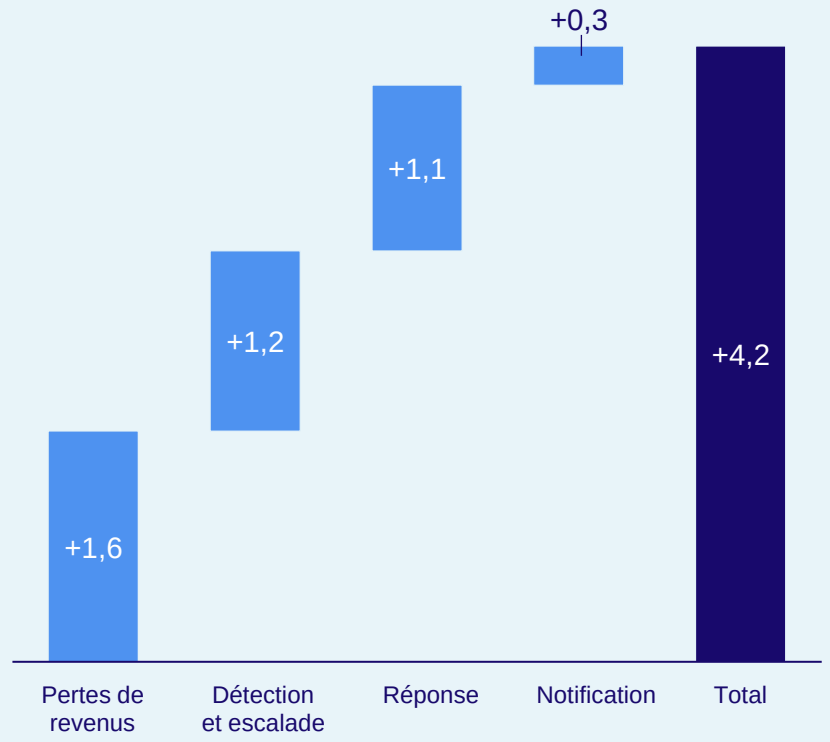
La perte cumulée de la rupture des activités, de la diminution de la clientèle et des dommages réputationnels demeure la composante la plus importante des coûts liées à une violation de la sécurité des données

– Elle représente 1,6M$, soit 38 % du coût de l'épisode moyen.

En amont, la détection de la violation, soit tous les frais déboursés pour l'enquête et les vérifications, la gestion de crise et les communications de la haute gestion, représentent la deuxième composante en importance avec 1,2 M$.

Enfin, la réponse à l'attaque, qui comprend les honoraires des techniciens et experts dédiés au rétablissement des systèmes, les frais légaux inhérents à la défense contre les poursuites des clients ou pour les procédures contre les cybercriminels, ainsi que les amendes potentielles, représentent 26 % des coûts.

Coût moyen d'une violation de données par type
Monde; 2021; en millions de dollars américains



Sources : IBM, Aviseo Conseil 2021.

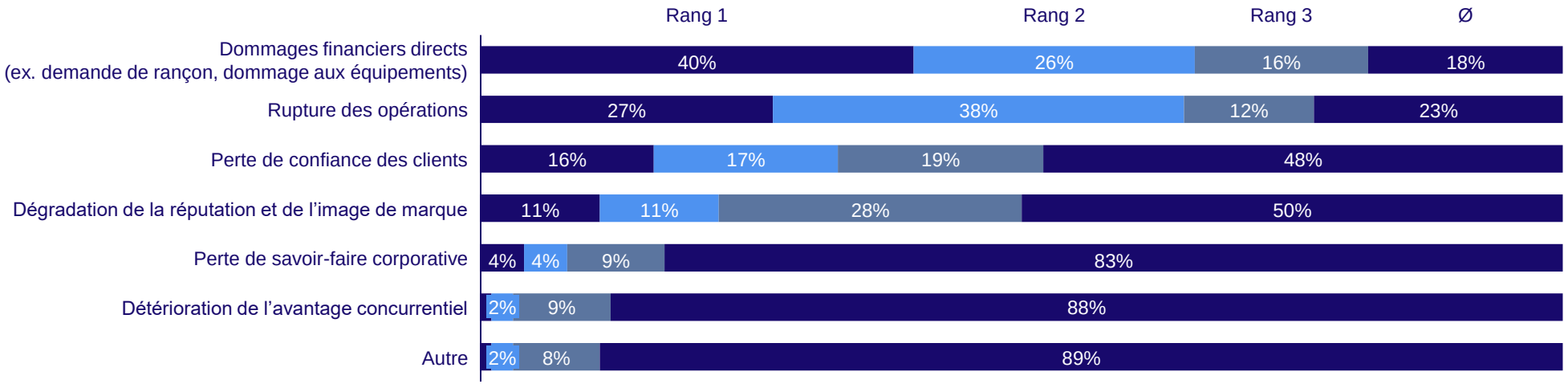
La vitesse d'évolution des techniques d'attaques rend les entreprises plus vulnérables

Certaines nouvelles tendances se manifestent depuis la dernière année :

- Il est devenu profitable d'attaquer les entreprises : Il se vend des produits de cyberattaques à des gens peu expérimentés contre une rémunération
- Les employés deviennent intéressés aussi à vendre des données car ils en réalisent la valeur monétaire

L'augmentation du nombre d'attaques et l'étendue des impacts liés aux cyberattaques forcent les entreprises à devoir déployer des mesures toujours plus rapidement. Les dommages financiers sont l'impact que les entreprises au Québec craignent le plus, suivi d'une rupture des opérations et la perte de confiance des clients.

Impacts liés à une cyberattaque que les entreprises craignent le plus
Membre FCCQ ; 2021 ; en pourcentage



Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021, Intercomité FCCQ, le 5 octobre 2021, Entrevues effectuées auprès d'experts du 15 aout au 14 septembre 2021 Aviseo Conseil 2021.

État des lieux en matière de cybersécurité

Analyse sectorielle

FCCQ
Fédération des chambres de commerce du Québec

Les formes d'attaques et les motivations des cyberpirates peuvent différer selon le secteur économique visé

SANTÉ

La pandémie de la COVID-19 aura montré une certaine vulnérabilité des infrastructures numériques dans les réseaux de la santé avec une hausse des occurrences de violation de données au cours de l'année 2020. Bien que le secteur recense un faible pourcentage d'incidents, ceux-ci sont extrêmement coûteux lorsqu'ils surviennent. Ils pourraient également s'accroître dans l'avenir avec la montée de la télémédecine.

SERVICES FINANCIERS

En raison de la nature des services et des gains potentiels que peut générer une cyberattaque envers une entreprise de services financiers, ce secteur est le plus exposé et risque les conséquences les plus importantes. En contrepartie, il est celui dont les mécanismes de protection sont parmi les plus sophistiqués.

SERVICES PROFESSIONNELS

Le secteur des services professionnels qui comprend entre autres le génie-conseil, les services d'architecture ou scientifiques, ont été désignés comme particulièrement vulnérables aux attaques par hameçonnage. L'utilisation intensive du courriel peut expliquer cette situation.

SECTEUR TECHNOLOGIQUE

Les entreprises technologiques dont le modèle d'affaires repose sur la collecte et l'exploitation des données de leurs utilisateurs, peuvent être vulnérables à l'usurpation de données personnelles. Comme leur expertise d'affaires se situe dans le domaine numérique, elles sont généralement mieux protégées contre les attaques mais peuvent aussi faire preuve d'une trop grande confiance.

MANUFACTURIER & LOGISTIQUE

Le secteur manufacturier ainsi que celui du transport et de la logistique étant de plus en plus numérisés, les entreprises œuvrant dans ces secteurs sont devenues vulnérables aux infiltrations dans les systèmes et de ce fait à l'espionnage industriel, le vol de données ou le sabotage des processus de production ou de livraison.

COMMERCE DE DÉTAIL

Avec la montée en popularité du commerce électronique, les boutiques en ligne et leur système de paiement sont devenus des cibles, notamment pour les attaques par hameçonnage. Comme les banques de données contiennent des informations financières et personnelles sur les consommateurs, ces attaques qui requièrent peu de sophistication peuvent s'avérer très payantes.

FCCQ

Sources : Proofpoint, Aviseo conseil 2021.

Les cybercriminels savent exploiter les vulnérabilités des organisations œuvrant dans le domaine de la santé

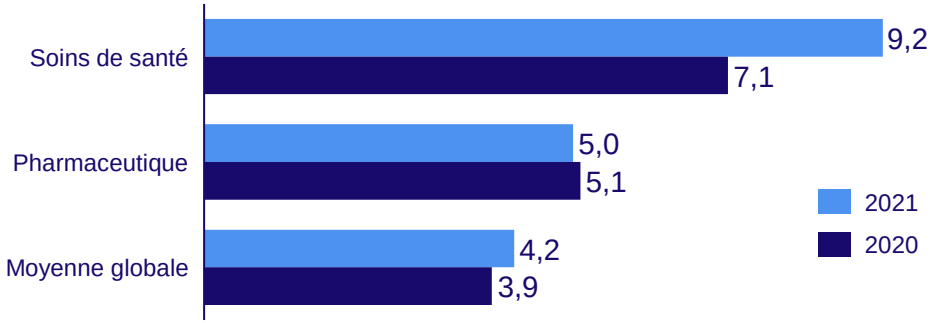
SECTEURS DES SOINS DE SANTÉ ET PHARMACEUTIQUE

Intérêt des cyberpirates

- **Une rupture d'activités névralgiques :** les opérations des organisations du secteur de la santé ayant une grande incidence sur la vie des usagers, le rapport de force est extrêmement fort en faveur des cybercriminels lorsque vient le temps par exemple d'exiger des rançons. Les cybercriminels menacent également de divulguer les données sensibles pour atteindre la réputation
- **Emprise sur des données de valeur :** les dossiers des patients ont une très grande valeur sur le marché noir puisqu'ils renferment des informations qui permettent de cibler efficacement des clients potentiels. Les données peuvent également être utilisées pour frauder les compagnies d'assurances.

Coût moyen d'une violation de données, par secteur

2020-2021; en millions de dollars américains



TYPES DE CAS

- En 2015, des cybercriminels ont accédé aux dossiers personnels de 78 millions d'usagers de la société américaine Anthem Blue Cross. Plusieurs autres sociétés ont vécu la même situation : Premera Bluecross (11 M $), Excellus Bluecross Blueshield (10 M$), Tricare (5 M$).

Sources : IBM, Forbes, Los Angeles Times, Aviseo Conseil 2021.

Les attaques dans le secteur financier provoquent un effet domino affectant plusieurs maillons du réseau et générant des coûts élevés

SECTEUR DES SERVICES FINANCIERS

Intérêt des cyberpirates

- **Les gains potentiels élevés.** Le secteur financier est particulièrement lucratif et les entreprises ont les moyens de débourser les rançons. Les attaques de déni de services sont fréquentes et souvent utilisées comme moyen de diversion pour voler des données sensibles. Les données sont par la suite utilisées pour procéder à des fraudes
- **Le rôle névralgique du système financier pour la sécurité nationale.** Le secteur financier en Amérique du Nord est vulnérable aux attaques commanditées par des états étrangers concurrents comme la Russie, la Chine et la Corée du Nord, qui voudraient déstabiliser l'économie et plus globalement le fonctionnement des sociétés occidentales.

Coût moyen d'une violation de données, par secteur

2021; en millions de dollars américains

TYPES DE CAS

- Le secteur financier a subi des cyberattaques auprès de joueurs majeurs, tels Desjardins, Equifax et Capital One
- Au cours des premiers mois de 2020, la hausse des cyberattaques a atteint 238 %
- Le nombre de demandes de rançon a été neuf fois plus élevé au début de la pandémie par rapport aux années antérieures.

Sources : Security Boulevard, VMWare Carbon black threat, Federal Reserve Bank, IBM, Aviseo Conseil 2021.

La vulnérabilité du secteur des services professionnels se situe principalement dans les données sensibles

SECTEUR DES SERVICES PROFESSIONNELS

Intérêt des cyberpirates

- **Une concentration de données sensibles.** Les bureaux d'avocats et de comptables, à titre d'exemple, détiennent des secrets corporatifs, des rapports d'impôts et d'autres documents renfermant des informations qui peuvent heurter sévèrement les entreprises si elles sont dévoilées. Le levier de négociation des cybercriminels, en cas d'attaque par rançongiciel, est élevé.
- **Des mécanismes de protection moins robustes.** Contrairement au secteur des technologies ou de la finance, les entreprises du secteur des services professionnels n'ont souvent pas l'expertise interne et les mécanismes appropriés en matière de cybersécurité. Outre les grandes organisations qui peuvent se permettre d'embaucher des experts, la totalité du personnel œuvrant dans les plus petites organisations possèdent des qualifications liées aux services offerts uniquement (ex. droit, architecture, génie).

Coût moyen d'une violation de données, par secteur

2021; en millions de dollars américains

TYPES DE CAS

- En 2020 aux États-Unis, des hackers ont envoyé des courriels à des firmes d'avocats comportant des pièces jointes infectées et ont réussi à subtiliser les données de cinq d'entre elles. Devant le refus de deux d'entre elles de payer la rançon exigée, ils ont publié des données sensibles sur un site web pouvant être consulté par tous
- Au Québec, en septembre 2021, le cabinet de comptables Mallette aurait été la cible de cyberattaque.

FCCQ

Sources : IBM, Lawsites blog, Forbes, https://www.journaldequebec.com/2021/09/03/un-cabinet-comptable-pirate, Aviseo Conseil 2021.

Les entreprises technologiques présentent des caractéristiques propres qui les exposent aux cyberattaques

SECTEUR TECHNOLOGIQUE

Intérêt des cyberpirates

- **Une concentration de données monnayables.** Les entreprises technologiques fondent leur modèle d'affaires sur la cueillette et l'exploitation des données. Les cybercriminels sont conscients que d'autres entreprises sont prêtes à payer pour acquérir ces données et les exploiter eux-mêmes. De plus, les entreprises du domaine informatique hébergent les données de milliers d'autres entreprises
- **Des vulnérabilités propres au secteur.** Les entreprises technologiques et leurs employés sont les premiers utilisateurs des nouvelles technologies, logiciels et applications disponibles sur le marché. Leurs mécanismes de protection peuvent varier selon leur degré de maturité.

Coût moyen d'une violation de données, par secteur

2021; en millions de dollars américains

TYPES DE CAS

- En 2021, Microsoft a été victime d'une cyberattaque qui a permis l'accès au contenu de 250 000 serveurs. Les auteurs ont pu espionner les courriels de chercheurs du domaine de la santé, de bureaux d'avocats, d'organisations non-gouvernementales et autres
- En 2021, le fournisseur de logiciels Kaseya a été victime d'une attaque qui a affecté 2 000 organisations à travers le monde.

Sources : Wikipedia, IBM, Aviseo Conseil 2021.

Le passage à l'industrie 4.0 augmente les risques de sécurité dans les secteurs manufacturier, du transport et de la logistique

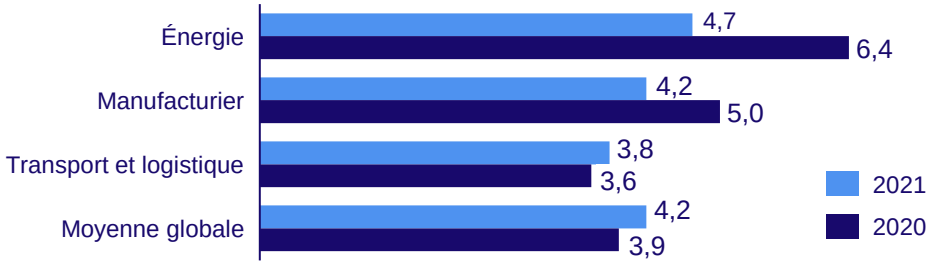
SECTEURS MANUFACTURIER, TRANSPORT ET LOGISTIQUE

Intérêt des cyberpirates

- **Les gains potentiels croissants.** Une attaque qui paralyse les opérations d'une firme manufacturière ou de transport et logistique peut s'avérer extrêmement coûteuse et les exigences de rançon peuvent être substantielles
- **Les données monnayables sur le maché noir.** Les opérations sont de plus en plus numérisées et les bases de données renferment les secrets industriels et autres données sensibles qui ont une valeur sur le marché noir. Cela donne lieu à un « second effet ».

