ÉLECTRO FÉDÉRATION CANADA EFC

SÉCURISER SES ACTIVITÉS :

les meilleures pratiques en matière de cybersécurité

RÉSUMÉ

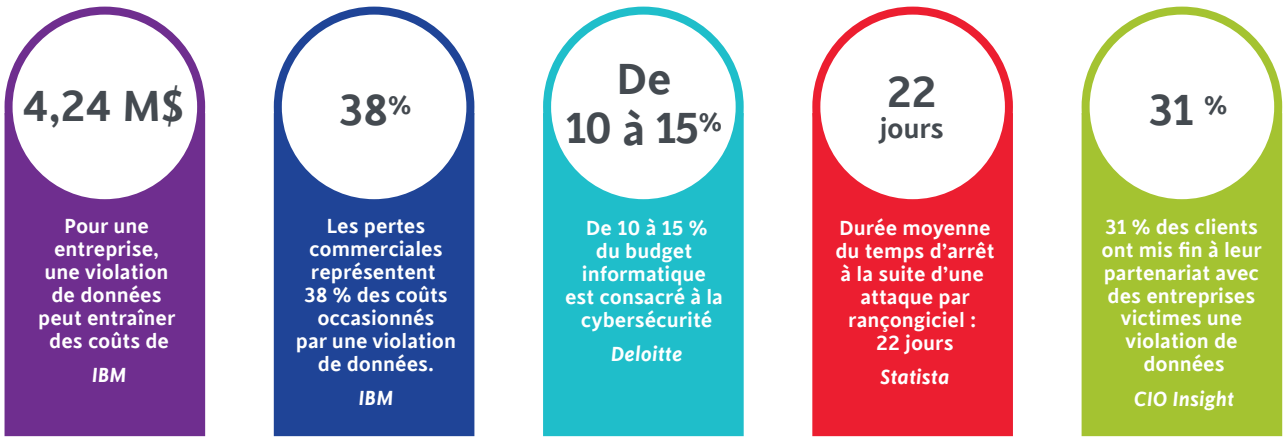
Aujourd'hui, dans ce monde interconnecté qu'est le nôtre, la cybersécurité est essentielle. Toute installation court le risque d'être la cible d'une cyberattaque, des entreprises et usines aux banques et établissements, en passant par les maisons et même les infrastructures telles que les réseaux de transmission d'électricité. Le but d'une cyberattaque est généralement d'accéder, de modifier ou de détruire des informations sensibles, d'extorquer de l'argent aux gens ou d'interrompre les processus normaux d'entreprises.

Sur l'enjeu de la cybersécurité, les spécialistes s'entendent pour dire que la question n'est pas de savoir si il faudra un jour faire face à une compromission, mais bien quand elle se présentera. Quand une compromission se produit, les organisations disposant d'un plan de cybersécurité efficace peuvent rapidement détecter le problème et y répondre, tout en évitant l'interruption des activités commerciales et la perte potentielle d'argent, de propriété intellectuelle, de confiance des parties prenantes et de réputation de la marque. Pour les organisations, l'impact financier d'une violation de données est très important. Elle entraîne souvent des pertes commerciales ainsi que la mise en place de mesures d'intervention, de détection et de signalisation progressive, entre autres, qui peuvent leur coûter en moyenne 4,25 millions de dollars[1].

> Les organisations doivent « évaluer les risques pour l'information et les systèmes avec la même vigueur qu'elles adoptent lors de l'évaluation des risques juridiques, réglementaires, financiers ou opérationnels ».
>
> Source: National Cyber Security Centre (UK)

Ce document offre des recommandations sur les meilleures pratiques et les mesures concrètes à adopter en tant qu'organisation afin d'établir des protocoles de sécurité capables de protéger ses données et ses systèmes. Ne pas agir de manière préventive peut vous coûter cher.

Vous trouverez ci-dessous les principales implications et mesures à prendre en compte lorsque votre organisation élabore son plan d'action en matière de cybersécurité :



[1] Rapport 2021 d'IBM sur le Coût d'une violation de données

Trousse de cybersécurité : Parvenir à un état sécurisé de votre environnement informatique exige du temps, des investissements, de la collaboration et des ressources. Les groupes de travail sur Les meilleures pratiques en matière de cybersécurité et sur Les mesures de réussite en matière de cybersécurité de l'ÉFC, composés de nos membres experts en informatique, ont préparé une trousse de cybersécurité afin d'aider votre organisation à planifier, préparer et améliorer sa stratégie d'atténuation des risques et d'intervention.

Veuillez consulter ce lien afin d'accéder aux ressources complètes de la trousse. Nous vous recommandons fortement de partager ces ressources avec votre équipe informatique. Pour toute question, veuillez joindre l'ÉFC à **info@electrofed.com**.

