Les risques de cyberincident catastrophique – une préoccupation grandissante

CHUBB®

Les cyberincidents peuvent causer des pertes qui ne sont pas limitées dans le temps ou dans l'espace.

Alors que le numérique gagne du terrain à l'échelle mondiale, la fréquence, la gravité et la complexité des cyberincidents augmentent, tout comme la dépendance à l'égard de la technologie. Compte tenu de l'interconnectivité accrue, les vulnérabilités et les expositions se multiplient, ce qui crée des risques systémiques vastes, croissants et difficiles à détecter ou à contrôler. La combinaison de ces risques systémiques et de leurs conséquences potentiellement graves et généralisées est susceptible de générer une catastrophe.

À l'instar des pandémies, les cyberincidents peuvent causer des pertes qui ne sont pas limitées dans le temps ou dans l'espace. Nous ne sommes plus dans la théorie : les cybercriminels ont déjà prouvé leur capacité à perturber les chaînes d'approvisionnement des entreprises du monde entier et à paralyser les infrastructures essentielles, comme lors de la récente attaque qui a forcé Colonial Pipeline à fermer ses oléoducs approvisionnant la côte est des États-Unis. À la lumière des récents cyberincidents ayant causé des pertes économiques se chiffrant en milliards de dollars, il n'est pas difficile d'imaginer une cyberattaque catastrophique qui mettrait à l'épreuve la capacité financière du secteur de l'assurance.

Contrairement aux catastrophes soudaines survenues précédemment, les cyberrisques augmentent de manière continuelle. Ce préavis représente une occasion de mettre en place des mesures de cyberdéfense et de protection économique avant qu'une catastrophe se produise.

Cyberassurance : le début d'une nouvelle ère

La popularité croissante de la cyberassurance signifie que davantage d'entreprises sont protégées, mais aussi que l'agrégation des cyberrisques prend de l'ampleur pour le secteur de l'assurance.

Au cours des dernières années, la promesse de la cyberassurance a été pleinement réalisée. Les pertes couvertes par les assureurs à la suite de cyberincidents importants ont permis de protéger de nombreuses organisations du monde entier.