Coût moyen d'une violation de données, par secteur

2021; en millions de dollars américains



TYPES DE CAS

- En 2017, Renault-Nissan a subi une attaque de type rançongiciel qui a mis à l'arrêt la production dans cinq usines à travers le monde, dont en France. Les pertes sont estimées à quelques milliards de dollars
- Le Colonial pipeline qui achemine du gaz et du carburant pour avions du Texas jusqu'aux états du sud-est des États-Unis a subi, en 2021, une attaque de rançongiciel ciblant le système informatique qui gère l'infrastructure. La demande de rançon était de 4,4 M $, mais les dommages sont estimés à 50 M$.

Sources : IBM,, Infidem, https://www.lesoleil.com/actualite/monde/une-cyberattaque-provoque-la-fermeture-du-plus-grand-oleoduc-dessence-aux-etats-unis-472e7ac11644ff6586ab825c2fd43684, Aviseo Conseil 2021.

La montée du commerce électronique accroît le nombre et la portée des attaques dans le secteur du commerce de détail

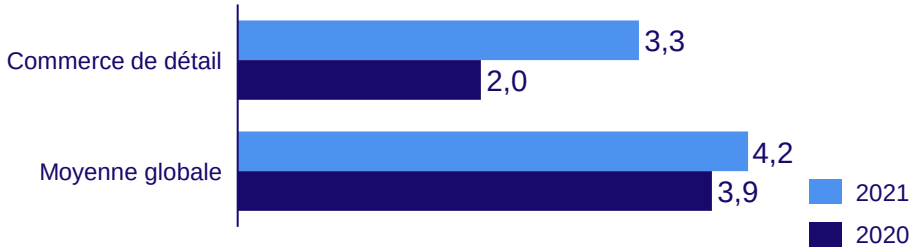
SECTEUR DU COMMERCE DE DÉTAIL

Intérêt des cyberpirates

- **Une concentration de données de paiement.** Les entreprises du commerce de détail possèdent des banques de données importantes renfermant les informations sur les cartes de crédit lesquelles peuvent être associées à des noms.
- **Des gains rapides.** Bien que les gains potentiels puissent être moins attrayants que ceux d'autres secteurs, les systèmes de protection moins sophistiqués peuvent s'avérer des cibles plus facilement pénétrables. Les employés constituent également une menace plus importante dans cette industrie où les qualifications exigées sont moindres et où le taux de roulement du personnel est plus important.

Coût moyen d'une violation de données, par secteur

2021; en millions de dollars américains



TYPES DE CAS

- Les courriels d'hameçonnage sont particulièrement fréquents, tout comme ceux par rançongiciel. Les cybercriminels ciblent des moments précis, comme le Vendredi Noir ou la période des fêtes afin de bénéficier d'un levier de négociation maximal.
- Un sondage réalisé par Sophos à travers le monde a révélé que 44 % des entreprises du commerce détail ont été victimes d'une attaque par rançongiciel en 2020, ce qui en fait le secteur le plus touché.

Sources : Sophos, IBM, Aviseo Conseil 2021.

État des lieux en matière de cybersécurité

Revue des mesures atténuantes

FCCQ
Fédération des chambres de commerce du Québec

Plusieurs stratégies et mesures existent pour limiter la probabilité d'occurrence d'une cyberattaque 1/2

Mesures pour diminuer la probabilité d'occurrence	Description	Exemples
Formation et sensibilisation des employés	La sensibilisation et la formation des employés aux risques de l'organisation leur permettent de devenir des alliés dans la lutte à la cybercriminalité. L'hameçonnage constituant une technique répandue et trop souvent efficace pour les cybercriminels, des employés conscients des méthodes et des risques seront plus alertes et plus efficaces pour parer les attaques en amont	– Création d'une « certification interne» obligatoire et octroyée à la suite d'une formation donnée par un expert – Lecture obligatoire d'un courriel mensuel de sensibilisation donnant des exemples de cyberattaques réelles
Authentification robuste	La mise en place de politiques d'authentification des utilisateurs répondant aux besoins en matière de cybersécurité limitera les risques d'infiltration	– Authentification multi facteur
Contrôles d'accès et d'autorisation	La prévention de la compromission des données passe par un octroi ciblé des accès et limité aux employés qui en ont réellement besoin	– Gestion des privilèges administratifs
Sauvegarde des données	La conservation des copies de sauvegarde chiffrées dans un endroit sécurisé	– Copies de sauvegarde hors site avec accès très limité
Audit de sécurité	Un recours aux services d'un expert externe afin de détecter les vulnérabilités et failles de sécurité exploitables, l'évaluation de leur niveau de criticité et la conception d'un plan afin d'améliorer la robustesse des mesures de cybersécurité	– Cartographie des points de vulnérabilité – Plan d'actions pour diminuer la probabilité d'occurrence d'une cyberattaque
Système de détection d'intrusion	Une surveillance intelligente protège la disponibilité, la confidentialité et l'intégrité des réseaux	– Système d'intelligence artificielle
Logiciels de sécurité	La mise en place de logiciels de sécurité pour bloquer les attaques et les sites malveillants et pour protéger contre les maliciels	– Pare-feu, antivirus, anti-maliciels – Filtre de système d'adressage par domaine (DNS)
Mise en place d'un chef de la sécurité informatique (CISO)	La création d'une fonction dédiée à la cybersécurité et piloté par une ressource certifiée de type CISO permet d'harmoniser les pratiques internes et de centraliser l'imputabilité en matière de gestion des risques technologiques	– Développement et partage de politiques et procédures s'appuyant sur les meilleures pratiques – Centralisation de l'expertise en sécurité technologique

Sources : Centre canadien pour la cybersécurité, Statistique Canada, Entrevues effectuées auprès d'experts du 15 aout au 14 septembre 2021, Aviseo Conseil 2021.

Plusieurs stratégies et mesures existent pour limiter la probabilité d'occurrence d'une cyberattaque 2/2

« **La hausse des cyberattaques est fulgurante.** L'enjeu est de déployer les mesures plus rapidement dans en environnement ou les ressources humaines spécialisées manquent.

Le premier outil est la sensibilisation des employés, encore plus vital en télétravail. Il faut assurer une bonne gouvernance des données, notamment la gestion des accès.

De plus, il faut **rehausser le niveau de sécurité des partenaires et tierces parties**.

Dans le futur, **l'objectif** ne sera pas seulement monétaire mais plus **politique et stratégique** (ex. attaquer des hôpitaux, des infrastructures publiques) »

— Expert en assurances

Sources : Experts consultés entre le 15 aout et 23 septembre 2021 Aviseo Conseil 2021.

Si les techniques visant à parer la cyberattaque ont failli, certaines mesures peuvent être déployées pour en atténuer l'impact 1/2

Mesures pour atténuer l'impact	Description	Exemples
Plan de récupération	En amont de l'attaque, la préparation d'un plan exhaustif et horizontal de gestion de crise, établissant le chemin vers le rétablissement normal des opérations selon divers scénarios.	– Restriction de l'accès au secteur touché – Préparation de la réaction face à une demande de rançon – Liste des actifs perdus ou affectés – Séquence d'actions pour le retour à la normale – Identification des employés ou consultants externes appelés à participer à la séquence d'actions
Correction et optimisation	L'automatisation des mesures d'intervention en cas d'incident.	– Système de gestion des correctifs
Intelligence artificielle	L'utilisation de l'intelligence artificielle pour repérer les attaques rapidement et pour agir avec célérité pour limiter les dommages.	– Analyse des comportements des usagers en temps réel et détection des anomalies – Prédiction du risque de faille
Formation des employés	L'adoption des programmes de formation aux protocoles, politiques et procédures de cybersécurité.	– Processus de gestion des incidents – Plan de continuité – Bases de connaissance
Assurances	Souscription à une assurance pour permettre une compensation financière en cas de dommages liés à une cyberattaque ainsi qu'un paiement d'une réclamation par une tierce partie pour des enjeux que l'entreprise n'aura pas su traiter par elle-même	– Couverture des pertes directes – Couverture d'assurance responsabilité

Sources : Centre canadien pour la cybersécurité, Statistique Canada, Entrevues effectuées auprès d'experts du 15 aout au 14 septembre 2021, Aviseo Conseil 2021.

Si les techniques visant à parer la cyberattaque ont failli, certaines mesures peuvent être déployées pour en atténuer l'impact 2/2

« L'aide gouvernementale est peu présente dans les services, mais plutôt dans l'innovation de l'industrie de la cybersécurité. Ça aide les entreprises à développer des nouveaux produits en cybersécurité. Mais les entreprises ont besoin d'aide **pour développer leurs programmes contre les cyber attaques**. »

— Expert In-Sec-M

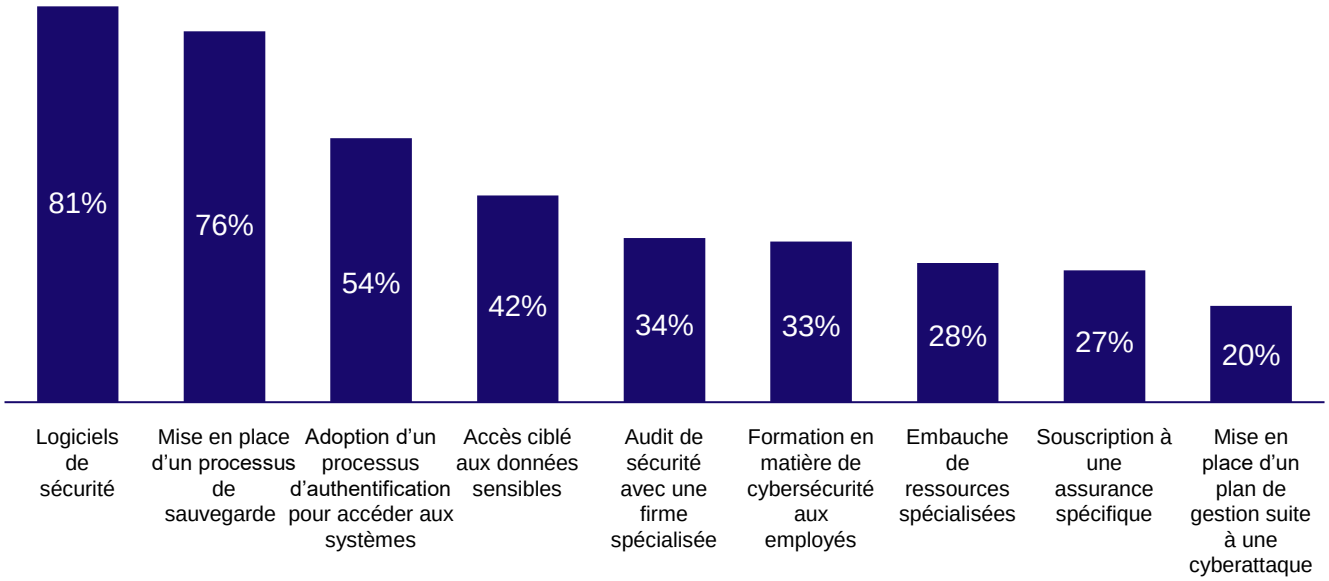
« Au Québec, on a beaucoup de PME. **Comment fait-on pour protéger ces entreprises** alors qu'ils ne connaissent même pas la problématique et qui n'ont pas d'expertise en matière de cybersécurité ? »

— Expert Cybereco

Sources : Experts consultés entre le 15 aout et 23 septembre 2021, Aviseo Conseil 2021.

L'installation de logiciels de sécurité et les dispositifs de sauvegarde constituent les mesures les plus implantées par les entreprises au Québec

Mesures de protection implantées dans les entreprises
Membre FCCQ; 2021; en pourcentage



« Les entreprises peuvent mettre en place un système de quatre contrôles de prévention :

- Avoir un plan de cybersécurité
- Avoir des applications automatiques
- Utiliser des mots de passe à facteurs multiples
- Avoir des sauvegardes »

— Expert du Centre canadien pour la cybersécurité

Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021; experts consultés entre le 15 aout et 23 septembre 2021; Aviseo Conseil 2021.

État des lieux en matière de cybersécurité

Analyse d'écart

FCCQ
Fédération des chambres de commerce du Québec

Le risque 0 n'est pas atteignable, mais les entreprises peuvent encore faire beaucoup de chemin pour optimiser leur niveau de protection

Situation actuelle au Québec

50 % des entreprises jugent que leurs mesures de cybersécurité sont adéquates et suffisantes

66 % des entreprises dédient des ressources pour connaître ses vulnérabilités et les risques

81 % utilisent des logiciels de sécurité

76 % ont un processus de sauvegarde des données

33 % offrent de la formation aux employés

27 % ont souscrit à une assurance visant à se protéger contre les cyber risques

20 % ont un plan de gestion en cas d'occurrence

« Il ne devrait pas avoir d'innovation technologique sans prendre en compte la cybersécurité. Cette dernière n'est pas pensée dès le départ dans les innovations technologiques.

La cybersécurité arrive trop tard dans l'équation et les entreprises ne veulent pas investir en cybersécurité.

Il y a de plus en plus d'objets connectés et il faut trouver des façons de former les gens en cybersécurité sur les nouvelles technologies (IoT, Infonuagique, etc). »

— Expert Cybereco

Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021; experts consultés entre le 15 aout et 23 septembre 2021; Aviseo Conseil 2021.

La rareté de la main-d'œuvre est un enjeu criant dans un contexte où la demande augmente de façon importante

L'un des principaux défis pour les organisations est de recruter des talents expérimentés. L'écart entre l'évolution des technologies et des cyber-risques et les capacités d'adaptation en cybersécurité pour les organisations ne cessent de croître. Cette tendance entraine une augmentation des besoins en termes de talents.

Bien que les investissements de la dernière décennie en cybersécurité aient augmenté, les organisations de tous les secteurs constatent des lacunes grandissantes.

Entre 2016 et 2021 la demande de talents en cybersécurité a augmenté de plus de 40%.

« Les besoins en matière de cybersécurité ne cessent d'évoluer car les attaques deviennent beaucoup plus sophistiquées et la surface d'attaque augmente.

Le manque de ressources compétentes est le problème majeur. »

— Expert In-Sec-M

Demande de cyber talents au Canada

Canada; 2016-2021; en nombre de professionnels

Entre 2016 et 2021. une estimation prévoit que les organisations devront pourvoir plus 8 000 nouveaux postes de professionnels de la cybersécurité pour répondre à la demande, ce qui représente une croissance annuelle d'environ 7 %

Sources : Deloitte; experts consultés entre le 15 aout et 23 septembre 2021; Aviseo Conseil 2021.

La sensibilisation et la formation des employés constituent des mesures incontournables pouvant générer des bénéfices importants

Seulement le tiers des entreprises affirme offrir de la formation relative à la cybersécurité à leurs employés, alors qu'on estime que quatre infractions de données sur dix résultent du comportement des employés

- Ces infractions peuvent être liées à un comportement malhonnête, mais également à la négligence ou à des incidents mettant en cause des employés
- Les attaques par hameçonnage sont fréquentes, et certaines études concluent même que 91 % des cyberattaques sont la résultante d'un clic inséré dans un courriel.