COMMENCER DU BON PIED GRÂCE À UNE VISION COMMUNE

La cybersécurité est un impératif commercial qui relève de la *responsabilité de tous*.

Pour qu'une stratégie de cybersécurité soit efficace, les chefs d'entreprise et le personnel informatique doivent avoir une compréhension commune des risques, des défis, des priorités et du plan d'action de leur organisation. Il existe souvent un gouffre qui sépare les connaissances des dirigeants et celles des responsables informatiques. Les chefs d'entreprise peuvent ne pas connaître les spécificités des types de cybermenaces ou des exigences du système, tandis que les équipes informatiques peuvent ne pas être conscientes des implications commerciales et financières.

Le tableau suivant présente des exemples de questions courantes que les dirigeants et les équipes informatiques peuvent aborder ensemble afin d'interpréter et de définir un plan de cybersécurité d'entreprise adapté à leur organisation :

Questions clés	Ce que cela implique
Nos pratiques sont-elles conformes?	• Quelles sont les normes de cybersécurité que nous devons respecter ou même dépasser? • Respectons-nous ces normes? *Si oui*, quelles mesures sont en place au sein de notre organisation pour nous assurer de maintenir cette conformité? *Si non*, quelles mesures devons-nous mettre en place pour assurer notre conformité?

Nos activités sont-elles sécurisées?	• Sommes-nous conscients de nos risques et des menaces? Quels sont-ils? • Est-ce que nous savons quels sont nos principaux atouts? • Comment les protégeons-nous?
Nos mesures de sécurité ont-elles évolué depuis l'année dernière? De quelles manières?	• Qu'est-ce qui a changé par rapport à nos approches de protection, ou au sein de notre organisation, au cours des douze derniers mois? • Comment abordons-nous les nouveaux défis de sécurité? • En quoi nous sommes-nous améliorés? • Que pouvons-nous faire de plus pour atténuer les risques? Quels coûts ou ressources est-ce que cela implique?
Quel est notre plan d'action en cas de violation de données ou d'attaque?	• Quels incidents de sécurité se sont produits au sein de notre organisation? • Comment ont-ils été traités? • Qu'avons-nous appris? • Comment nous sommes-nous adaptés?

TYPES DE MENACES À LA CYBERSÉCURITÉ

La première étape pour protéger votre entreprise consiste à comprendre les types les plus communs de menaces à la cybersécurité :

Violations de données

Une violation de données se produit lorsque des données sensibles sont volées d'un système sans l'autorisation du propriétaire du système. Les cybercriminels opèrent en cherchant des faiblesses dans les paramètres de sécurité d'une entreprise au sein des systèmes de réseau ou de point de vente (PDV), puis en exploitant cette faiblesse afin d'accéder aux informations confidentielles de l'utilisateur, aux détails concernant les cartes de crédit et la sécurité sociale, ainsi qu'aux noms d'utilisateur et aux mots de passe. Les violations de données peuvent également se produire sous forme d'attaques d'ingénierie sociale. Dans ces cas, les cybercriminels trompent les utilisateurs en leur faisant télécharger des pièces jointes nuisibles ou en leur demandant de récupérer leurs identifiants de connexion. Ils obtiennent ainsi l'accès au réseau de l'entreprise. Lorsqu'une violation de données se produit, les entreprises doivent prendre des mesures immédiates servant à limiter la violation et à résoudre le problème afin d'éviter les temps d'arrêt du système et les interruptions de service.

Mots de passe compromis

Les mots de passe sont le plus souvent compromis lorsqu'un utilisateur saisit ses identifiants de connexion sur un site Web illégitime sans le savoir. Les combinaisons de nom d'utilisateur et de mot de passe choisies par défaut ou trop courantes peuvent également rendre les comptes vulnérables aux attaques. L'utilisation du même mot de passe sur plusieurs plateformes peut rendre les systèmes encore plus vulnérables aux pirates informatiques, puisque plusieurs comptes deviennent alors à haut risque. Plusieurs rapports suggèrent que plus de la moitié des utilisateurs utilisent un même mot de passe pour leurs comptes professionnels et personnels. Nous vous recommandons donc d'exiger du personnel la création de mots de passe uniques pour leurs comptes d'entreprise. Dans la mesure du possible, fournissez un service de gestion des mots de passe au personnel afin de les aider à gérer et à protéger leur mot de passe.

Les coûts reliés aux violations de données ont considérablement augmenté d'une année à l'autre. Ils sont passés de **3,86 millions** de dollars en 2020 à **4,24 millions** de dollars en 2021.