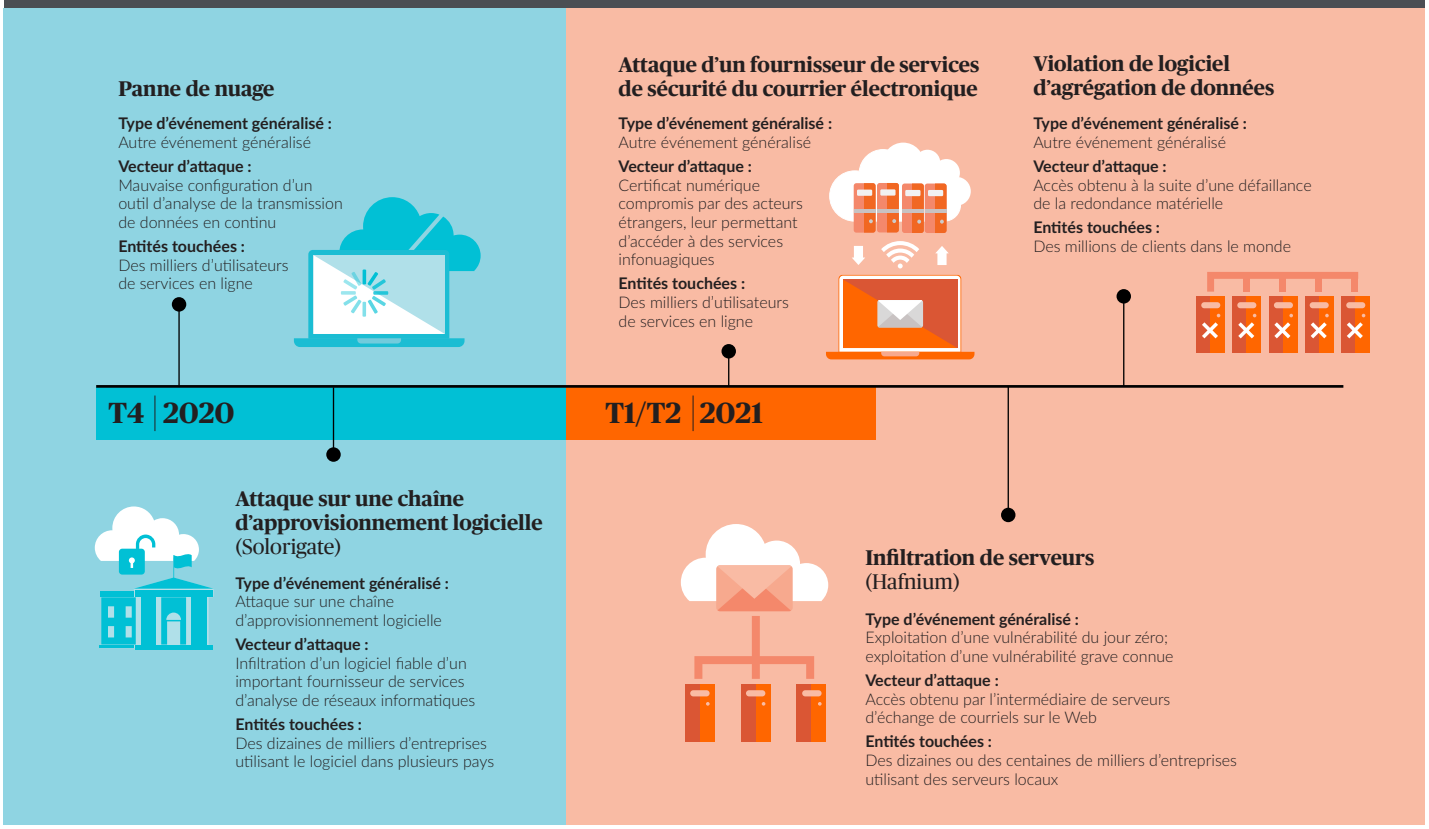
À l'heure actuelle, les garanties de base - frais d'intervention en cas d'incident, cyberrisques de première partie, cyberresponsabilité et responsabilité civile professionnelle/erreurs et omissions - fournissent d'importantes solutions de transfert et de gestion des risques aux organisations de toutes les tailles et de tous les secteurs d'activité. Qui plus est, les services de gestion des cyberrisques proposés par les assureurs aident les entreprises à réduire les risques et à améliorer leurs mécanismes de défense technologiques en amont, tandis que les équipes d'intervention en cas d'incident se révèlent efficaces pour rétablir plus rapidement la présence en ligne des entreprises à la suite d'un cyberincident.

La popularité croissante de la cyberassurance - selon un rapport du Government Accountability Office datant de mai 2021[1], le nombre de polices en vigueur serait actuellement de près de 4 millions pour les assureurs non agréés basés ou non aux États-Unis, et près de 50 % des entreprises américaines seraient couvertes - signifie que davantage d'entreprises sont protégées, mais aussi que l'agrégation des cyberrisques prend de l'ampleur pour le secteur de l'assurance.

Parallèlement, les entreprises ont également renforcé leur cyberrésilience au cours des dernières années. En 2020, 53 % des professionnels des TI et de la sécurité sondés à l'échelle mondiale ont déclaré que leur organisation avait atteint un niveau élevé de cyberrésilience, contre 35 % en 2015[2].

S'il est clair que la cyberassurance joue un rôle de plus en plus important dans la gestion des cyberrisques auxquels les organisations sont exposées, la capacité des assureurs à absorber la totalité du potentiel de perte à long terme est quant à elle incertaine.

La portée des cyberincidents est de plus en plus grande



Augmentation des risques et des répercussions

Sur une période de 100 jours, de décembre 2020 à mars 2021, plusieurs attaques majeures ont compromis une série de cibles, allant de la chaîne d'approvisionnement logicielle au fournisseur de services de sécurité du courrier électronique, en passant par les serveurs de données et les infrastructures municipales.

Malgré la prise de conscience des organisations à l'égard des cyberrisques et de leurs conséquences, les cyberincidents et les cybermenaces ne cessent d'augmenter et d'évoluer.