La formation magistrale traditionnelle n'est pas considérée comme la meilleure forme de sensibilisation des employés puisque la cybersécurité constitue pour plusieurs un sujet aride qui s'ajoute à leur charge de travail

- Les formations interactives peuvent être davantage mobilisatrices et efficaces.

Méthodes les plus efficaces pour réduire les coûts liés aux violations de données

Rang	Mesure
1	**Encryptage des données**
2	**Désignation d'une équipe dédiée pour répondre aux cyberattaques**
3	**Politique de gouvernance des données**
4	**Formation des employés**

Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021; Intercomité FCCQ le 5 octobre 2021; Forrester; Harvard Business Review; Ponemon Institute; Wall Street Journal; Aviseo Conseil 2021.

Trop peu d'entreprises ont préparé un plan de gestion détaillé pour faire face à une cyberattaque

Il semble un peu paradoxal que 66 % des entreprises au Québec affirment dédier des ressources pour connaître les vulnérabilités et les risques que présentent leur organisation en matière de cybersécurité et que seulement 20 % ont mis en place un plan de gestion détaillé suite à une cyberattaque

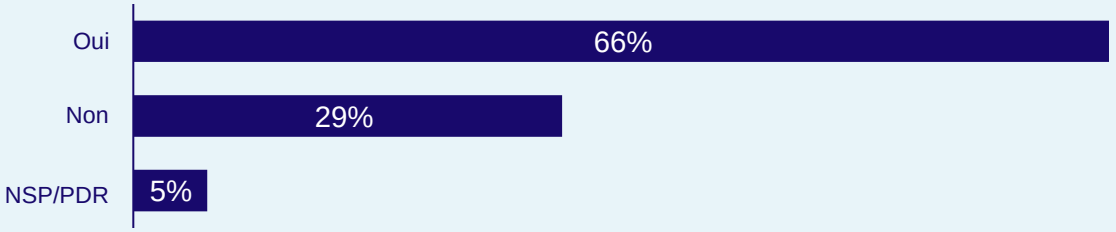
– Et cette situation ne s'explique pas par un sentiment de sécurité car la moitié des entreprises juge que leurs mesures ne sont pas adéquates.

Or, la très grande efficacité des plans de gestion des cyberattaques est reconnue par 61 % des organisations américaines sondées en 2020

– Il s'agissait de la meilleure méthode de protection selon les répondants.

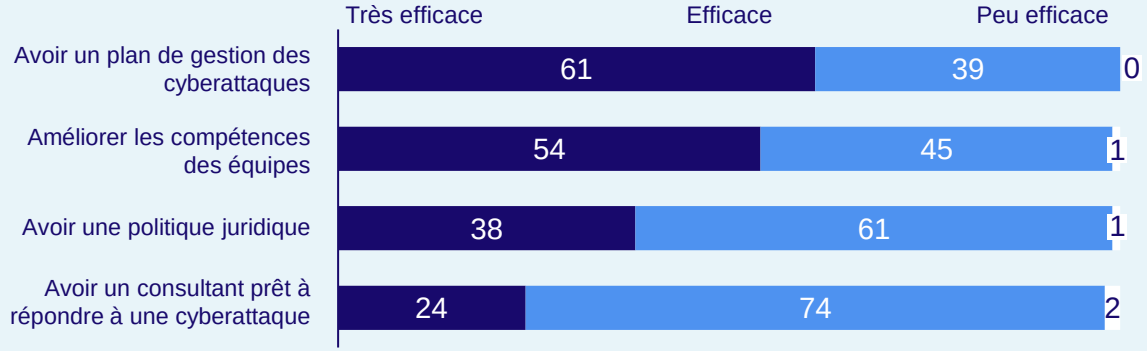
Nombre d'entreprises qui dévouent des ressources afin de connaître leurs vulnérabilités et risques liés aux cyberattaques

Membre FCCQ; 2021, en pourcentage



Perceptions des organisations face à l'efficacité de diverses méthodes pour faire face à des cyberattaques

États-Unis; en pourcentage



Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021, Osterman Research; Aviseo Conseil 2021.

Le quart des entreprises affirme souscrire à une assurance contre les cyberattaques, mais cette proportion pourrait s'éroder dans l'avenir

La hausse marquée des incidents de cybersécurité au cours des derniers mois a affecté considérablement la rentabilité de cette activité pour les sociétés d'assurances

- 17% des organisations canadiennes ont subi une cyberattaque de type rançongiciel au cours des derniers mois. 69% des entreprises ciblées par un rançongiciel disent qu'elles ont payé la rançon que leur demandaient les pirates informatiques
- Les primes pourraient augmenter au cours des prochaines années afin de s'ajuster à l'augmentation des occurrences et des coûts
- L'étendue des couvertures pourrait également devenir plus limitée ou le montant maximal d'une réclamation plus faible.

Les entreprises doivent donc se soucier autant sinon davantage de la mise en place de mesures de protection adéquates pour parer les cyberattaques et les neutraliser rapidement

- Une collaboration étroite entre l'assurée et l'assureur permettrait également à celui-ci de raffiner ses connaissances des risques et d'être davantage proactif pour contrer les cyberattaques et à terme réduire ses coûts.

« La valeur ajoutée de la police d'assurance est l'accompagnement offert pour le rétablissement des activités offert en collaboration avec le réseau de partenaires. »

— Un expert du domaine de l'assurance

« Les entreprises ne savent pas trop quoi faire et à défaut, elles prennent une assurance mais qui n'est pas forcément adéquate. »

— Membre inter-comité FCCQ

Sources : Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021; experts consultés entre le 15 aout et 23 septembre 2021; Cira, l'Autorité canadienne pour les enregistrements internet, qui gère les domaines .ca, Aviseo Conseil 2021.

FCCQ
Fédération des chambres de commerce du Québec

SECTION 2

LA VALORISATION DES DONNÉES : De nouvelles opportunités pour les entreprises

La valorisation des données est désormais un incontournable pour toute entreprise qui aspire à se distinguer, à poursuivre son développement

AUTANT POUR LES GRANDES ENTREPRISES QUE LES PME.

Si autrefois l'enjeu était la disponibilité des données, aujourd'hui c'est leur abondance qui représente un défi pour les organisations.

On réfèrera à l'expression ***Big Data*** – les données massives – pour faire référence à ces données fragmentées qui offre un potentiel stratégique et économique.

La présente section vise à présenter l'importance de ces bénéfices pour les entreprises en particulier et pour la société de manière générale.

Valorisation des données

L’opportunité pour les entreprises

FCCQ
Fédération des chambres de commerce du Québec

Cette nouvelle ressource qu'est la donnée

Les données sont maintenant qualifiées de véritable « or digital » car il est de plus en plus évident que les données sont désormais considérées comme une ressource clé et un atout stratégique pour les entreprises :

- Les nouvelles technologies ont rendu possible la collecte et l'exploitation d'une masse de données importante et c'est ainsi que la donnée a fini par être considérée par tous comme un actif clé de l'entreprise
- Mais comme tout actif, son exploitation a un coût et nécessite en l'occurrence la mise en place d'un minimum d'outils informatiques
- Avec l'augmentation du volume de données disponibles, les enjeux se déplacent ainsi davantage vers l'utilisation de ces données.

« Le *Big Data* représente les actifs informationnels caractérisés par un volume, une vélocité et une variété tellement élevés qu'ils nécessitent une technologie et des méthodes d'analyse spécifiques pour leur transformation en valeur. »

— De Mauro et al. (2015)

« La valorisation de données offre des opportunités de faire des revenus additionnels et de créer de nouveaux modèles d'affaire. Qui plus est, les données permettent non seulement de faire de la prévention, de réduire le d'arrêt de production mais offrent également un potentiel de prévision incroyable. »

— Membre inter-comité FCCQ

Sources : De Mauro 2015; Hilbert 2016; Intercomité FCCQ le 5 octobre 2021; Aviseo Conseil 2021

Le *Big Data* est caractérisé par quatre grandes dimensions

Dans les faits, le terme Big Data est utilisé pour décrire un large éventail de concepts : de la capacité technologique à stocker, agréger et traiter les données, au changement culturel qui affecte les entreprises et la société.

L'ampleur actuelle de la production et de la mise à disposition des informations exigent des méthodes de traitement qui vont au-delà des méthodes statistiques traditionnelles même si parfois on a tendance à complexifier inutilement les approches. La connaissance de ces méthodes, de leur potentiel et, surtout, de leurs limites, requiert des compétences spécifiques.

Il existe généralement quatre caractéristiques qui doivent faire partie d'un ensemble de données pour le qualifier de Big Data : le volume, la vélocité, la variété et la véracité.

Volume : Nos économies créent chaque jour 2,4 trillions de gigabits de données. La croissance du volume de données entraine une augmentation des besoins en systèmes de gestion de bases de données mais aussi en personnel TI

Vélocité : Aujourd'hui, la rapidité avec laquelle les données sont générées et traitées est toujours plus rapide et se fait en temps réel

Véracité : L'obsolescence rapide des données implique que les informations partagées ne sont pas toujours actuelles et les décisions qui en résultent peuvent alors ne plus être pertinentes

Variété : La diversité et les sources de provenance des données se multiplient de plus en plus rapidement

Sources : Intersystems; de Mauro et Al.; Aviseo Conseil 2021

C'est l'organisation des données et le manque d'expertise qui constituent le principal frein à la mise en valeur des données

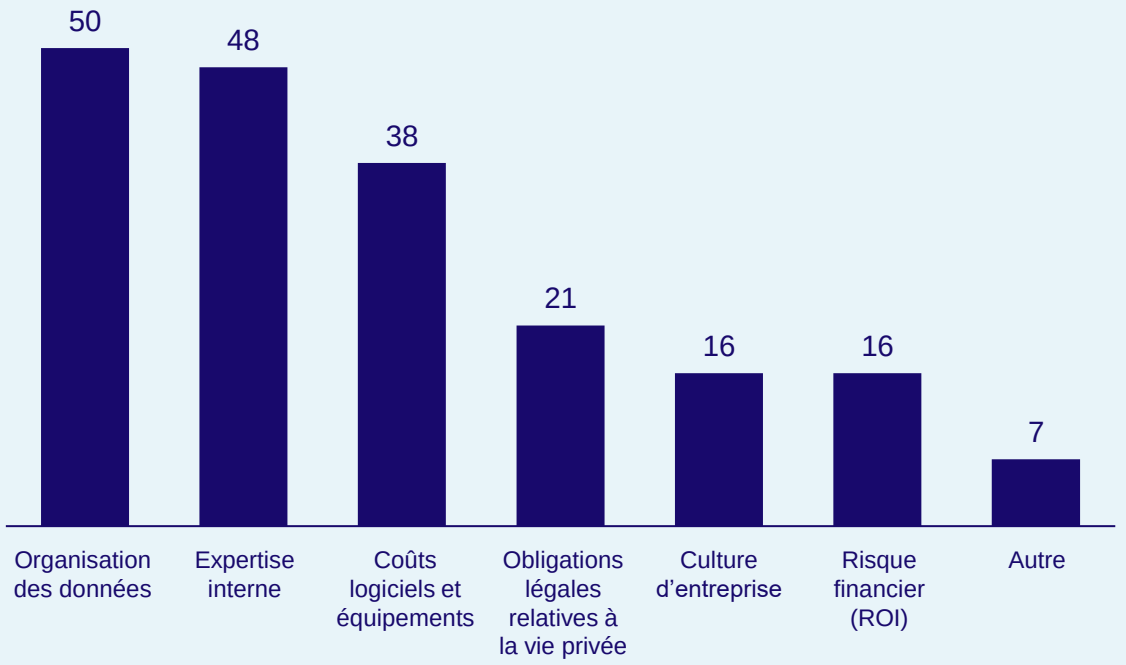
La moitié des entreprises ont fourni ces raisons quand venait le temps d'expliquer pourquoi elles ne mettaient pas en valeur leurs données.

L'exploitation et la gestion des données demeurent un enjeu de taille pour les entreprises au Québec. Cela demande un profil d'expertise qui implique précision et performance des processus tout en comprenant les besoins du client.

> « Les entreprises ne savent pas comment valoriser les données et surtout elles ignorent souvent si une donnée brute pourrait avoir de la valeur »
>
> — Membre inter-comité FCCQ

Principaux enjeux qui représentent un frein pour les entreprises au Québec, afin de tirer profit de la valorisation des données

Membres FCCQ; 2021, en pourcentage



Sources : Intercomité FCCQ le 5 octobre 2021; Sondage mené auprès des membres de la FCCQ du 31 août au 23 septembre 2021; Aviseo Conseil

La mise en valeur des données procure d'importants bénéfices

On peut identifier deux grands vecteurs stratégiques pour lesquels les données peuvent contribuer à générer de la valeur, soit l'analyse prédictive et l'accroissement des connaissances des clientèles

- Ces vecteurs contribueront en définitive à l'augmentation de l'efficacité
- Ils seront analysés dans les pages suivantes.

En dépit des quatre défis que posent les données massives (volume, vélocité, variété, véracité), on peut identifier de nombreux avantages positifs, en particulier sur la productivité et la profitabilité

- La recherche indique que les organisations s'appuyant sur la valorisation des données étaient 5 % plus productives et 6 % plus rentables que leurs concurrents. Certaines études avancent même des gains de rentabilité allant jusqu'à 22%
- En termes de secteurs, les banques et les assurances sont les plus avancées en matière de valorisation de leurs données.

5 %
Gains de productivité

6 % - 22 %
Gains de rentabilité

Sources : De Mauro 2015; Hilbert 2016; Intercomité FCCQ le 5 octobre 2021; Aviseo Conseil 2021

Valorisation des données

Les bénéfices

FCCQ
Fédération des chambres de commerce du Québec

L’analyse prédictive procure directement des gains aux entreprises

L’analyse prédictive vise à reconnaître des patterns dans les données pour obtenir la probabilité d’un événement. Elle s’appuie sur une collecte de données minimale alliée à des techniques statistiques, principalement l’analyse de régression

– Plus récemment, combinée à du data mining et parfois du machine learning, l’analyse prédictive est parvenue à considérer des facteurs d’influence dans un éventail beaucoup plus large qu’auparavant.

Bénéfices attendus de l’analyse prédictive

– Gain d’efficacité
– Hausse de productivité
– Qualité des services et de la production
– Diminution des accidents

Exemples de champs d’application de l’analyse prédictive

– Gestion de la non-conformité
– Amélioration de la sécurité
– Prévention de l’entretien
– Optimisation de chaîne de production
– Gestion des risques financiers

Une étude révélait que les entreprises du secteur de l’énergie ayant mis en place des programmes de maintenance prédictive ont réussi à éliminer pas moins de **75% des pannes** sur leurs équipements.

Sources : Roland Berger, Praxedo

Un manufacturier plus intelligent est un manufacturier plus productif

Le secteur manufacturier offre des gains majeurs quant à l'analyse prédictive :

1. Les **processus d'entretien** dans le manufacturier peuvent gagner en prévisibilité. Une entreprise peut mettre en place un système qui détecte à l'avance les besoins de remplacement des équipements, avant même qu'ils ne brisent.

2. Il est possible d'utiliser les données pour mieux **prévoir des événements de non-conformité** dans les chaînes de production. De telles analyses réduisent les erreurs et le nombre de produits défectueux avant même que le consommateur ou le partenaire y soit exposé.