Source: Cost of Data Breach Report (IBM, 2021)

Hameçonnage

Cette méthode de piratage incite les utilisateurs à télécharger des messages nuisibles, exposant ainsi leurs organisations à des risques considérables. Les utilisateurs reçoivent des courriels frauduleux qui semblent provenir d'une source fiable et qui contiennent des liens, des pièces jointes, des noms commerciaux et des logos d'apparence légitime. Ces courriels ou messages incitent souvent les utilisateurs à procéder à une certaine action, qu'il s'agisse de cliquer sur un lien ou de télécharger une pièce jointe, dans le but de voler des données sensibles, telles que les informations de carte de crédit ou de connexion, ou d'installer des logiciels malveillants sur le dispositif de l'utilisateur. La plupart des violations de données impliquent l'hameçonnage d'une manière ou d'une autre. Selon Cisco, 86 % des organisations ont déclaré avoir eu à gérer la connexion d'au moins un de leurs utilisateurs à un site d'hameçonnage[2].

Logiciels malveillants

Également appelés « maliciels », les logiciels malveillants sont conçus pour endommager et nuire aux ordinateurs et aux systèmes en les ralentissant ou en les empêchant de fonctionner correctement. Les types de logiciels malveillants les plus courants incluent les virus de type cheval de Troie, les logiciels espions, les logiciels publicitaires, les vers informatiques et les rançongiciels. Les logiciels malveillants obtiennent l'accès à l'ordinateur lorsqu'un utilisateur clique sur un lien qui mène à un site infecté ou sur une publicité ou lorsqu'il télécharge une pièce jointe à un courriel d'un expéditeur inconnu. Une fois que le logiciel malveillant a pénétré le système informatique, les pirates peuvent alors accéder aux mots de passe de l'entreprise, aux numéros de carte de crédit, aux données bancaires, aux fichiers du personnel, etc.

Rançongiciels

Le rançongiciel est un type de logiciel malveillant qui empêche les utilisateurs d'accéder aux systèmes ou aux fichiers jusqu'à ce que le paiement d'une rançon soit versé aux cybercriminels.Les rançongiciels se propagent souvent par le biais de téléchargements malveillants inclus dans un courriel d'hameçonnage. Une attaque peut cibler un employé individuel ou des organisations entières.

Les coûts reliés aux attaques des rançongiciels sont plus élevés que ceux associés aux autres formes de violations et peuvent atteindre des centaines ou des milliers, voire des millions, de dollars. Malheureusement, de nombreuses entreprises qui paient la rançon auprès des pirates informatiques ne récupèrent tout de même pas l'accès à leurs systèmes.

[2] Banks, Joe "5 cybersecurity threats for businesses in 2021." Security Magazine, September 12, 2021.

CHIFFRES CLÉS SUR LES RANÇONGICIELS EN 2021

Le nombre de courriels malveillants a augmenté de 600 % en raison de la pandémie de la COVID-19

La plus importante rançon payée s'est élevée à 40 millions de dollars

La somme moyenne des rançons ciblant des entreprises était de

200 000 $

La durée moyenne du temps d'arrêt à la suite d'une attaque est de

21 jours

Seulement 8 % des victimes qui paient leur rançon récupèrent tous leurs fichiers cryptés

80 % des victimes qui ont payé une rançon ont subi une deuxième attaque

46 % des victimes qui ont payé une rançon ont récupéré des données corrompues

60 % des victimes ont souffert des pertes de revenu en raison de l'attaque

Source: phoenixnap.com/blog/what-is-ransomware

L'IMPACT DES CYBERATTAQUES SUR LES ACTIVITÉS COMMERCIALES

Les cyberattaques ont un impact direct sur la rentabilité d'une entreprise. Pourtant, plusieurs chefs d'entreprise ne sont pas conscients **du coût que peut représenter l'inaction** pour leur organisation.

Selon une étude d'IBM, les entreprises victimes d'atteintes à la protection des données sont confrontées, en moyenne, à 4,24 millions de dollars de coûts. Cette somme est en grande partie attribuable à quatre facteurs : **les coûts d'intervention après la violation, les coûts de détection et de signalisation progressive, les coûts de notification, et les coûts reliés aux pertes commerciales.**

Intervention après la violation

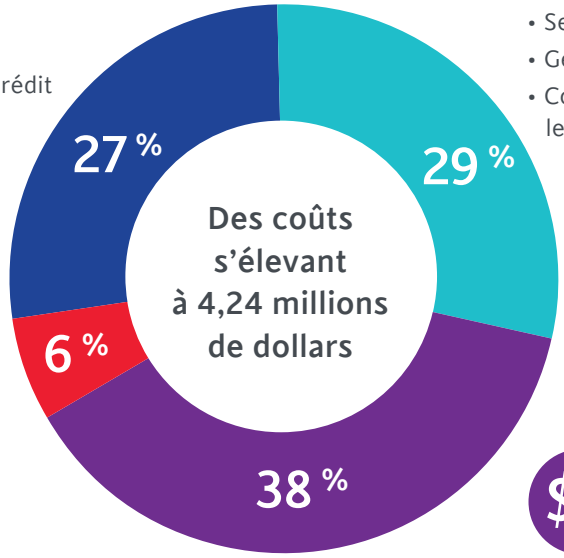
Services et activités servant à aider les victimes d'une violation de données à communiquer avec l'entreprise et services de recours auprès des victimes et des organismes de réglementation