Plus de 18 000 nouvelles vulnérabilités logicielles ont été publiées en 2020, soit près de trois fois plus qu'en 2015, et leur nombre continue d'augmenter[3]. Parallèlement, près de 1,2 million de nouvelles menaces de logiciels malveillants ont été relevées en 2020, soit plus de deux fois le nombre recensé en 2015[4]. Parmi les atteintes à la sécurité réussies en 2020, 85 % comportaient un aspect humain, tel qu'un stratagème de fraude psychologique[5].

Alors que la fréquence et les coûts associés à l'adoption de tactiques telles que les rançongiciels ont augmenté, la compromission des courriels professionnels et les violations de données continuent de porter la fréquence des cyberincidents à des niveaux rarement atteints, surtout depuis que la pandémie de COVID-19 a frappé et que le travail à distance est devenu pratique courante.

Les conséquences des cyberincidents sont également plus importantes. Sur une période de 100 jours, de décembre 2020 à mars 2021, plusieurs attaques majeures ont compromis une série de cibles, allant de la chaîne d'approvisionnement logicielle au fournisseur de services de sécurité du courrier électronique, en passant par les serveurs de données et les infrastructures municipales. Plus de 100 000 organisations du monde entier ont été touchées par ces incidents.

Parmi les incidents recensés, on compte notamment Solorigate, une attaque massive de chaîne d'approvisionnement. Dans le cas de cette attaque, un code malveillant intégré à la mise à jour d'un logiciel d'analyse de réseaux fiable est passé inaperçu pendant près de huit mois, touchant environ 20 000 entreprises et organismes gouvernementaux.

Dans le cas d'une autre attaque, un regroupement d'acteurs étatiques et de groupes criminels présumés connu sous le nom de Hafnium a exploité une vulnérabilité alors inconnue (vulnérabilité « du jour zéro ») d'un logiciel commun pour possiblement accéder aux serveurs locaux de centaines de milliers d'entreprises.

Des incidents notoires font monter la tension

Ce n'est qu'une question de temps avant que nous soyons témoins d'un cyberincident catastrophique à la fois généralisé et destructeur.

Les attaques de Solorigate et de Hafnium ont touché de nombreuses organisations et entraîné des coûts importants, mais leurs conséquences auraient pu être bien pires. En effet, il semble que, dans les deux cas, l'objectif des cybercriminels ait été de faire de l'espionnage. Si toutefois leur intention avait été de voler ou de détruire des données sensibles ou d'autres renseignements, les conséquences économiques auraient aisément pu être décuplées. Selon Kevin Mandia, directeur général de la société de cybersécurité FireEye, qui a témoigné devant le comité du Renseignement du Sénat américain, les auteurs malveillants à l'origine de l'attaque Solorigate disposaient de l'accès et des capacités nécessaires pour causer de sérieux dommages[6].

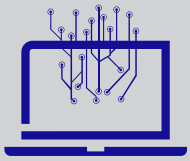
Voici un autre exemple. En 2017, l'attaque NotPetya a exploité un logiciel fiscal appelé M.E.Doc utilisé presque exclusivement en Ukraine. Le logiciel malveillant s'est ensuite propagé, allant toucher de nombreuses grandes entreprises basées en Europe, aux États-Unis et ailleurs, et causant des pertes estimées à 10 milliards de dollars. Certaines entreprises victimes de l'attaque NotPetya ont subi des pertes de plus de 100 M$. Si ce type de logiciel malveillant destructeur avait été déployé lors des attaques de Solorigate ou de Hafnium, les dommages financiers auraient pu être exponentiellement plus importants que ceux causés par NotPetya.

La même année, l'attaque par rançongiciel WannaCry a touché plus de 200 000 ordinateurs dans le monde. Heureusement, le rançongiciel exploitait une vulnérabilité connue pour laquelle il existait déjà un correctif, de sorte que la plupart des utilisateurs étaient protégés. Toutefois, comme dans l'exemple de Hafnium cité précédemment, les conséquences auraient pu être beaucoup plus graves si WannaCry avait plutôt exploité une vulnérabilité du jour zéro.

Jusqu'à présent, nous avons été témoins d'incidents de grande envergure (p. ex. Solorigate, Hafnium) et d'incidents destructeurs (p. ex. NotPetya, WannaCry), mais les pertes découlant de ces incidents ont toujours été gérables. Comme le potentiel de pertes est immense et qu'il ne cesse de grandir, ce n'est qu'une question de temps avant que nous soyons témoins d'un cyberincident catastrophique à la fois généralisé et destructeur.