3. La valorisation des données permet aussi de **mieux planifier les ressources** qui servent d'intrant à la production. Il est dès lors possible de prévoir des ruptures d'inventaire ou des soubresauts de la production.

4. Des indicateurs relatifs à la **santé et sécurité** peuvent permettre de mieux anticiper des blessures, des incidents ou l'absence d'employés. Une telle approche contribue à établir un environnement plus sécuritaire.

Outre le manufacturier, plusieurs autres secteurs peuvent profiter de l’analyse prédictive

La finance

Les institutions financières peuvent prévenir les défauts de paiement, prévoir des tendances financières, maximiser les opportunités de ventes et développer des évaluations du risque.

Le commerce de détail

L’industrie du détail peut utiliser l’analyse prédictive pour prévoir la demande, planifier de manière proactive les approvisionnements et prédire le comportement de certaines clientèles.

La santé

L’analyse prédictive peut être un intrant à la santé personnalisée, améliorer les décisions médicales, mieux prévoir la réaction des patients à un traitement et aider à détecter plus rapidement des maladies.

L’assurance

Ce secteur souffre des fausses déclarations. L’analyse prédictive permet de détecter de potentielles fraudes sans investir lourdement dans des vérifications. Également, la valorisation des données permet aussi d’optimiser le cycle de vie du développement des produits.

L’énergie et les ressources naturelles

Le recours à l’analyse prédictive, à l’instar du manufacturier, peut permettre au secteur de diminuer les bris d’équipements et les interruptions de service. Il serait également possible de signaler à l’avance lorsqu’un client risque de faire face à une facturation irrégulière en raison de sa consommation ou d’anticiper les périodes de pointe

La valorisation des données offre une plus grande efficacité pour les organisations dans une optique de relation client

Efficacité commerciale

- Génération de contenu axé sur les données clients
- Ciblage plus fin des produits et services à offrir à chaque client
- Développement des recommandations (en lien avec le NPS)
- Tarification individualisée

MAXIMISATION DES REVENUS

Efficacité opérationnelle

- Diminution des coûts d'acquisition et de fidélisation des clients
- Automatisation des processus internes (marketing, développement de produits/services)
- Meilleur arrimage entre le marketing et les ventes
- Performance et taux de conversion des campagnes marketing

RÉDUCTION DES COÛTS

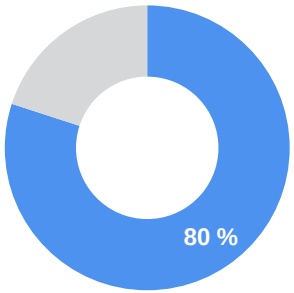
Efficacité relationnelle

- Parcours clients axés sur le moment présent et dans une logique de cycle de vie
- Développement d'une expérience de marque cohérente, personnalisée et mémorable sur tous les supports ou à travers tous les canaux
- Segmentation de la clientèle en temps réel

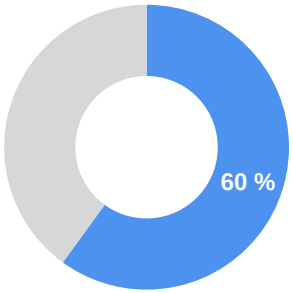
REHAUSSEMENT DE L'EXPÉRIENCE CLIENT

Sources : Personnaliser l'expérience client au moyen des données, de l'analytique et de l'IA, Deloitte, 2021; Analyse Aviseo

En autorisant la collecte et l'utilisation de leurs données, les clients attendent des gains significatifs en termes d'expérience



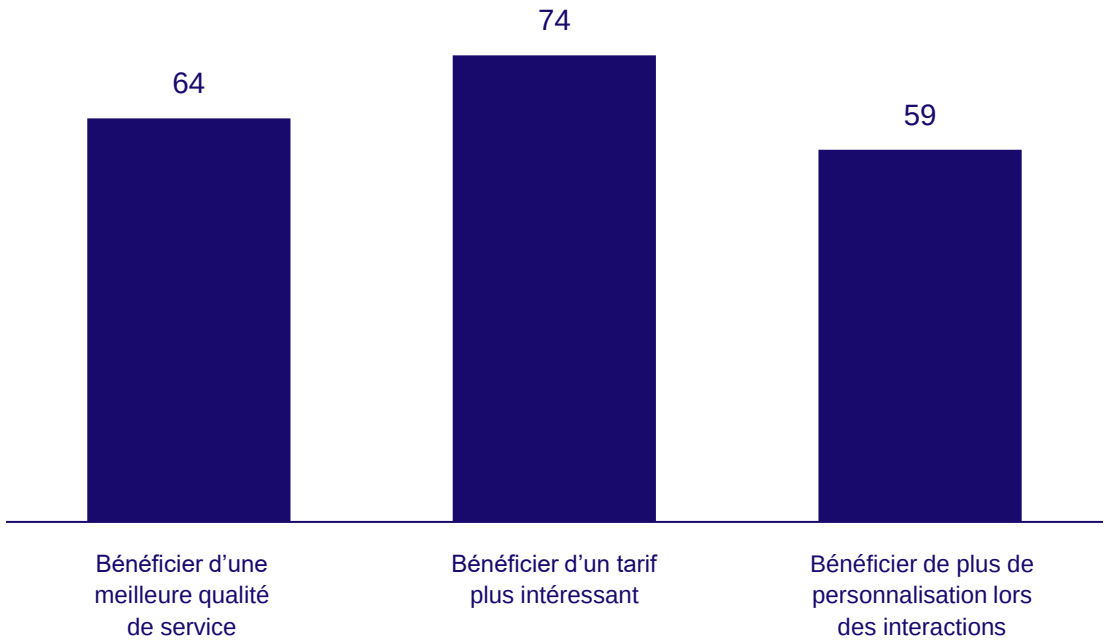
80 % des clients sont plus susceptibles d'acheter des produits ou services d'une organisation qui offre des **expériences personnalisées**



60 % des entreprises estiment qu'au cours des 3 prochaines années, **l'expérience client personnalisée sera la principale source de différenciation** vis-à-vis de la compétition

Attentes exprimées par les clients en échange de la collecte et de l'exploitation de leurs données personnelles

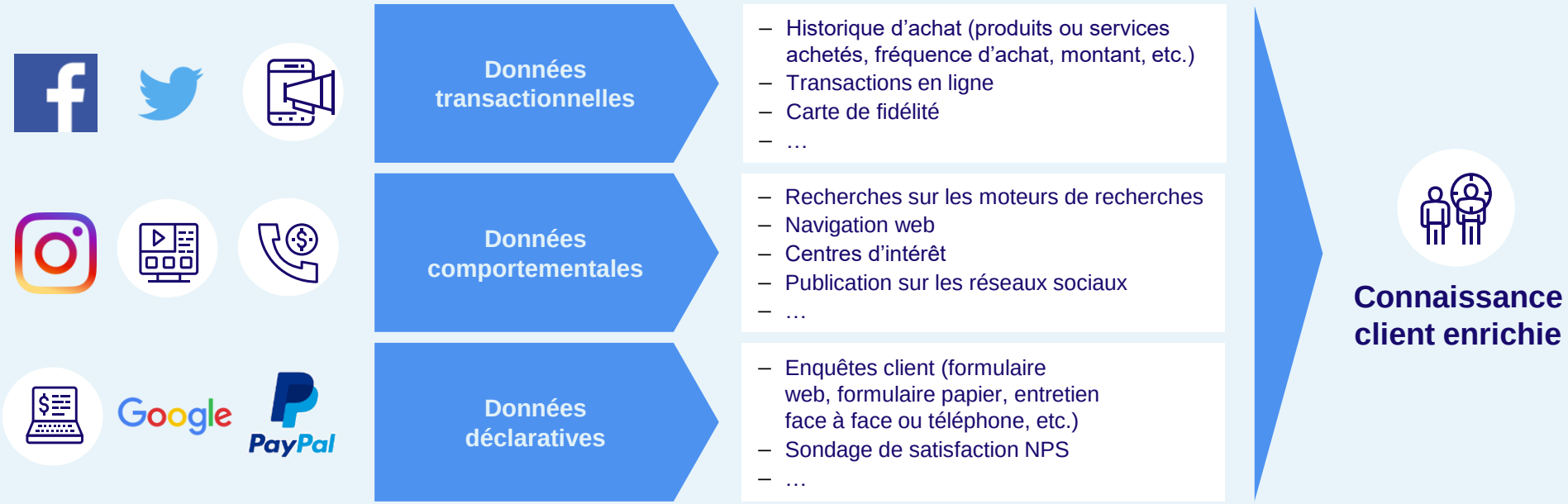
France; 2020, en pourcentage



Sources : Personnaliser l'expérience client au moyen des données, de l'analytique et de l'IA, Deloitte, 2021; Analyse Aviseo

Différentes catégories de données peuvent enrichir la connaissance des clients et à contribuer à personnaliser leur expérience

La multiplication des interactions via différents canaux ou points de contact permet d'avoir une connaissance client enrichie et variée par la collecte de différents types de données, soutenant le rehaussement et la personnalisation de l'expérience client



Sources : Ailancy; Aviseo Conseil 2021

L’exploitation des données soutient activement la personnalisation de la relation client à travers une approche marketing sur-mesure

Bénéfices marketing visés	Exemples de déclinaison et de gains attendus
Marketing prédictif	– Identification des tendances d’achat et de consommation des clients – Veille et pilotage de l’e-réputation – Compréhension et anticipation de comportements et de parcours clients complexes – Innovation de produits et services
Analytique web avancée	– Optimisation de la création de trafic – Personnalisation des messages publicitaires – Optimisation des parcours clients web
Marketing relationnel omnicanal	– Connaissance du client (attentes, priorités, comportements) – Aide au choix des canaux les plus performants par individu – Segmentation & ciblage plus fins des clients (les plus rentables, les plus à risque…) – Recommandation personnalisée de produits et services – Optimisation des parcours clients dans une logique cross canal – Personnalisation de la navigation et des contenus après identification – Tarification personnalisée

Sources :Data Management; Aviseo Conseil 2021

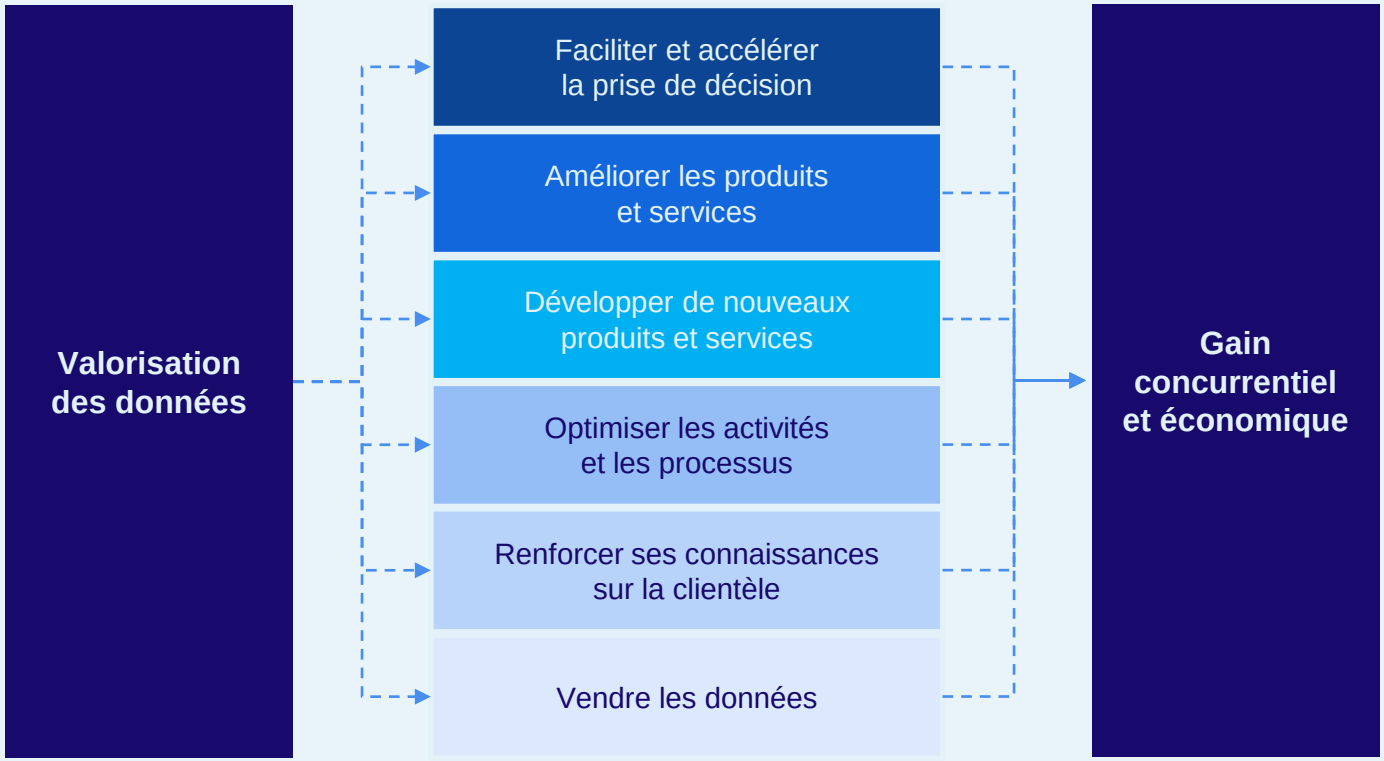
La transposition des données collectées et exploitées en parcours client renforce la proposition de valeur des organisations

Secteur d'activité	Exemples de parcours client bonifié par la donnée		
Banque, assurance, sociétés de gestion	**Recherche de produits financiers** La donnée, combinée à l'intelligence artificielle, permet aux entreprises de s'assurer que le contenu est adapté au client, qui peut trouver plus facilement l'information qu'il recherche	**Obtenir un conseil financier** Grâce à l'analytique en temps réel et à l'information recueillie sur la clientèle, les conseillers savent exactement ce dont les clients ont besoin	**Disposer d'une offre personnalisée** Les données détaillées sur les clients permettent d'adapter les offres financières pour des clients spécifiques, ce qui réduit le risque et améliore l'expérience
Commerce de détail	**Disposer d'offres ciblées** Grâce aux programmes de fidélité, à l'identification des clients, à une meilleure compréhension de leurs besoins, les organisations sont en mesure de faire des offres ciblée	**Personnaliser le contenu web** Les entreprises sont en mesure de personnaliser leurs recommandations de produit et les renseignements fournis en modifiant le contenu de leur site web en fonction du profil du client	**Proposer une tarification personnalisée** En connaissant la disposition du client à dépenser et ses facteurs de motivation, l'organisation peut utiliser la tarification dynamique et accroître la probabilité de conversion.

Sources : Personnaliser l'expérience client au moyen des données, de l'analytique et de l'IA, Deloitte, 2021

La finalité de la valorisation des données est d'en tirer un avantage concurrentiel

Les objectifs peuvent varier selon chaque organisation, outre ces gains en efficacité. Si la facilitation et l'accélération de la prise de décision sont plus évidents quant à un potentiel objectif (naturel pourrait-on même affirmer) de la valorisation des données, d'autres peuvent être plus complexes, notamment lorsqu'on a l'intention de vendre ces données.