- Services d'assistance et de communications entrantes
- Services de surveillance du crédit et de protection de l'identité
- Attribution de nouveaux comptes ou émission de nouvelles cartes de crédit
- Dépenses juridiques
- Remises sur les produits
- Amende réglementaire

Détection et signalisation progressive

Services et activités qui permettent, dans la mesure du raisonnable, à une entreprise de détecter la violation de données

- Activités médicolégales et d'enquête
- Services d'évaluation et d'audit
- Gestion de crises
- Communication avec les dirigeants et les conseils d'administration



Notification

Services et activités qui permettent à l'entreprise de notifier les personnes concernées, les organismes de réglementation sur la protection des données et autres tiers

- Courriels, lettres, appels sortants ou communication générale aux personnes concernées
- Détermination des exigences réglementaires
- Communication avec les organismes de réglementation
- Engagement d'experts externes

Pertes commerciales

Services et activités qui tentent de minimiser la perte de clients, les interruptions d'activité et les pertes de revenus

- Interruption des activités et pertes de revenus dues aux temps d'arrêt du système
- Coûts reliés aux clients perdus et acquisition de nouveaux clients
- Pertes reliées à l'impact sur la réputation et diminution du fonds commercial

Adapté à partir du : Rapport sur le Coût d'une violation de données (IBM, 2021)

Outre leurs impacts sur la rentabilité, les cyberattaques peuvent également compromettre la propriété intellectuelle d'une entreprise et la réputation de la marque. Elles peuvent également engendrer des conséquences juridiques et réglementaires. Examinons certains de ces autres facteurs :

Impact sur la marque

Nous souhaitons tous faire affaire avec des organisations capables de protéger nos informations. L'un des atouts les plus importants d'une entreprise est donc la confiance qu'elle réussit à établir avec ses clients. Ainsi, l'impact qu'une cyberattaque peut avoir sur une marque peut être désastreux. Selon une enquête menée par CIO Insight, 31 % des clients interrogés ont déclaré avoir mis fin à leur partenariat avec des entreprises victimes d'une violation de données. Parmi ces clients, 65 % ont déclaré avoir perdu confiance dans l'organisation ayant subi une violation de données[2].

Pour pallier les conséquences liées à ces pertes de réputation de la marque et de confiance des clients, les entreprises se doivent d'être transparentes auprès de leurs clients et partenaires par rapport aux approches concrètes qu'elles adoptent pour protéger leurs données. Dès que votre entreprise investit dans des améliorations de la sécurité des données et démontre un effort supplémentaire dans le cadre de la protection des données de ses utilisateurs, assurez-vous d'en informer vos clients et partenaires. Une telle approche transparente devrait faire partie intégrante de votre proposition de valeur.

Il est essentiel que les équipes de marketing participent à l'élaboration d'un plan de communication avec les clients avant qu'une violation ne se produise. Les départements de marketing occupent une position unique qui leur permet de bien comprendre les intérêts des parties prenantes. Plus que quiconque, ils ont les moyens d'entretenir et de protéger la confiance que les entreprises se sont efforcées d'établir avec leurs clients et partenaires depuis des décennies.

Répercussions juridiques

Une violation de données peut compromettre des informations sensibles, entraînant une perte de propriété intellectuelle et des répercussions juridiques importantes. Les équipes juridiques sont tenues de respecter les lois provinciales et fédérales régissant la notification des violations de données et, si elles s'appliquent à leur clientèle, les lois internationales également.

En vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), les organisations sont tenues de signaler les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus. Les personnes concernées doivent être notifiées et un registre de toutes les activités concernant la violation de données doit être conservé. Comme il a été indiqué précédemment, les coûts de notification représentent environ 6 % des coûts reliés aux cyberattaques. Ils incluent les dépenses liées à la notification d'une violation de données aux organismes de réglementation, aux partenaires, aux clients et au grand public.

[3] Frenkel, Karen A. "Linking Breaches, Brand Reputation & Stock Prices," *CIO Insight*, June 2017.

Lorsqu'une organisation subit une violation de données, l'affaire est alors traitée devant le système de justice. L'entreprise doit alors démontrer qu'elle a bel et bien fait preuve de « diligence raisonnable ». Ce terme est utilisé par les juges pour décrire le « caractère raisonnable » des exigences requises. Les organisations doivent donc démontrer qu'elles avaient mis en place des mesures raisonnables et appropriées pour l'entreprise ainsi que pour les autres parties prenantes, et que celles-ci existaient au moment de la violation. Il est important pour votre organisation d'évaluer le niveau des données sensibles que votre entreprise s'occupe de recueillir, et de conserver une trace des mesures de « diligence raisonnable » mises en place pour protéger ces données.