Risques de cyberincident catastrophique

La dépendance croissante des organisations et des consommateurs à l'égard de la technologie ainsi que l'interconnectivité des technologies et des partenaires ont entraîné la création d'un environnement au sein duquel la gravité des conséquences des cyberincidents peut augmenter de façon exponentielle. Les types d'incidents suivants ont le potentiel d'être catastrophiques, surtout en cas de combinaison.



Exploitation d'une vulnérabilité grave connue

En moyenne, environ 50 nouvelles vulnérabilités logicielles sont publiées chaque jour. Si aucun correctif n'est appliqué, ces vulnérabilités peuvent être exploitées. Environ 15 % d'entre elles sont graves, c'est-à-dire qu'elles sont faciles à exploiter, qu'elles peuvent être déployées à distance au moyen de privilèges d'accès limités et qu'elles ont des conséquences négatives importantes[7]. Comme les vulnérabilités graves sont largement connues et qu'elles peuvent être détectées sur les réseaux des victimes potentielles grâce à des techniques courantes de balayage sur Internet, les entreprises qui omettent de remédier aux vulnérabilités logicielles graves s'exposent à un risque élevé.

Exploitation d'une vulnérabilité du jour zéro

Les vulnérabilités logicielles du jour zéro ne sont connues que des cybercriminels. Ces vulnérabilités sont particulièrement préoccupantes, car certaines sont facilement exploitables, peuvent avoir de graves conséquences et ne font pas l'objet de mesures de protection. Autrement dit, même les entreprises dotées de programmes de gestion des cyberrisques efficacement gérés peuvent être exposées à des attaques du jour zéro.

Attaques sur une chaîne d'approvisionnement logicielle

Les attaques sur une chaîne d'approvisionnement logicielle permettent à des individus malveillants d'accéder à des systèmes au moyen de logiciels de confiance certifiés et d'y introduire un cheval de Troie. L'attaque de Solorigate a mis en lumière le niveau de sophistication élevé des adversaires en ce qui a trait à l'exploitation de pratiques de développement de logiciels courantes utilisées au sein du secteur des technologies. Ces attaques, dont bon nombre semblent être dirigées ou parrainées par des acteurs étatiques, devraient se poursuivre, voire s'accélérer. En effet, les frictions géopolitiques, en particulier entre l'Occident et ses adversaires, continueront d'alimenter la menace de tels incidents.

Pannes d'infrastructure

Les attaques et autres cyberincidents touchant des infrastructures peuvent avoir des conséquences considérables. Par exemple, lors de l'attaque de mai 2021 contre Colonial Pipeline, la société d'approvisionnement en essence qui sert la côte est des États-Unis, des cybercriminels étrangers ont forcé la fermeture d'une infrastructure en lançant une attaque par rançongiciel, aggravant ainsi les dommages causés. L'oléoduc a ainsi dû être fermé pendant plusieurs jours, ce qui a provoqué des pénuries d'essence touchant 45 % de l'approvisionnement en carburant de millions de citoyens et d'entreprises dans plusieurs États. Le risque de panne d'infrastructure est unique en ce sens qu'il peut résulter d'une cyberattaque, mais aussi de défaillances d'un système, d'erreurs humaines, d'erreurs de programmation ou d'autres types de cyberévénements non malveillants.

Autres événements généralisés

Certains types de cyberattaques peuvent être menés contre un grand nombre de victimes de façon simultanée ou automatique. Internet et certains services de télécommunications se sont élevés au rang d'infrastructures sociétales d'importance critique, ce qui accroît considérablement le risque de défaillance. Dans certains cas, il arrive qu'une entreprise de télécommunication soit le seul fournisseur d'une grande ville ou d'une ville de taille moyenne. Dans d'autres cas, l'utilisation de certaines grandes entreprises d'informatique en nuage est si répandue qu'une panne généralisée aurait des conséquences sur les activités de milliers voire de millions d'entreprises différentes en même temps. Toute attaque de ce type pouvant être déployée à grande échelle est susceptible de provoquer un cyberincident catastrophique.