Valorisation des données

Répondre aux enjeux

FCCQ
Fédération des chambres de commerce du Québec

Les coûts et le manque d'expertise sont les plus grands enjeux des entreprises au Québec pour se conformer à leurs obligations légales

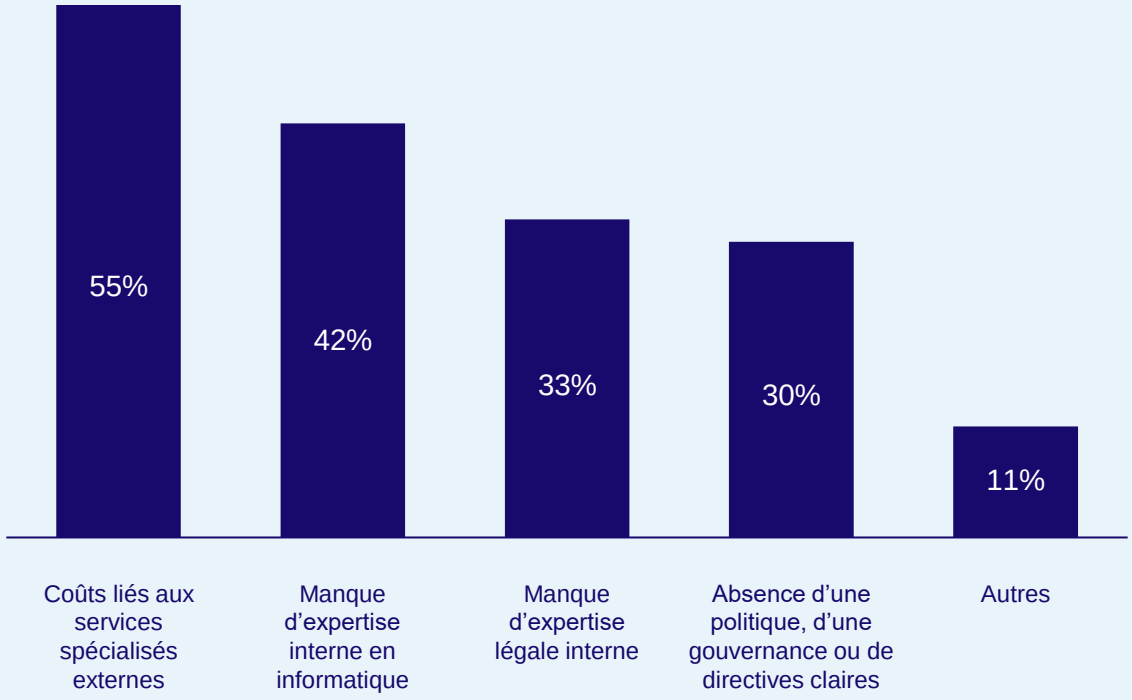
Pour répondre aux obligations légales et morales qui entourent l'exploitation des données, les entreprises au Québec font face à plusieurs enjeux. Ce sont 55 % d'entre elles qui déclarent que les coûts liés aux services externes représentent leur principal défi, en réponse au manque d'expertise interne en informatique.

« Face au dilemme entre le partage et la protection des données, une fiducie de données pourrait constituer un instrument qui aurait la responsabilité de gérer les paramètres des données sous son égide et en assurer la sécurité en répondant aux objectifs éthiques et moraux »

— Membre inter-comité FCCQ

Principaux enjeux pour les entreprises au Québec relatifs à leurs obligations légales quant à la protection des données

Membres FCCQ; 2021, en pourcentage



Sources : Sondage FCCQ; Intercomité FCCQ le 5 octobre 2021; Aviseo 2021

RÉPONDRE AUX ENJEUX

La fiducie de données, un modèle de partage de données qui offre un équilibre entre la juste valorisation et la protection des données et de la vie personnelle

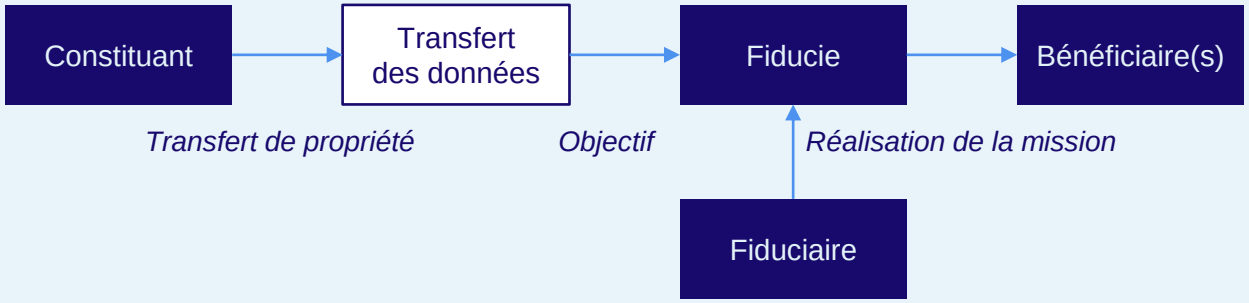
Une fiducie constitue un moyen juridique de gérer les droits relatifs à un « objet » au profit d'une autre personne. Elle peut constituer un véhicule pour mettre en commun des données

– Il s'agit d'une approche qui permet aussi de se distancer des grands joueurs technologiques et, parfois, de leur attitude monopolistique.

Selon l'Open Data Institute, une fiducie de données doit disposer d'un objectif clair; d'une structure juridique et d'une constitution légale. Ses fiduciaires doivent détenir certains droits et obligations sur les données gérées, être régis par une gouvernance et des processus décisionnels bien définis. Son application doit prévoir un mode de répartition des bénéfices et pouvoir miser sur un financement durable.

– La fiducie de données a l'avantage de pouvoir impliquer tous les acteurs (entreprises, ONG, gouvernements, institutions, experts)

– Le bénéficiaire peut être une personne, un groupe de personnes ou une personne qui doit être identifiable. Le constituant nomme une organisation ou un individu fiduciaire chargé de gérer les données dans l'intérêt des bénéficiaires.



Sources : Element AI, Open Data Institute, Laboratoire de cyberjustice

Il est fondamental de pouvoir judicieusement interpréter les données

Il ne suffit pas aux entreprises de collecter les données et d'investir dans l'intelligence artificielle. Les organisations se trouvent souvent face au dilemme d'analyser leurs données et d'en communiquer les « résultats » sans perdre la valeur ajoutée créée et donc leur positionnement

– Selon une étude, seulement 18% des entreprises aux États-Unis pensent qu'elles sont capables de le faire efficacement.

En raison de cette réalité, certaines organisations ont choisi d'ajouter un traducteur de données (data translator) pour aider à combler l'écart entre les possibilités offertes par les technologiques et les impératifs d'affaires

Un traducteur de données est une personne qui peut combler le fossé d'expertise entre les équipes techniques, composées de scientifiques des données, d'ingénieurs de données et de développeurs de logiciels, et les parties prenantes de l'entreprise.

« Les données ne sont pas bien gérées. Il faut les rendre accessibles. On ne les exploite pas de manière efficace.

Il y a un fossé entre le besoin d'affaire, les algorithmes d'intelligence artificielle et les experts. Cela nécessite précision et rapidité des processus tout en comprenant le besoin client.

Le *data translator* est un métier qu'on va voir émerger. Il dispose d'un profil en affaire et en informatique. »

— Membre inter-comité FCCQ

Sources : Hilbert 2016; Intercomité FCCQ le 5 octobre 2021; Aviseo Conseil 2021

L'anonymisation des données est une réponse efficace à donner aux enjeux fondamentaux de la sécurité et du respect de la vie privée

Il existe plusieurs techniques dont la « k-anonimity » pour généraliser ou supprimer certaines données ou catégories de données afin de rendre l'identification plus difficile.

Le contenu du tableau à gauche rend une identification plus facile, ce qui pose des problèmes à l'utilisation de ces données. La suppression de la catégorie « nom de famille » et la généralisation des données de la catégorie « revenu annuel » rendent une identification beaucoup plus difficile tout en permettant une utilisation qu'elle soit commerciale ou d'origine institutionnelle.

Nom de famille	Revenu annuel	État marital	Sexe	Ville
Tremblay	**87 500 $**	Marié	Femme	Saguenay
Gagnon	**23 900 $**	Célibataire	Homme	Val d'or

Nom de famille	Revenu annuel	État marital	Sexe	Ville
***	**75 000 à 100 000 $**	Marié	Femme	Saguenay
***	**0 à 24 999 $**	Célibataire	Homme	Val-d'Or

« Il y a un travail d'acceptabilité sociale de la part des institutions publiques : il faut trouver le bon équilibre entre le partage, l'utilisation et la confidentialité des données. Le gouvernement a un leadership à prendre sur le partage de données. Le Québec est en retard par rapport aux autres provinces et pays »

— Membre inter-comité FCCQ

« Il faut qu'il y ait plus d'éducation et de transparence sur ce qu'on fait avec les données du consommateur »

— Membre inter-comité FCCQ

Sources : Intercomité FCCQ le 5 octobre 2021; Jain 2016; Aviseo Conseil 2021

La mise en place d'une expertise dédiée à la sécurité informatique représente une opportunité pour les entreprises du Québec

Avec l'émergence de risques technologiques toujours plus sophistiqués, les organisations créent de plus en plus de fonction dédiée, soutenue par des profils certifiés de type CISO (Chief information security officer).

Un tel expert est responsable de plusieurs domaines d'activités, directement corrélés aux enjeux et défis en matière de cybersécurité :

- **Sécurité opérationnelle** : Il analyse en temps réel des menaces et priorisation en cas de problème
- **Prévention des violations de données et de la fraude** : Il s'assure que le personnel interne ne fait aucune mauvaise utilisation ni ne vole des données de l'entreprise
- **Architecture de sécurité** : Il planifie, achète et déploie du matériel et des logiciels de sécurité. Il s'assure également que l'infrastructure informatique et réseau est conçue sur la base des meilleures pratiques de sécurité
- **Gestion des identités et des accès** : Il s'assure que seules les personnes autorisées ont accès aux données et aux systèmes protégés
- **Gestion de projet et de programme** : Il met en œuvre des programmes ou des projets réduisant les risques technologiques
- **Enquêtes et expertises légales** : Il détermine ce qui s'est mal passé et identifie les mesures à prendre pour éviter la répétition d'une crise identique
- **Gouvernance** : Il s'assure que toutes les initiatives ci-dessus se déroulent sans heurts et qu'elles reçoivent le financement et les ressources dont elles ont besoin. Il s'assure également que les dirigeants de l'entreprise comprennent bien leur rôle et leur importance dans la sécurité

Sources : How does security evolve from bolted on to built-in, 2020, EY; Analyse Aviseo 2021

SECTION 3

PRATIQUES INSPIRANTES
En matière de cybermenaces et de valorisation des données

Des applications dans le domaine de l'hébergement

Red Roof Inn

Red Roof Inn a utilisé des données publiques (open source) pour prédire les vols qui seraient annulés en raison de la mauvaise température à l'hiver 2013-2014.

En anticipant de nombre de personnes qui seraient à la recherche d'un hôtel de dernière minute, la compagnie a été en mesure de mettre en œuvre des initiatives publicitaires ciblées aux utilisateurs de téléphones intelligents dans les régions géographiques les plus susceptibles d'être affectées.

Cette stratégie basée sur des données publiques a permis à Red Roof Inn d'augmenter son chiffre d'affaires de 10 % pendant cette période.

Denihan Hospitality Group

Denihan et IBM ont collaboré afin de créer une plateforme d'analyse d'intelligence économique et analytique.

La compagnie reconnaît l'importance de la tarification et de l'optimisation des revenus afin d'offrir le bon produit au bon client, et ce, à un prix et un moment qui lui conviendra.

Grâce à une combinaison de données provenant de l'externe (ex: sites Internet, blog, etc) et de données internes (ex: sondage de satisfaction, plaintes, etc), Denihan a été capable d'optimiser ses processus et son offre, ce qui a eu comme impacts d'augmenter le revenu, d'améliorer la gestion des dépenses et d'offrir une direction claire dans la planification stratégique de l'entreprise.

Sources : Cobanoglu et al. (2021)

Mesurer et prédire : des besoins pour les entreprises

Mesurer l'impact des dépenses publicitaires

Les données détenues par cinq entreprises (Nigeria Bottling Company Lagos, UAC Lagos, PZ Lagos, May & Baker Lagos et Unilever Group Lagos) ont été analysées pour isoler l'impact des dépenses publicitaires sur le profit de chacune des entreprises.

L'analyse des données a également permis de mettre en exergue une relation significative entre l'inventaire et la profitabilité de l'entreprise.

L'étude révèle non seulement que le lien est significatif, mais elle quantifie la relation, ce qui permet aux dirigeants d'optimiser les stratégies publicitaires ainsi que le profit attendu en fonction des dépenses engagées.

Prédire le nombre de clients dans une chaîne de restaurant

Cinq succursales de la chaîne de restauration K au Japon ont mis leurs données ensemble pour construire un modèle qui prédirait le nombre de clients attendus à chaque journée. Les variables, qui incluent notamment le jour de la semaine, les jours fériés, la saison, les évènements susceptibles de survenir et la météo, ont alimenté un modèle d'apprentissage machine qui prédit avec un taux de précision d'environ 85%.

Les restaurants participants continuent à améliorer la précision du modèle et à utiliser les résultats pour augmenter l'efficacité de la gestion de chaque restaurant. Par exemple, cela pourrait prendre la forme d'horaires de travail modifiés ou de commandes d'ingrédients ou d'aliments basées sur les prédictions du modèle.

Sources : Agbeja et al. (2015); Tanizaki et al. (2019)

Les données au cœur du modèle d'affaires de géants comme Netflix et Amazon

Netflix

En 2006, Netflix a annoncé le Prix Netflix, une compétition d'apprentissage machine et de minage de données pour améliorer la prédiction des notes d'évaluation des films octroyées par ses usagés.

Netflix a offert 1 million $US à ceux qui seraient en mesure d'augmenter l'efficacité de leur système existant (Cinematch) de 10%. À mi-chemin de la compétition, une équipe avait déjà amélioré les résultats de 8,43%. À la fin de la compétition, grâce à une combinaison de multiples algorithmes, le modèle de prédiction des notes d'évaluation avait augmenté de 33% par rapport au modèle de base.

De plus, étant donné que l'objectif est de personnaliser l'expérience pour les utilisateurs, plusieurs nouvelles composantes ont été rajoutées au modèle (outre les notes d'évaluation et la popularité), ce qui a amélioré la performance du modèle de 261% par rapport au modèle de base.

En définitive, cela a permis à Netflix d'améliorer l'expérience client et de faire croître la valeur de l'entreprise.

Amazon

À chaque fois qu'un utilisateur accède au site Internet d'Amazon, une multitude de données est collectée incluant le contenu de ses recherches, les pages à laquelles il a accédé, le temps passé sur chacune d'entre elles, les produits ajoutés ou retirés du panier d'achats, l'adresse IP de l'utilisateur, etc.

Ces données permettent à la compagnie de prédire en amont les produits qui pourraient intéresser le client et son système de recommandations personnalisées serait responsable d'environ 35% des ventes annuelles d'Amazon.

En outre grâce aux données massives accumulées, la compagnie est en mesure de réduire ses coûts de transport de 10 à 40%, notamment en choisissant l'entrepôt le plus proche du consommateur, minimisant les coûts.

Sources : Amatrian (2013); Prescott (2014); SupplyChainDigital.com

L’importance des données secondaires : une source d’informations fréquemment négligée

Des parcours de soins pour les patients atteints du cancer de la prostate

Une multitude de données médicales sont disponibles, mais elles sont souvent complexes et hétérogènes. Elles ont aussi tendance à ne pas être centralisées et à être plutôt éparpillées au sein de plusieurs banques de données.

Un projet de recherche réalisé en Angleterre a permis de mettre en place de meilleurs parcours de soins pour 1904 patients atteints du cancer de la prostate.