ÉTUDE DE CAS : YAHOO

L'une des plus importantes violations de données d'entreprise enregistrées impliquait la compagnie Yahoo. En 2016, Yahoo a déclaré que, deux ans auparavant, environ 500 millions de comptes d'utilisateurs avaient été volés. La situation de Yahoo s'est particulièrement aggravée lorsque les responsables ont révélé que la société était au courant de la violation depuis déjà trois mois et qu'elle n'en avait pas informé ses clients. La mauvaise gestion de Yahoo face à cette situation et leur particulière lenteur de divulgation ont eu des implications commerciales et de marque importantes : plusieurs poursuites ont été déposées et le cours des actions de Yahoo a chuté, faisant perdre à la compagnie 1,5 milliard de dollars de valeur marchande.

Source: ResearchGate: Journal of Advertising Research (March 2017)

POURQUOI INVESTIR DANS LA CYBERSÉCURITÉ

Investir dans la cybersécurité, c'est aussi miser sur l'atténuation des risques. C'est une approche concrète qui permet de protéger les systèmes et les applications contre les attaques malveillantes. Mais attention, ne vous fiez pas au rendement du capital investi pour juger de l'efficacité de cet investissement. Sachez simplement que si votre entreprise est victime d'un cas de violation de données et qu'elle réussit à maintenir un état sécurisé des affaires grâce à un plan d'intervention bien planifié, vos investissements auront déjà amplement porté leurs fruits.

Mais à quel point faut-il raisonnablement dépenser dans la cybersécurité? Le budget consacré à la cybersécurité varie, bien sûr, d'une entreprise à une autre, mais les organisations doivent s'attendre à consacrer **10 à 15 % de leur budget informatique à la cybersécurité**. Selon une étude récente réalisée par Deloitte, les entreprises du secteur des services financiers consacrent en moyenne 10 % de leur budget informatique à la cybersécurité. Cela équivaut à environ 1 300 $ à 3 000 $ par employé dans un poste à temps plein[3]. (Remarque : cette estimation risque d'être plus élevée pour les plus petites entreprises, car elles ne peuvent pas tirer parti de la taille ou du volume de leur compagnie.)

Pour certains, l'attribution de 10 à 15 % du budget aux dépenses de cybersécurité peut sembler élevée. Cependant, ne pas investir suffisamment de fonds dans la protection des données peut avoir des conséquences désastreuses sur la continuité des opérations. Sur une période d'un an et demi, Statista s'est occupé de suivre les opérations d'entreprises qui avaient subi une attaque de rançongiciel et a constaté que la durée moyenne du temps d'arrêt qu'elles avaient subi était de 22 jours[4]. Même les entreprises bien préparées connaissent des temps d'arrêt de 14 jours en moyenne. C'est une durée qui entraîne des pertes commerciales substantielles qui équivalent à plus que le montant attribué aux mesures de cybersécurité.

Investir dans la cybersécurité est primordial, mais cela implique aussi des investissements assez divers. La planification en cybersécurité implique généralement la mise en place de mesures et d'opérations de cybersurveillance, de protection des points terminaux et du réseau, ainsi que des applications et des données, de gestion des identités et des accès et de gestion de la sécurité des tiers et des fournisseurs. La prochaine section de ce document présente un aperçu des neuf piliers clés sur lesquels les organisations devraient se baser dans le cadre de leur planification pour la cybersécurité.

[4] Bernard, Julie and Nicholson, Mark, "Reshaping the Cybersecurity Landscape", Deloitte Insights: July 24 2020
[5] statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ – consulté en mars 2022

LES NEUF PILIERS CLÉS DE LA PLANIFICATION POUR LA CYBERSÉCURITÉ

La mise en place d'une stratégie de cybersécurité complète implique plusieurs points de contact et mesures de sécurité afin de garantir la protection des actifs contre les menaces et les attaques malveillantes. Voici neuf champs clés de la sécurité qui devraient faire partie intégrante du plan d'action en matière de cybersécurité :

LES MEILLEURES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ

1. **Soutien à la réalisation de l'équipe et du chef de la sécurité :** Assurez-vous que votre équipe informatique dispose du budget, des outils et des ressources nécessaires pour protéger les données et les systèmes de votre entreprise contre les risques de sécurité.

2. **Protection des points terminaux :** Sécurisez les ordinateurs de bureau, les ordinateurs portables, les appareils mobiles et les serveurs contre les cyberattaques en installant des logiciels gérés de manière centralisée par des administrateurs de la sécurité.

3. **Protection du réseau et du périmètre :** C'est la ligne de défense la plus importante, puisqu'elle implique les systèmes qui filtrent et examinent les données entrant et sortant du réseau de l'entreprise et se déplaçant entre les différents composants ou branches du réseau. Les pare-feu sont l'exemple principal de ce type de systèmes.