Incidents de rançongiciels

Bien qu'elles ne soient pas nécessairement de nature catastrophique, les attaques par rançongiciel, qui consistent à prendre en otage les fichiers électroniques ou les renseignements d'une organisation ou d'une personne jusqu'à ce qu'une somme d'argent soit versée, sont désormais menées avec une efficacité industrielle. Alors que les montants demandés se chiffraient au départ en milliers de dollars, ils atteignent maintenant les dizaines de millions, les criminels ciblant des organisations de toutes les tailles.

Renforcer la cyberrésilience

Il est plus que jamais essentiel pour les organisations de se préparer efficacement en vue d'un potentiel cyberincident catastrophique.

Compte tenu de l'augmentation des cyberrisques - que ce soit en raison de la nature des activités et des environnements informatiques, de la défaillance des infrastructures communes ou de l'exploitation des vulnérabilités par des individus malveillants - il est plus que jamais essentiel pour les organisations de se préparer efficacement en vue d'un potentiel cyberincident catastrophique.

Pour ce faire, les organisations peuvent commencer par s'efforcer de comprendre les risques particuliers auxquels elles sont exposées à la lumière des cyberincidents catastrophiques potentiels décrits dans le présent document, puis tirer parti des ressources nécessaires pour améliorer leurs cyberdéfenses et leur cyberrésilience. Les fournisseurs de services informatiques partagés représentent un risque systémique important pour les organisations. Il convient donc de procéder à une vérification diligente approfondie de ces fournisseurs et d'établir une redondance et une résilience autour d'eux, en plus d'examiner les modalités relatives à l'indemnisation dans les contrats afin d'évaluer la manière dont le risque est transféré.

Les organisations devraient également tirer pleinement parti de l'expertise offerte par leur courtier ou agent d'assurance et par leur fournisseur de cyberassurance. Bien que les équipes des TI, de la gestion des risques et de la continuité des activités puissent avoir confiance en leurs mesures de cyberprotection et d'intervention en cas d'incident, aucune organisation ne peut se protéger entièrement contre tous les cyberincidents potentiels, en particulier les cyberincidents catastrophiques.

De nombreux assureurs proposent une gamme de services de préparation aux incidents pour aider les organisations à renforcer leur cyberdéfense, notamment l'évaluation de la rapidité d'intervention, l'analyse comparative des performances de sécurité, les tests de vulnérabilité du réseau et la simulation d'attaques courantes. Les organisations doivent également être prêtes à réagir en cas de cyberincident. L'équipe d'experts en intervention en cas d'incident d'un assureur peut contribuer à limiter les dommages causés par de tels événements et aider les organisations à reprendre leurs activités dans les plus brefs délais. Ces services peuvent faire la différence entre la simple capacité à survivre à un cyberincident majeur et l'aptitude à affronter l'avenir en toute confiance.

Faire avancer les solutions

Tout comme l'assurance des biens, la cyberassurance est associée à des risques d'événements catastrophiques.

D'un point de vue mondial, un cyberincident catastrophique pourrait entraîner l'interruption du commerce et paralyser les infrastructures essentielles. Comme dans le cas de la pandémie de COVID-19, les secteurs public et privé devront se pencher ensemble sur des sujets importants, notamment la divulgation et le signalement des cyberincidents aux fins d'amélioration de l'uniformité des données, ainsi que la mise en place de cadres juridiques pour dissuader et punir les cybercriminels.

L'augmentation de la fréquence et de la gravité des cyberincidents pousse les assureurs à revoir leur tarification et leurs conditions. Pour assurer la stabilité du marché de la cyberassurance tout en tenant compte de l'ampleur potentielle des risques catastrophiques, il faudra trouver de nouvelles solutions, par exemple un partenariat avec le gouvernement, et apporter des modifications aux produits d'assurance proposés. Pour le secteur de l'assurance, le défi consiste à mettre en place des polices qui procurent une certitude en matière de couverture et une protection pertinente, en plus de contribuer à la gestion des cyberincidents, qu'il s'agisse de cyberincidents sur attrition ou catastrophiques, pour les clients et les assureurs.