Une nouvelle voie de recherche dans la lutte contre le cancer de la prostate

Les nouveaux parcours de soins ont aussi été analysés en fonction des biomarqueurs du cancer de la prostate. Les résultats de l’étude démontrent que ces parcours contiennent suffisamment d’information sur les biomarqueurs pour être d’intérêt significatif pour la recherche clinique en oncologie.

La recherche conduite par Bettencourt-Silva et al. (2015) démontre que les données collectées de façon routinière dans le réseau de la santé peuvent être transformées et préparées afin d’être utilisées dans des recherches cliniques et pour améliorer les processus de décision et le mécanisme de support décisionnel.

Sources : Bettencourt-Silva et al. (2015)

La mise en commun des données: une pratique qui revêt un fort potentiel, mais qui ne doit pas nuire à la compétition

Des facteurs de succès

La mise en commun des données pourrait favoriser l'augmentation de l'efficacité, permettre une plus grande personnalisation des services ou des biens offerts ou encore contribuer à l'innovation.

Cependant, la mise en commun des données peut aussi induire une augmentation du pouvoir de marché, réduire la compétition et, dans certains cas, être en violation de la *Loi sur la concurrence*.

Il est néanmoins suggéré que la mise en commun des données devrait être encouragée parce que :

1) Elle contribue à créer de nouvelles formes de produits et de services
2) Elle peut grandement augmenter l'efficacité des chaînes de valeurs
3) Elle pourrait s'avérer un outil particulièrement important pour le maintien de la compétitivité des petites et moyennes entreprises dans un contexte où les grandes entreprises bénéficient de beaucoup de données. Cela freinerait la création de monopoles, au bénéfice des consommateurs.

Asnef-Equifax

Afin d'améliorer l'évaluation des risques de crédits et d'améliorer leurs activités de prêts ou de crédit, des banques espagnoles et des institutions financières ont mis en commun leurs données. L'ensemble des données était organisé et administré par Asnef-Equifax.

Bien que l'objectif de l'initiative était d'augmenter l'efficacité, le partage d'informations entre les différentes organisations a mené à des poursuites judiciaires en raison de craintes à l'égard de pratiques anticoncurrentielles.

La Cour s'est montrée généralement favorable au système de mise en commun des données, bien qu'une analyse au cas par cas soit toujours nécessaire.

Les lignes directrices formulées par l'Union européenne dérivée du cas d'Asnef-Equifax et d'autres cas similaires comme *John Deere* et *Wood Pulp* mentionnent que l'échange d'information entre les compétiteurs ne crée pas une présomption de violation des lois antitrust (article 101(1) TFEU).

Sources : Lundqvist (2018)

Un soutien spécifique apporté aux citoyens, aux organisations et aux secteurs vitaux pour endiguer les cybermenaces

Une plateforme de signalement face aux risques technologiques et aux cybermenaces proposées par le gouvernement français

Créée en 2016, la plateforme de signalement « PHAROS » (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) permet aux citoyens français de signaler en ligne les contenus et comportements illicites constatés sur internet, dont les cyberattaques.

Des policiers et gendarmes affectés à la plateforme PHAROS vérifient que les contenus et comportements signalés constituent bien une infraction à la loi française. Leur mission est de les traiter et d'alerter les services compétents tels la Police nationale, la Gendarmerie nationale, les Douanes, la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes en France et à l'étranger (en passant par Interpol), déclenchant au besoin une enquête sous l'autorité du Procureur de la République.

Une protection accrue face aux cybermenaces pour les secteurs vitaux de la Belgique

Soucieux de protéger ses citoyens et ses organisations, l'État belge met à leur disposition un ensemble d'outils de sensibilisation et d'éducation face aux risques technologiques et aux cyberattaques par le biais de son Centre pour la Cybersécurité Belgique (CBB).

Ce dernier a lancé plusieurs projets destinés à renforcer la cybersécurité des secteurs vitaux en Belgique. Il s'agit des secteurs jugés cruciaux pour assurer la sécurité de la population belge, à savoir les secteurs de l'énergie, de la mobilité, des télécommunications et des finances, l'accès à l'eau potable, la santé publique et les pouvoirs publics.

Afin d'alerter de manière rapide et standardisée les secteurs vitaux en Belgique quant aux nouvelles cybermenaces et nouvelles attaques, le CCB a mis en place un Early Warning System.

Les secteurs vitaux ont accès à des alertes filtrées concernant des intrusions ou d'autres cybermenaces via une plateforme partagée. Ils reçoivent ainsi rapidement des informations de la part d'une source fiable et sont en mesure de prendre des mesures tout aussi rapidement.

Sources : Centre pour la Cybersécurité Belgique; Ministère de l'Intérieur, France; Analyse Avise 2021

L’exploitation des données massives permet d’améliorer les services offerts par les organisations publiques

Les consommateurs sont habitués à des produits et à des services commerciaux personnalisés et sur demande. Ils souhaiteraient des services publics tout aussi intelligents, proactifs et personnalisés.

PRESTATION DE SERVICES	
Flux financiers	Les techniques de Big Data transforment les processus pour détecter la fraude, la collusion et le blanchiment d'argent par l'analyse des marchés publics et des informations financières.
Santé	Les données sont utilisées pour le suivi et l'amélioration des services de santé, les opérations de gestion hospitalière, l'assurance et les traitements.
Éducation	Les données peuvent être utilisées de manière innovante pour suivre les élèves, mieux comprendre les pratiques d'enseignement, compléter les sources traditionnelles pour permettre de nouvelles méthodes d'enseignement en suivant les progrès vers les objectifs gouvernementaux et mondiaux.
Administration terrestre	L’imagerie haute résolution provenant de satellites et de drones peut offrir des capacités pour révolutionner les méthodes d'arpentage. L'enregistrement foncier améliore les recettes publiques en augmentant la perception des impôts, des revendications concurrentes sur les frontières des droits de propriété.
Sécurité publique	Des informations de base comme le type et la localisation des crimes peuvent aider les agents à prendre des décisions plus avisées lors de leurs patrouilles. Les forces de l'ordre utilisent également le Big Data, par le biais d'entreprises d'analyse des médias sociaux pour être plus efficaces dans leurs campagnes de sensibilisation du public.

Sources : World Bank Group; EY; Aviseo Conseil 2021

Les données peuvent améliorer l'élaboration de politiques publiques pour les rendre plus robustes et plus pertinentes

Traditionnellement, l'élaboration des politiques publiques est basée sur des rapports qui sont largement informés par des enquêtes traditionnelles et des données et des statistiques administratives. Le Big Data peut potentiellement fournir des informations sur les politiques sur une base plus fréquente et plus rentable.

ÉLABORATION DE POLITIQUES	
Transport et planification urbaine	La télédétection, les données des téléphones portables et l'apprentissage automatique peuvent fournir aux décideurs et aux planificateurs une meilleure compréhension de la mobilité urbaine. Les responsables politiques peuvent utiliser ces informations pour rendre les villes plus durables, inclusives, productives et vivables.
Statistiques officielles	Dans de nombreux pays, les données de recensement sont incomplètes et périmées. Le Big Data et l'apprentissage automatique peuvent être utilisés pour créer des approximations statistiques viables pour le suivi et les décisions politiques.
Sécurité alimentaire	Les outils de Big Data permettent l'analyse sophistiquée des données météorologiques et des données satellites pour raffiner les stratégies de culture et formuler des politiques agricoles optimales.
Service de l'emploi	Les agences pour l'emploi utilisent le Big Data pour déterminer les politiques les plus appropriées pour aider les individus à retourner au travail, par exemple en adaptant les services de formation à différents segments de demandeurs d'emploi.
Politique environnementale	L'analyse de données environnementales et climatiques provenant de sources multiples permet aux autorités de comprendre les impacts environnementaux. Les phénomènes météorologiques extrêmes tels que les inondations, tempêtes et incendies de forêt sont devenus plus fréquents ces dernières années. De nombreux instituts météorologiques partagent ouvertement leurs données pour aider à suivre les changements du temps et du climat.

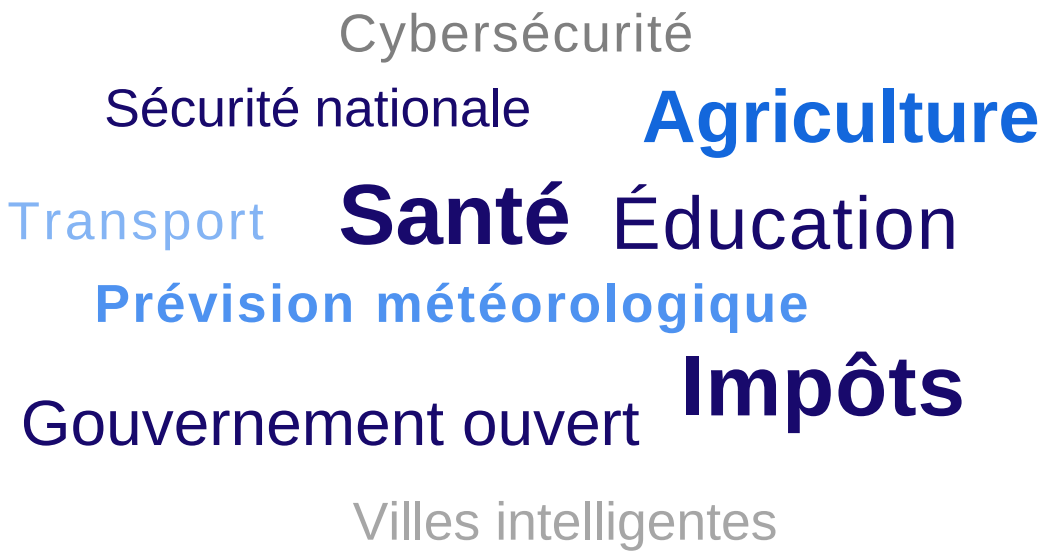
FCCQ

Sources : World Bank Group; EY; Aviseo Conseil 2021

Le *Big Data* a un énorme potentiel dans tous les secteurs d'interventions du domaine public

Les activités quotidiennes d'un gouvernement, telles que la gestion des prestations sociales, la collecte des impôts, la surveillance des systèmes nationaux de santé et d'éducation, l'enregistrement des données de circulation et la publication de documents officiels génèrent et sont source d'importantes quantités de données.

Ces informations facilement disponibles en temps réel permettent aux différentes organisations d'identifier les domaines nécessitant une attention particulière, de prendre des décisions plus éclairées plus rapidement et de mettre en œuvre les changements nécessaires.



Opportunités pour le Gouvernement du Québec en terme d'une meilleure valorisation des données en santé

Accélérer l'innovation

– Permettre aux entreprises de développer des traitements plus efficaces, notamment par la médecine de précision avec un recrutement plus efficace dans les essais cliniques et en accélérant toutes les étapes de la R&D

Développer une culture de la donnée

– Abandonner l'actuelle approche de silo et permettre un meilleur accès aux données entre organisations et secteurs
– Adopter une approche de gestion des risques dans la conformité des programmes gouvernementaux à l'aide de l'intelligence artificielle

Effectuer une meilleure évaluation de la performance des innovations

– Améliorer l'évaluation des impacts des innovations en santé et assurer une meilleure intégration dans le réseau

Optimiser l'utilisation du médicament

– Accélérer la médecine personnalisée dans le but de donner le bon traitement, au bon patient, au bon moment
– Faciliter des analyses des données en milieux réels de soins aux fins de recherche et d'évaluation des médicaments, des traitements et des technologies

Assurer une gestion plus efficace du réseau de la santé

– Quantifier le coût des trajectoires de soins et assurer leur efficience
– Permettre au réseau de la santé de mieux planifier le déploiement des ressources
– Permettre aux patients d'accéder aux soins en temps opportun

Améliorer la pratique médicale

– Développer des systèmes basés sur l'intelligence artificielle qui pourront appuyer les professionnels de la santé dans le diagnostic, le traitement et le suivi

FCCQ

Source : Recommandations du Groupe de travail sur les données et du Comité Sciences de la vie de la FCCQ , septembre 2021

Les États-Unis et le Royaume-Uni ont recours à l'utilisation des données pour contrer l'évasion fiscale

États-Unis

Le Big Data joue un rôle important dans la lutte contre la fraude fiscale. L'exploitation de données s'est avérée être l'une des stratégies les plus efficaces dans plusieurs pays, dont les États-Unis.

Il y a quelques années, l'Internal Revenue Service des États-Unis a révélé qu'il utilisait les données massives pour freiner les fraudeurs fiscaux. Parmi les stratégies employées, il y a l'exploration de données dans les médias sociaux pour identifier les individus qui mènent un style de vie plus opulent que ce que leurs déclarations d'impôts suggèrent comme étant plausible. L'Internal Revenue Service estime que l'exploitation des données des médias sociaux et d'autres stratégies de valorisation de données ont été essentielles pour réduire les 300 milliards de dollars d'impôts perdus chaque année.

Royaume-Uni

Les autorités fiscales britanniques ont également investi dans l'utilisation des données massives pour améliorer l'efficience de leur lutte contre l'évasion fiscale. Les autorités recueillent des données sur les citoyens afin de générer des analyses prédictives pour de meilleurs audits. Les autorités fiscales ont augmenté la quantité de données que Her Majesty Revenue and Custom (HMRC) peut détenir et analyser, en étendant le droit légal de collecter des données auprès des fournisseurs de services marchands et des agrégateurs de données, y compris à l'étranger. Cette étape est cruciale car de nombreux stratagèmes d'évasion fiscale utilisent des entreprises basées à l'étranger.

Ces contrevenants à l'évasion fiscale sont identifiés comme des individus à haut risque pendant une certaine période après avoir été condamnés, et font l'objet de surveillance pour éviter qu'ils ne répètent le même crime.

Sources : smartdatacollective, Govinsider, Aviseo Conseil 2021

L’Australie et Singapour utilisent les données massives pour améliorer le contrôle des coûts et la pertinence des soins de santé

Australie

En Australie, le financement des soins de santé pour une population de 22 millions d'habitants est assuré en grande partie par le gouvernement. Afin d’identifier des coûts de santé par épisode de soins anormalement élevés, le gouvernement a développé des modèles prédictifs (le système I+Plus) qui permettent d’anticiper les coûts hospitaliers, médicaux et prothétiques ainsi que la durée du séjour à l'hôpital pour chaque admission. I+Plus met en lumière les coûts d’admissions anormaux, tels des frais d'hospitalisation plus élevés que prévus. Il identifie également les cas de surconsommation de services, par exemple lorsque le nombre de tests de pathologie ou de services d'imagerie réalisés est sensiblement plus élevé que les chiffres relevés pour des admissions similaires pour le même traitement.

Singapour

Singapour a intensifié l’utilisation de l’intelligence artificielle dans les soins de santé pour l'analyse de données génomiques. La génomique constitue la base de nombreux tests de diagnostic pour prédire la probabilité de souffrir d'une maladie.

Des chercheurs de Singapour utilisent des algorithmes pour comprendre l'importance d'une variation génétique donnée, regrouper des échantillons ayant des profils moléculaires similaires et prédire comment la variation génétique peut entraîner une maladie. L'apprentissage automatique peut également lier les données génomiques à d'autres types de données, telles que les données de capteurs portables et de tests sanguins et peut guider les décisions de traitement des médecins.