4. **Gestion des comptes et des identités :** Mettre en place un cadre de sécurité qui autorise et authentifie l'accès des utilisateurs à travers les applications, les portails Web, les données, les systèmes et les plateformes en nuage, garantit que seules les bonnes personnes ont accès aux bons outils et pour les bonnes raisons.

5. **Formation des utilisateurs et sensibilisation à la sécurité :** Suivre une formation formelle en cybersécurité permet à votre personnel de savoir faire l'évaluation et d'être à l'affût des menaces de sécurité potentielles. Le suivi d'une formation est d'autant plus efficace lorsque cette dernière fait partie d'une pratique continue et lorsque des politiques de sécurité sont établies pour fournir à votre personnel des définitions, des règles, des processus et des comportements attendus en matière de sécurité.

6. **Plan d'intervention en cas d'incident et reprise :** Ce plan consiste en un ensemble d'instructions conçues pour aider les entreprises à se préparer aux incidents de sécurité majeurs, à les détecter, à y réagir et à s'en remettre.

7. **Mesure, surveillance, évaluation, contrôle :** Il est essentiel de surveiller et de tester en permanence les réseaux informatiques, les systèmes, l'utilisation des données et les applications et l'infrastructure informatiques afin de pouvoir détecter de manière proactive les vulnérabilités, les menaces ou les violations des données.

8. **Prévention de la perte de données et confidentialité des données :** Ces outils et processus protègent les données sensibles contre la perte, l'utilisation abusive ou l'accès par des utilisateurs non autorisés.

9. **Sécurité des applications :** Il est essentiel d'utiliser des outils et des méthodes servant à sécuriser les applications une fois qu'elles ont été déployées.

TRACER SON PROPRE PARCOURS EN MATIÈRE DE CYBERSÉCURITÉ

Lors de la préparation de ce guide, les groupes de travail sur Les meilleures pratiques en matière de cybersécurité de l'ÉFC se sont donné pour objectif de fournir une feuille de route facile à utiliser pour les organisations du secteur afin qu'elles puissent renforcer leurs stratégies en matière de cybersécurité. Le groupe de travail recommande une ressource complète et exhaustive créée par le Center for Internet Security (CIS) dans le but d'aider les entreprises à développer leur stratégie en matière de cybersécurité. Le CIS est un organisme communautaire à but non lucratif responsable du développement des **CIS Controls®**, un ensemble de 18 contrôles de sécurité critiques mondialement reconnus visant à atténuer l'impact des cyberattaques les plus communes sur les systèmes et les réseaux. Les contrôles de sécurité CIS présentent une structure complète et détaillée qui englobe plusieurs cadres juridiques, réglementaires et politiques.

Veuillez scanner ce code QR pour visionner une courte vidéo sur les contrôles CIS

Les 18 contrôles CIS sont présentés ci-dessous :

01 Inventaire et gestion des actifs de l'entreprise	02 Inventaire et gestion des biens logiciels	03 Protection des données
04 Configuration sécurisée des biens logiciels et des actifs de l'entreprise	05 Gestion des comptes	06 Gestion du contrôle d'accès
07 Gestion continue des vulnérabilités	08 Gestion des journaux d'audit	09 Protection des courriels et du navigateur Web
10 Protection contre les programmes malveillants	11 Récupération des données	12 Infrastructure du réseau
13 Protection et surveillance du réseau	14 Formation et sensibilisation à la sécurité	15 Gestion des fournisseurs de service
16 Sécurité des logiciels d'application	17 Gestion de l'intervention en cas d'incident	18 Essais de pénétration

Les contrôles CIS et les groupes de mise en œuvre

Les contrôles CIS ne sont pas une solution unique pour tous. Ils sont plutôt divisés en **trois groupes de mise en œuvre distincts (G1, G2, G3)**. Toutes les organisations appartiennent à un groupe de mise en œuvre selon leur profil de risque, leurs ressources disponibles et leur budget, ce qui signifie qu'elles peuvent toutes profiter du plan des contrôles CIS de manière accessible et abordable afin d'atteindre la cybersécurité. Chacun des trois groupes de mise en œuvre possède une liste de **mesures de garantie** en cybersécurité afin d'aider les entreprises à hiérarchiser selon leurs priorités les pratiques les plus essentielles en fonction de leurs capacités, de leur budget et de leur taille. Il existe 153 mesures de garantie au total.

Le **G1** est la définition même de la cybersécurité de base et représente la norme minimale de sécurité de l'information pour toutes les entreprises. Le G1 permet aux entreprises présentant une expertise limitée en cybersécurité de se protéger des attaques générales non ciblées.

Niveau de base :
S'attaque aux besoins les plus essentiels en matière de « cyberhygiène ». Ce niveau inclut 56 mesures de garantie en cybersécurité de base.