Les assureurs ont toujours assuré les biens contre les événements catastrophiques, tels que les inondations et les tremblements de terre, au titre d'une couverture distincte pour pouvoir établir une tarification transparente et surveiller ces risques. Cette façon de procéder a contribué à assurer la stabilité globale du marché et la disponibilité de la couverture. Par exemple, bien que les tremblements de terre, les inondations et les ouragans importants survenus au cours des cinquante dernières années aient été coûteux pour le secteur de l'assurance de dommages, ils ont rarement entraîné l'insolvabilité des compagnies d'assurance. Ainsi, le secteur de l'assurance est resté résistant et stable pour les titulaires de police, même après des événements catastrophiques.

Tout comme l'assurance des biens, la cyberassurance est associée à des risques d'événements catastrophiques. Ainsi, le secteur de la cyberassurance pourrait devoir réagir de la même manière que le secteur de l'assurance des biens. Le secteur doit se montrer proactif en offrant une couverture distincte pour les événements catastrophiques. La couverture des événements catastrophiques ne serait pas exclue, mais plutôt mieux définie, pour que la couverture distincte fasse l'objet d'une tarification transparente, en plus de comprendre une souscription appropriée, des montants de garantie adéquats et des stratégies de fidélisation de la clientèle. Cette approche permettra au secteur de la cyberassurance de continuer à fournir des solutions novatrices aux titulaires de police tout en assurant la viabilité à long terme du marché.

À propos de l'auteur

Michael Kessler est vice-président, Groupe Chubb et président de division, Cyberrisques mondiaux, de Chubb. À ce titre, il supervise tous les aspects du domaine, notamment la stratégie, le développement des produits et des affaires, les activités de souscription et de service, ainsi que les résultats globaux. M. Kessler possède près de 30 ans d'expérience dans le domaine de l'assurance et de l'actuariat-conseil. Il a auparavant occupé les fonctions de chef de la réassurance de Chubb (de 2016 à 2021) et d'actuaire en chef pour ses activités d'assurance à l'échelle internationale (de 2008 à 2016). M. Kessler est titulaire d'un baccalauréat ès arts en mathématiques de l'Université Cornell. Il est membre de l'American Academy of Actuaries et Fellow de la Casualty Actuarial Society.

Notes de fin

1. Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (2021) (en anglais seulement). Consulté à l'adresse www.gao.gov/products/gao-21-477
2. Cyber Resilient Organization Report (2020) (en anglais seulement). Consulté à l'adresse www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Vulnerability Database du National Institute of Standards and Technology (en anglais seulement). Accessible à l'adresse https://nvd.nist.gov/vuln/search
4. Institut AV-TEST (2021). Accessible à l'adresse www.av-test.org/fr/statistiques/logiciels-malveillants/
5. Rapport d'enquête 2021 de Verizon sur la compromission des données (2021) (en anglais seulement). Consulté à l'adresse https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. Comité spécial sur le renseignement du Sénat américain (2021) (en anglais seulement). Accessible à l'adresse www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021) (en anglais seulement). Consulté à l'adresse www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

À propos de Chubb

Chubb est le plus important groupe d'assurance IARD coté en bourse du monde. Présente dans 54 pays et territoires, Chubb offre des assurances de dommages aux particuliers et aux entreprises, des assurances individuelles contre les accidents, des assurances maladie complémentaires pour les particuliers, ainsi que de la réassurance et de l'assurance vie à une grande variété de clients. En tant que souscripteurs, nous évaluons, gérons et assumons les risques avec perspicacité et rigueur. Nous réglons les dossiers et indemnisons les clients équitablement et rapidement. Nous sommes également réputés pour notre large éventail de produits et services, notre vaste capacité de distribution, notre stabilité financière exceptionnelle, en plus de notre présence locale à travers le monde. Chubb Limited, la société mère de Chubb, est cotée à la bourse de New York (NYSE : CB) et est incluse dans l'indice S&P 500. Les bureaux de direction de Chubb se trouvent à Zurich, New York, Londres, Paris et ailleurs. À l'échelle mondiale, la société compte plus de 30 000 employés. D'autres renseignements sont accessibles au chubb.com/ca-fr.

Pour en savoir plus sur l'expérience et l'expertise de Chubb en matière de gestion des cyberrisques, consultez le site www.chubb.com/ca-fr/ ou envoyez un courriel à l'adresse cyber@chubb.com.

Chubb. Insured.℠