Sources : Srinivasan & Arunasalam (Leveraging Big Data Analytics to reduce healthcare costs), GovInsider, Aviseo Conseil 2021

Israël et le Danemark développent des technologies pour créer des solutions innovantes en matière de cybersécurité

Israël

Le gouvernement israélien a créé le programme d'incubateurs technologiques au début des années 1990. Aujourd'hui, il existe plus de 25 incubateurs à travers le pays, qui ont tous été privatisés. Les incubateurs offrent un financement gouvernemental allant jusqu'à 85% des coûts des projets en phase de démarrage. Israël investit environ 4,1 % de son PIB dans la R&D, la moyenne au sein de l'OCDE étant de 2,0 %.

La dynamique d'innovation se poursuit ; la société israélienne a produit quelque 300 start-ups de cybersécurité en 2015, contre 150 en 2012. Le secteur de la cybersécurité est particulièrement porteur. Les entreprises israéliennes de cybersécurité ont enregistré une croissance de 70 % de leur financement en 2020.

Danemark

La cybersécurité est un enjeu important et croissant. Le gouvernement danois l'a bien compris en allouant un budget de 740 M EUR dans le cadre de sa stratégie pour la « Croissance Numérique du Danemark jusqu'en 2025 », incluant un volet de cybersécurité des entreprises. Au cours des prochaines années, le Danemark prévoit d'investir au moins 202 millions d'euros dans sa cybersécurité et sa sécurité informatique. Selon la stratégie du gouvernement pour 2018-2021, sa politique repose sur une triade : augmenter la résilience technologique, améliorer les connaissances des citoyens et renforcer la coordination entre les différents acteurs.

Le gouvernement danois a également lancé la stratégie nationale pour l'intelligence artificielle en 2019, qui permettra aux entreprises d'utiliser l'IA pour obtenir un avantage concurrentiel et contribuera à promouvoir le Danemark en tant que leader de la technologie de l'IA.

Les opérateurs de centres de données obtiennent également des sources d'énergie renouvelables pour alimenter leurs installations et cette tendance devrait se poursuivre dans tout le Danemark au cours de la période de prévision.

Sources : Cigref

FCCQ
Fédération des chambres de commerce du Québec

SECTION 4

RECOMMANDATIONS: Pistes d’actions pour renforcer la cybersécurité et la valorisation les données

Les recommandations

Fédération des chambres de commerce du Québec

Le présent rapport propose des recommandations qui s’inspirent principalement des entretiens avec les experts rencontrés, des discussions avec les membres de la FCCQ lors de l’inter comité et des suggestions écrites dans le sondage auprès des membres de la FCCQ.

Elles s’adressent aux entreprises et à leur environnement d’affaires. C’est pourquoi les chambres de commerce et les gouvernements ont également un rôle.

Les entreprises et leur écosystème au cœur de la réponse à donner aux enjeux de cybersécurité

1 Continuer de sensibiliser et former les entreprises aux risques relatifs à la cybersécurité

- Les entreprises gagneront à mieux connaître les ressources existantes dans l'écosystème de la cybersécurité, telles que le CyberQuébec, le Centre canadien sur la cybersécurité, Cybereco, Promptinnov, etc.
- Les groupes universitaires devraient être davantage impliqués

2 Appliquer les pratiques exemplaires en matière de cybersécurité

- Le principe du droit d'accès minimal pour prévenir les accès non autorisés et la compromission de données
- La sauvegarde des données et des applications essentielles sur au moins un autre endroit protégé
- L'adoption de politiques d'authentification robustes
- Un plan d'intervention en cas d'incident

3 Former de manière continue les employés sur les risques relatifs à la cybersécurité

- Développer et offrir des programmes de sensibilisation et de formation aux employés pour améliorer les compétences afin de mieux se protéger des cyberattaques
- Assurer en continue ces formations en raison de l'évolution rapide de la nature des risques

4 Mettre en place une fonction dédiée à la cybersécurité

- Encourager la création d'une expertise TI spécialisée dans les risques technologiques
- Disposer de ressources certifiées CISO, rehaussant l'approche en prévention, détection et traitement des cyberattaques
- Centraliser les activités de sensibilisation et de prise en charge des risques technologiques

L’État gagnerait à être davantage proactif face à une menace en constante progression

5 Renforcer l’écosystème d’expertises et constituer un réseau de veille préventive

- Il importe de soutenir les organisations avec l’expertise afin d’accroître les compétences
- À l’instar d’Israël, la création d’un incubateur devrait être analysée
- La création d’un réseau d’experts en région, ou des « cellules de cyber-résilience » avec un support financier public-privé

6 Accélérer le projet de mise en place du portefeuille numérique du gouvernement du Québec

- Une telle initiative rendrait les renseignements personnels peu utilisables pour de la fraude de toute sorte
- Cela facilitera du même coup la gestion des entreprises de même que leurs relations avec l’État

7 Apprendre de nos leçons récentes

- Les cyberattaques subies par les organisations québécoises (et ailleurs) devraient faire l’objet d’un inventaire et d’un apprentissage systématique dans une plateforme dédiée
- Le partage de bonnes pratiques des organisations affectées, de la prévention à la résolution des menaces apparaît fondamental

8 Interdire le paiement de rançons

- L’expérience montre que cette mesure réduit ce type de criminalité
- Comme près de deux-tiers des entreprises sont favorables à ce que les gouvernements légifèrent pour interdire le paiement de rançon, il semble pertinent d’évaluer la viabilité et la faisabilité d’une telle mesure

Mettre en place les clés de succès d'une valorisation efficace des données

9 Développer une capacité transversale à générer et gérer les données

- Il peut s'agir des capacités numérique et technologique qui demeurent le point de départ de la valorisation des données. Les divers systèmes de l'entreprise (production, gestion des clients, finances, ressources humaines, etc.) doivent se parler
- Les données ouvertes ont déjà porté des fruits

10 Prévoir des règles internes établissant les politiques d'accès sur l'ensemble du cycle de vie des données

- Toute organisation doit définir les acteurs, les rôles et les responsabilités quant à la gestion des données. Elle doit se donner des règles de gouvernance
- La mise en place de processus permettant de collecter, stocker, exploiter et sécuriser les données tout au long de leur cycle de vie est une priorité

11 Adapter la disponibilité et la présentation de l'information pour répondre à différents besoins

- Trop d'information diffuse peut tout aussi mal servir, d'où l'importance de cibler les contenus stratégiques
- Une donnée trop brute, sans analyse ou mal présentée ne fera pas la démonstration de son utilité

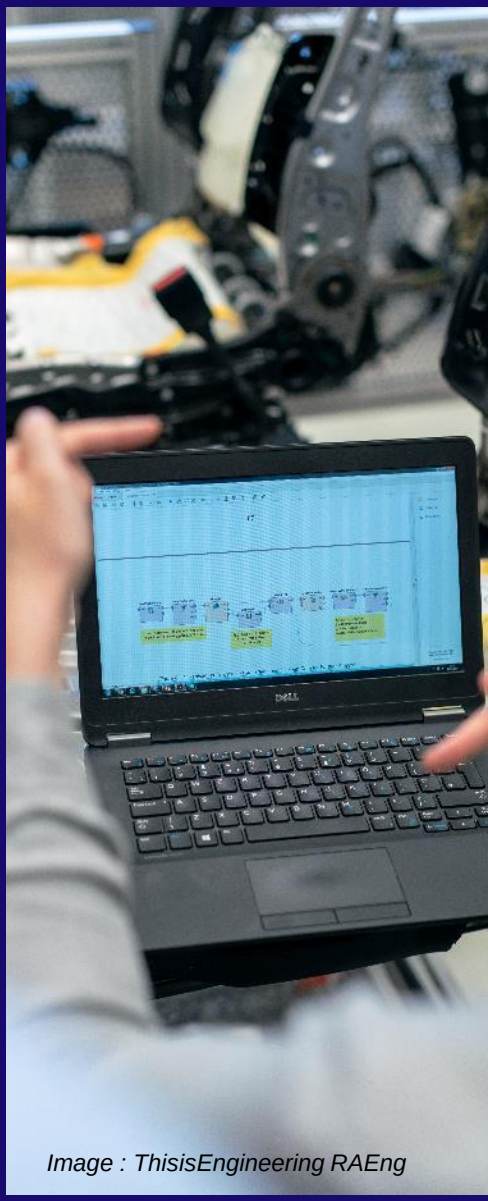


Image : ThisisEngineering RAEng

La mise en valeur des données doit faire appel à toutes les expertises et miser sur la collaboration

12 Intégrer l'apport d'un « traducteur de données » et mieux faire connaître les ressources externes

- Ce rôle peut être dévolu à une ressource interne ou encore à l'externe
- Le traducteur de données utilisera son expertise afin de tirer le plus des données disponibles dans l'organisation
- Les organisations externes gagneraient à mieux faire connaître leurs expertises

13 Soutenir la création de modèles collaboratifs et de partenariats entre entreprises

- Développer des modèles d'affaires fondés sur le partage de données offre un espace d'innovation aux entreprises
- Mener des discussions sur les données et leur usage responsable qui permet de générer et partager de la valeur

14 Accroître les budgets de l'Institut de la statistique du Québec

- Les entreprises ont recours aux données produites par l'ISQ, par exemple pour des études de marché. Mais la qualité et l'accessibilité de ces données se sont détériorées au fil des années
- Les dépenses de l'organisation, à quelque 29M$, n'ont pas augmenté dans la dernière décennie

15 Ouvrir de manière anonymisée les données publiques en santé

- L'instauration d'une gouvernance collaborative, notamment par une fiducie, pour l'utilisation de données sensibles est une réponse à l'équilibre entre l'importance de leur valorisation et de leur protection
- Une application dans le secteur de la santé offre des gains tangibles dont le Québec ne peut plus se passer

FCCQ
Fédération des chambres de commerce du Québec

SECTION 4

ANNEXES

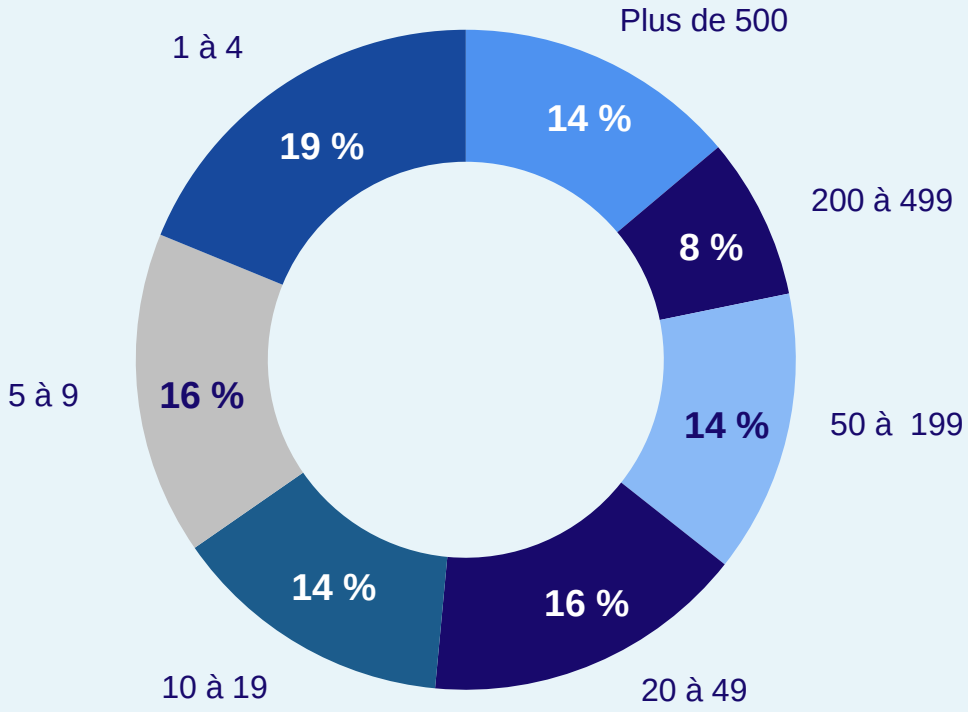
Données du sondages

Cybersécurité

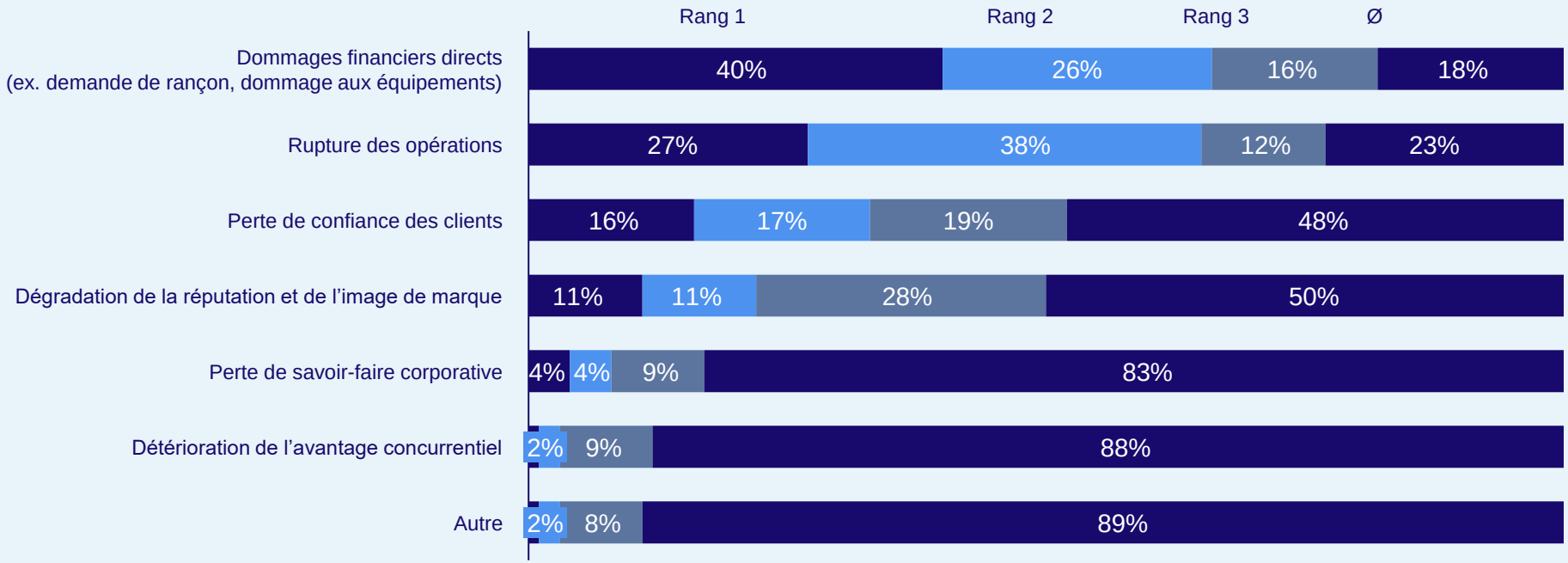
FCCQ
Fédération des chambres de commerce du Québec

Dans quel secteur d’activité œuvre votre entreprise ?

Combien d’employés compte votre entreprise ?

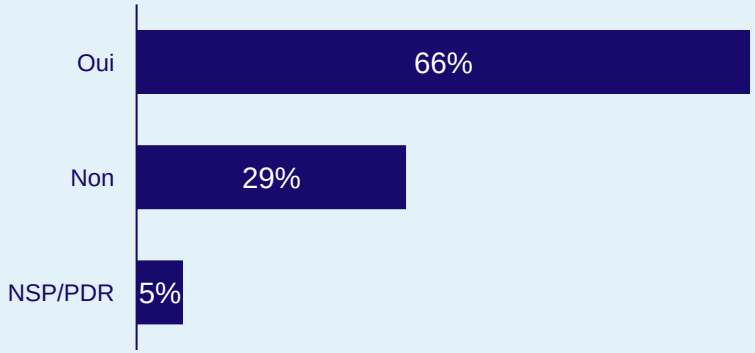


Quel impact négatif lié à la perpétration d'une cyberattaque votre entreprise craint-elle le plus ?