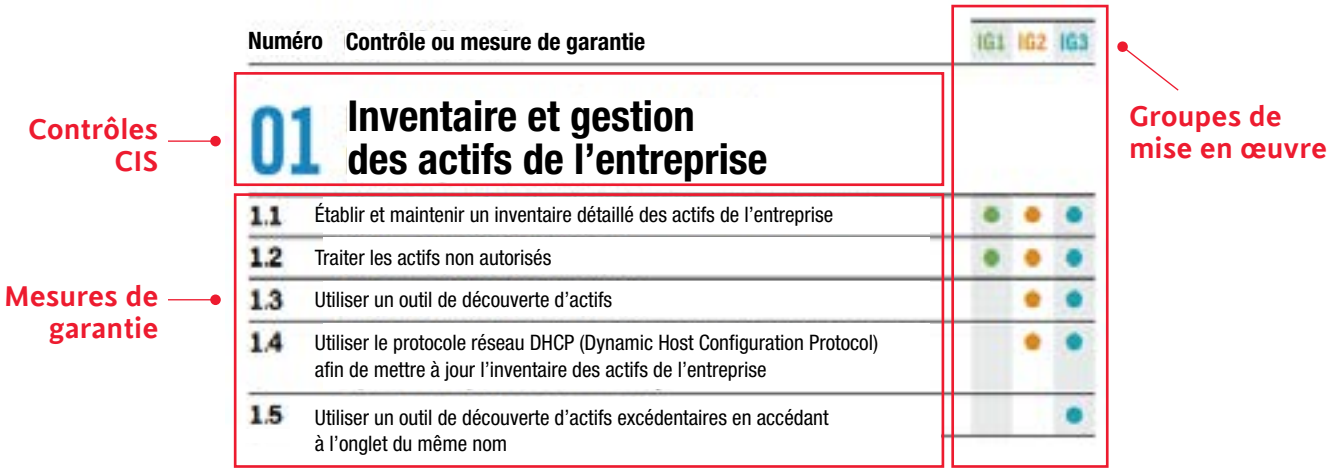
Le **G2** s'adresse aux entreprises qui doivent gérer l'infrastructure informatique de plusieurs départements présentant des profils de risque différents. Le G2 vise à aider les entreprises à faire face à une complexité opérationnelle accrue.

Niveau intermédiaire :
Fournit une structure de sécurité et de protection plus complète. Ce niveau inclut 74 mesures de garantie en cybersécurité supplémentaires.

Le **G3** s'adresse aux entreprises disposant déjà d'experts en sécurité informatique et les aide à sécuriser les données sensibles et confidentielles. Le G3 vise à prévenir ou à réduire l'impact d'attaques plus sophistiquées.

Niveau avancé :
Fournit les protocoles de sécurité les plus complets et comprend les 18 contrôles CIS. Ce niveau inclut 23 mesures de garantie en cybersécurité supplémentaires (soit, au total, toutes les 153 mesures).

Afin de mieux illustrer cette méthodologie, l'exemple ci-dessous présente le premier contrôle CIS et décrit une série de cinq mesures de garantie classées selon le groupe de mise en œuvre concerné :



Un exemple d'un contrôle CIS et ses mesures de garantie et groupes de mise en œuvre appropriés

Afin de consulter les 18 contrôles CIS ainsi que leurs mesures de garantie et groupes de mise en œuvre associés, accédez à la trousse de cybersécurité (vous devrez, pour y accéder et la télécharger, saisir vos coordonnées). (Remarque : Les groupes de travail chargés de la cybersécurité de l'ÉFC ont élargi le cadre des contrôles CIS en déterminant les niveaux les plus prioritaires et en fournissant un ensemble de recommandations d'outils capables de satisfaire aux mesures de garantie).

MENER DES ÉVALUATIONS DES RISQUES

L'évaluation des risques en matière de cybersécurité est le nom donné au processus, ou à la méthode, global utilisé afin d'identifier les facteurs de risque susceptibles de nuire aux systèmes et aux réseaux. Cette évaluation comprend également une analyse et une appréciation des risques permettant ensuite de déterminer des stratégies d'atténuation et de prévention efficaces.

Le Center for Internet Security a développé deux outils d'évaluation des risques afin de vous aider à déterminer la posture de votre organisation en matière de cybersécurité par rapport aux contrôles CIS :

1. **Outil d'auto-évaluation des contrôles CIS (CSAT) :** une méthode de base pour les organisations disposant de ressources ou de connaissances techniques limitées. L'outil CSAT permet une collaboration interdépartementale. Avec cet outil, les utilisateurs peuvent confier certaines questions à d'autres utilisateurs, valider des réponses et créer des sous-organisations. L'utilisation à titre non commercial de l'outil CSAT est gratuite pour toutes les organisations. Elles pourront ainsi mener des évaluations de leur organisation dans le cadre des contrôles CIS. Afficher la FAQ

2. **Méthode d'évaluation des risques (CIS RAM)** une méthode avancée qui fournit des instructions sur la façon de mener une modélisation des menaces prévisibles à l'encontre des contrôles CIS au fur et à mesure que votre organisation les met en œuvre. La méthode suit la logique des cadres de sécurité formels et permet aux entreprises de « tracer une ligne » entre les risques qui sont en dessous de la ligne (« diligence raisonnable ») et ceux qui sont au-dessus de la ligne (et qui nécessitent un traitement des risques). Les organisations peuvent également utiliser la version de la méthodologie d'évaluation du risque CIS RAM appelée « Diligence raisonnable » afin d'obtenir une idée des risques si les contrôles ne sont pas mis en place, et ainsi évaluer les résultats potentiels. Consultez le manuel de la RAM. Il comprend des instructions complètes, des exemples, des modèles et des exercices afin de vous aider à effectuer une évaluation des risques en matière de cybersécurité.

Une autre ressource d'évaluation des risques que les entreprises peuvent envisager est celle du Centre canadien pour la cybersécurité, développée en partenariat avec l'équipe d'audit interne de la Bourse des valeurs canadiennes.

3. **Programme d'audit de la cybersécurité :** offre des outils gratuits à utiliser dans l'ordre : un tableau de bord, un guide d'audit, un outil d'enquête préliminaire et un programme d'audit. Tous ces outils s'adressent à toutes les organisations canadiennes. Aucune connaissance préalable en matière d'audit de sécurité informatique n'est requise pour utiliser ces outils. Plus de détails

4. **Fournisseurs de services tiers :** les organisations peuvent également engager une tierce partie afin qu'elle effectue des évaluations des risques et qu'elle mette en œuvre des mesures de sécurité pour protéger les actifs de l'entreprise. Les conseillers en évaluation des risques sont des experts compétents formés dans le domaine de l'atténuation et de la stratégie de risques.

La méthode d'évaluation des risques que vous choisirez dépendra, en dernier ressort, de vos ressources et de votre budget. Voici un résumé des outils à envisager selon votre groupe de mise en œuvre :

Outils	Groupe de mise en œuvre 1	Groupe de mise en œuvre 2	Groupe de mise en œuvre 3
CIS CSAT	X		
CIS RAM	X	X	X
Programme d'audit de la cybersécurité	X	X	
Conseiller en évaluation des risques		X	X

Enfin, même si vous disposez des plans d'évaluation les plus élaborés, il sera tout de même important d'investir également dans un régime d'assurance pour compléter votre stratégie de cybersécurité. L'assurance cybersécurité protège votre organisation contre les risques financiers potentiels associés aux cyberattaques (telles que les violations, les rançongiciels, les attaques par déni de service et les coûts associés aux enjeux de conformité aux normes).

PARTENAIRES COMMERCIAUX DE L'ÉFC

Ignite fournit des évaluations des risques personnalisées et des stratégies analytiques vous permettant de renforcer votre cyberrésilience. En savoir plus

Lawrie Insurance est un courtier indépendant qui rassemble des gestionnaires des risques certifiés qui pourront créer des plans afin de fournir à votre entreprise une couverture complète en matière de cybersécurité. En savoir plus

LA CYBERSÉCURITÉ EST UNE QUESTION DE COMMUNAUTÉ

Développer et déployer une stratégie de cybersécurité doit figurer parmi les priorités de toute organisation. Cette stratégie doit englober tous les employés d'une entreprise ainsi que tous les clients et partenaires faisant partie de la chaîne de valeur. Après tout, un plan stratégique de cybersécurité dépendra toujours de son maillon le plus faible. Par conséquent, la protection des systèmes et des réseaux d'entreprise ne peut s'accomplir qu'avec une collaboration et une communication qui s'étendent à l'ensemble du marché.

Aidez vos clients à demeurer toujours sur le bon chemin en matière de cybersécurité en partageant avec eux ce guide de ressources afin qu'ils puissent adopter une approche concrète de protection de leurs systèmes. Cela contribuera, par extension, à protéger vos propres données et actifs de réseau.

RESSOURCES

Vous trouverez ci-dessous des liens rapides vers des ressources abordées dans ce guide ainsi que des informations supplémentaires pour vous aider à lancer ou à renforcer votre stratégie de cybersécurité :

La bibliothèque des ressources en matière de cybersécurité de l'ÉFC

Centre canadien pour la cybersécurité

Conseil stratégique des DPI

CIS Center for Internet Security

Data Governance Institute

IBM : Rapport sur le Coût d'une violation de données (2021)

Commissariat à la protection de la vie privée du Canada : déclaration obligatoire des atteintes à la vie privée

Sécurité publique Canada

Pour toute question concernant ce guide de ressources, veuillez joindre **l'ÉFC à info@electrofed.com**