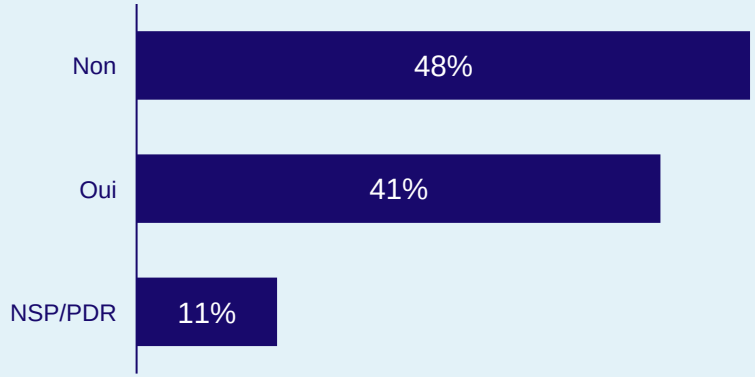


SONDAGE FCCQ

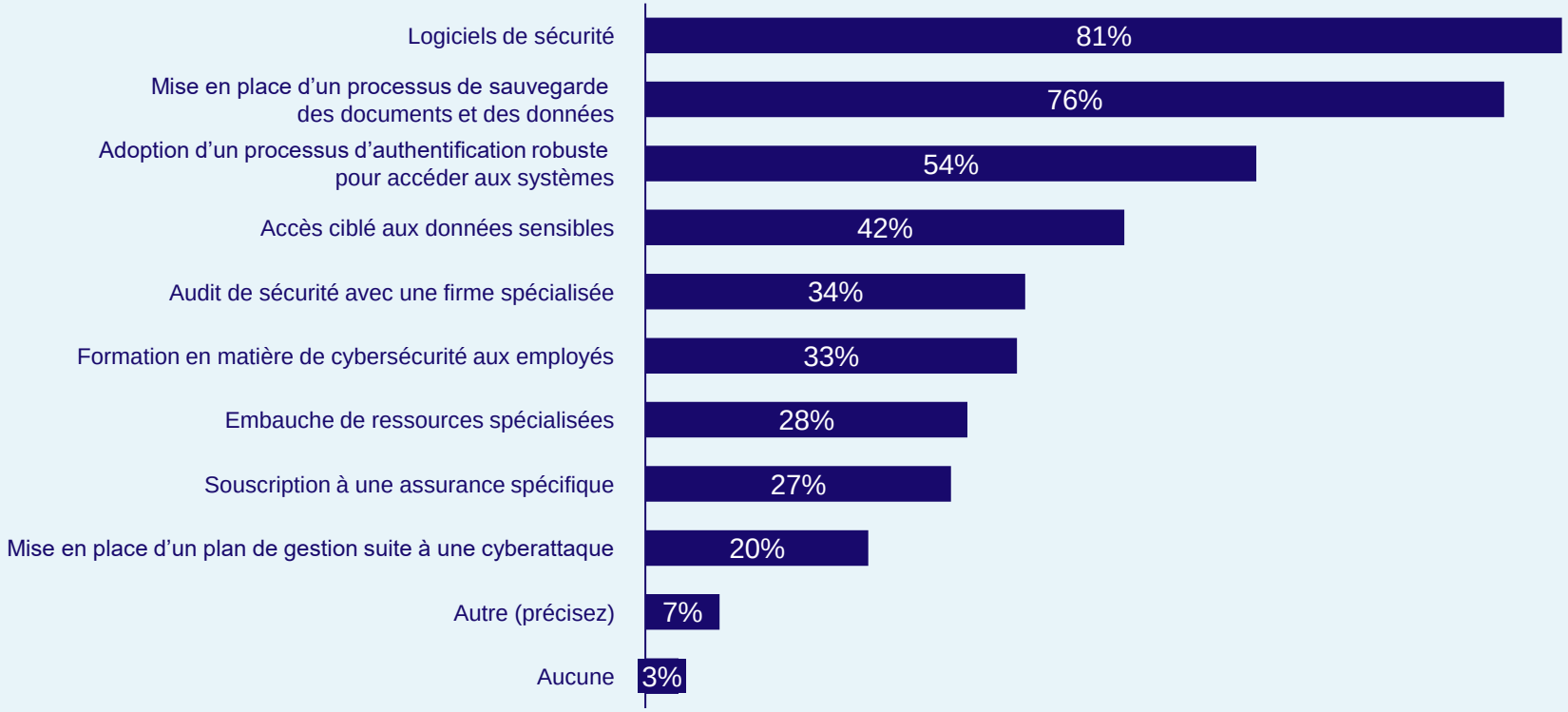
Votre entreprise a-t-elle dévoué des ressources afin de connaître ses vulnérabilités et ses risques liés aux cyberattaques ?



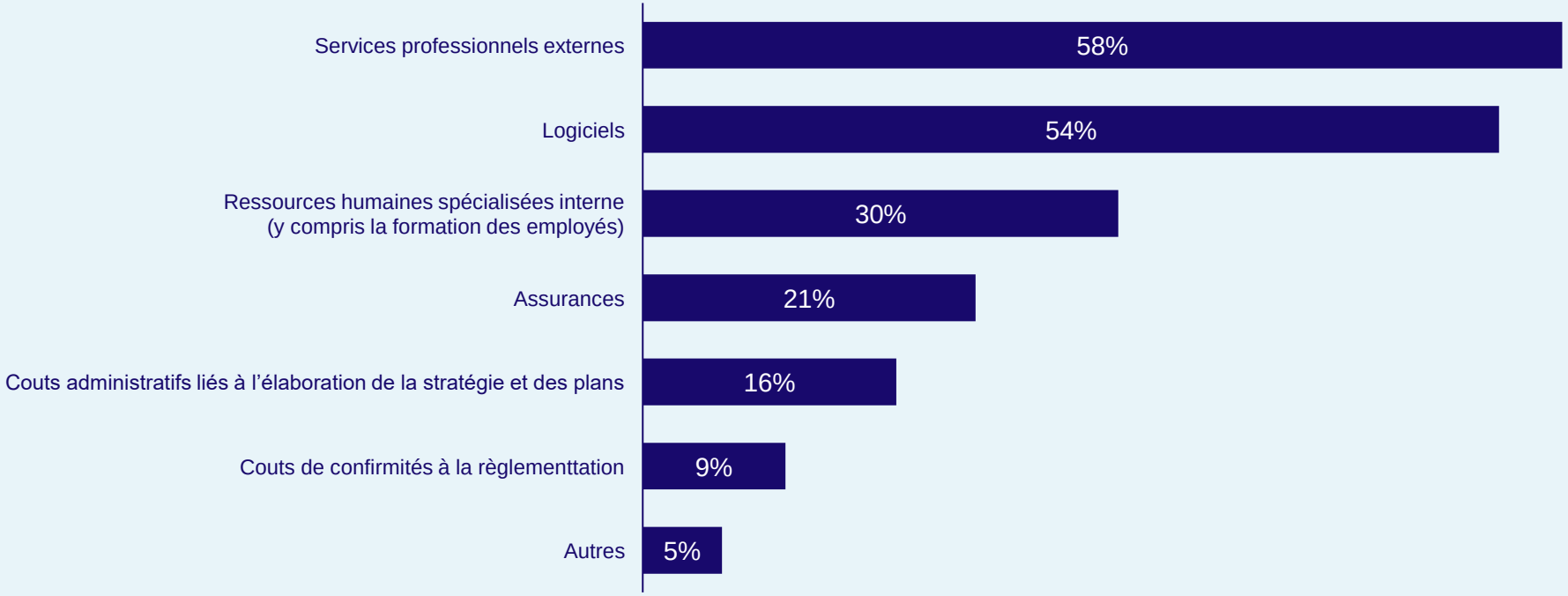
À votre connaissance, votre entreprise a-t-elle fait l’objet d’une ou de plusieurs cyberattaques ?



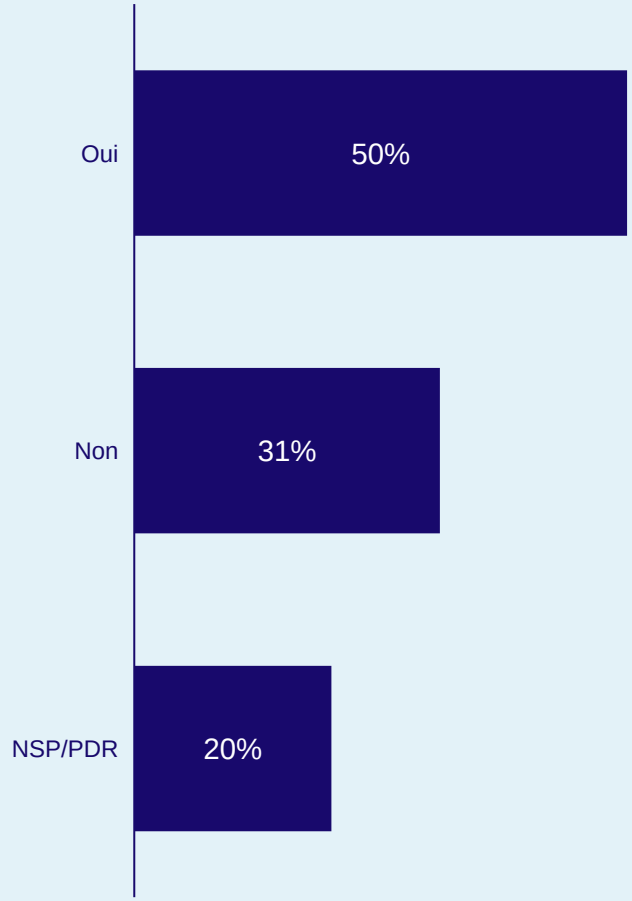
Quelles mesures de protection contre les cyberattaques avez-vous implanté dans votre entreprise ?



Quels sont les coûts les plus importants dans votre entreprise pour se protéger contre les cyberattaques ?



Trouvez-vous que les mesures de protection contre les cyberattaques en place dans votre entreprise sont adéquates et suffisantes ?



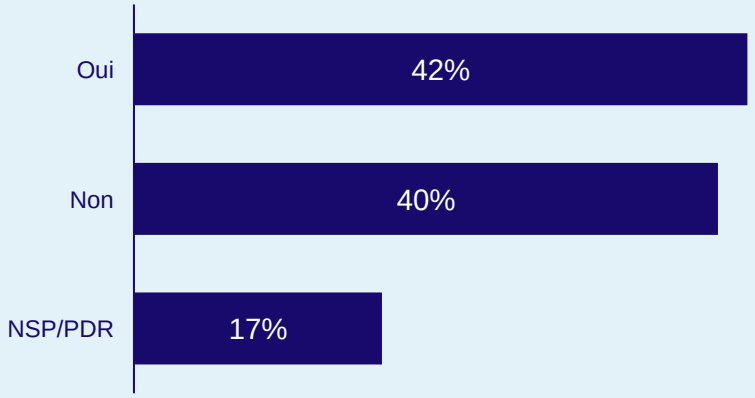
Données du sondages

Valorisation des données

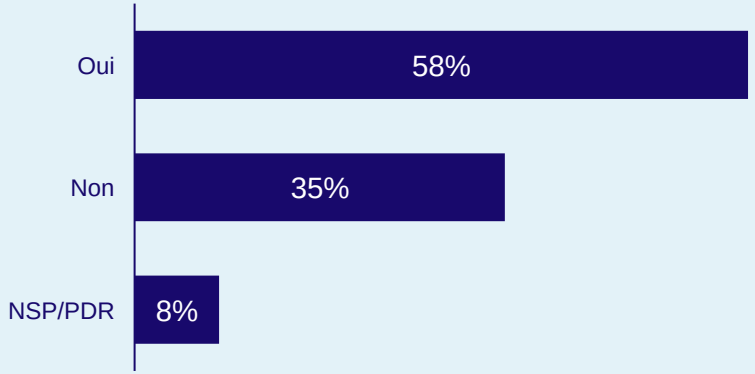
FCCQ
Fédération des chambres de commerce du Québec

SONDAGE FCCQ

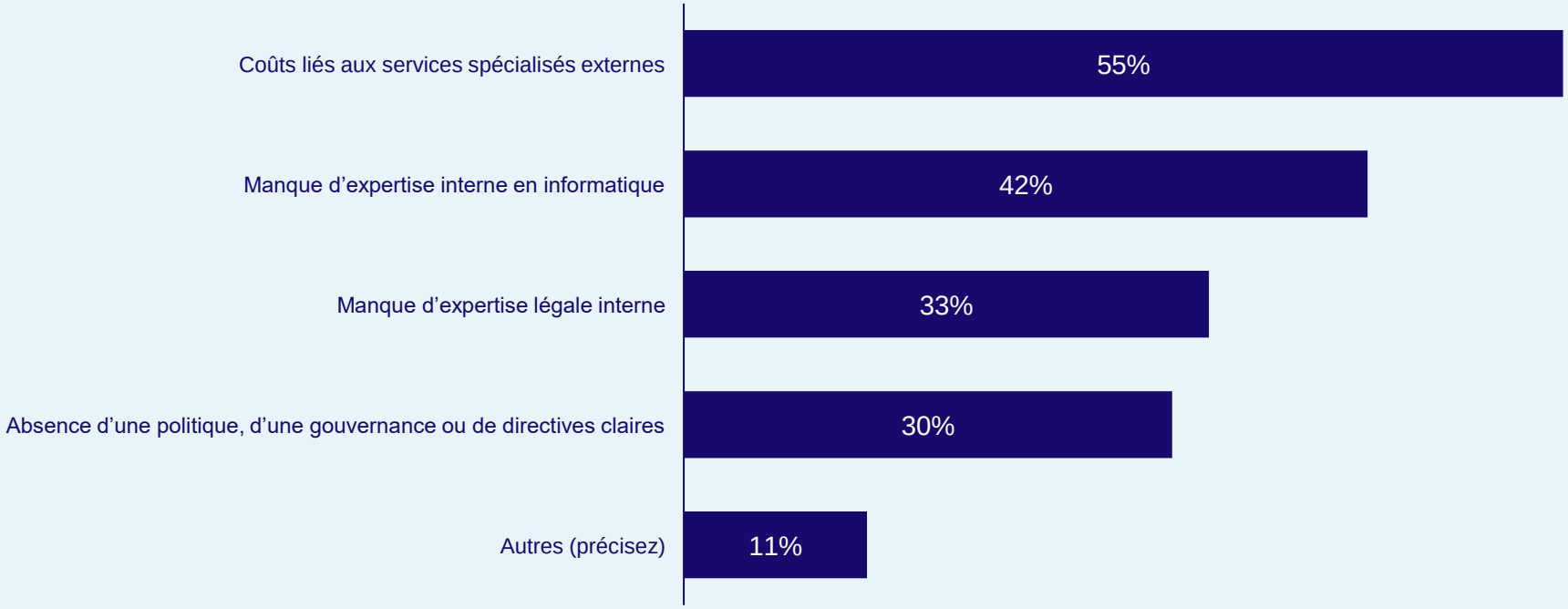
Est-ce que votre entreprise extrait de la valeur de ses propres banques de données ?



Est-ce que votre entreprise a une politique de gestion des données ?



Quels sont les principaux enjeux auxquels fait face votre organisation pour se conformer à ses obligations légales et morales quant aux données ?



Quels sont les principaux enjeux liés à la valorisation des données qui empêchent présentement votre entreprise d’en extraire le maximum de valeur ?