Se préparer à l'imprévu – Tendances et tactiques en continuité des activités et sécurité de l'information

AOÛT 2018

Par Kevin Kondo
vice-président adjoint,
Sécurité de l'entreprise

Kevin Kondo est vice-président adjoint, Sécurité de l'entreprise à CIBC Mellon. M. Kondo supervise le programme de continuité de l'exploitation et de reprise des activités en cas de sinistre, en plus de gérer les programmes de sécurité de l'information de CIBC Mellon. Il compte plus de 15 ans d'expérience dans le secteur canadien des services financiers.

Les incidents technologiques qui nuisent aux activités d'exploitation sont largement relayés par les médias et, au pays comme ailleurs, touchent les entreprises de plus en plus fréquemment dans notre monde interconnecté et numérique. Les investisseurs institutionnels, les autorités de réglementation et les parties prenantes, à l'échelle du secteur des services financiers et d'autres segments du secteur, veulent s'assurer que leurs fournisseurs et partenaires ont mis en place des processus pour atténuer les répercussions d'incidents imprévus, de perturbations et de menaces aux services essentiels.

En tant que gardiens d'actifs d'une valeur totale de plus de 1 900 milliards de dollars pour le compte de banques, de caisses de retraite, de fonds communs de placement, de sociétés et d'autres investisseurs institutionnels, nous reconnaissons l'importance de notre résilience pour nos clients. C'est pourquoi nous travaillons en permanence à la consolidation de notre cadre de gouvernance et de contrôle. Il nous faut surmonter des défis inattendus de manière rapide, organisée et efficace pour continuer à fournir nos services et nos solutions à nos clients.

TENDANCES EN CONTINUITÉ DES ACTIVITÉS ET SÉCURITÉ DE L'INFORMATION

Le Business Continuity Institute (BCI) est un organisme de premier plan regroupant des membres internationaux et offrant un programme de certification au profit des professionnels de la continuité des activités à travers le monde. Il produit un rapport annuel d'analyse prospective, qui fait le point sur les risques et menaces auxquels les organisations sont exposées en évaluant les menaces perçues, selon l'évaluation menée à l'interne par des professionnels en exercice. Son plus récent sondage, mené auprès de 657 organisations dans 76 pays, lui a permis de dégager plusieurs tendances majeures.

DIX PRINCIPALES MENACES POUR LA CONTINUITÉ DES ACTIVITÉS – ANALYSE PROSPECTIVE DU BCI POUR 2018

1. Cyberattaque
2. Violation de données
3. Interruption de service non planifiée des systèmes d'information et de télécommunication
4. Interruption des services publics
5. Conditions météorologiques défavorables
6. Acte de terrorisme
7. Incident de sécurité
8. Incendie
9. Perturbation de la chaîne d'approvisionnement
10. Perturbation du réseau de transport

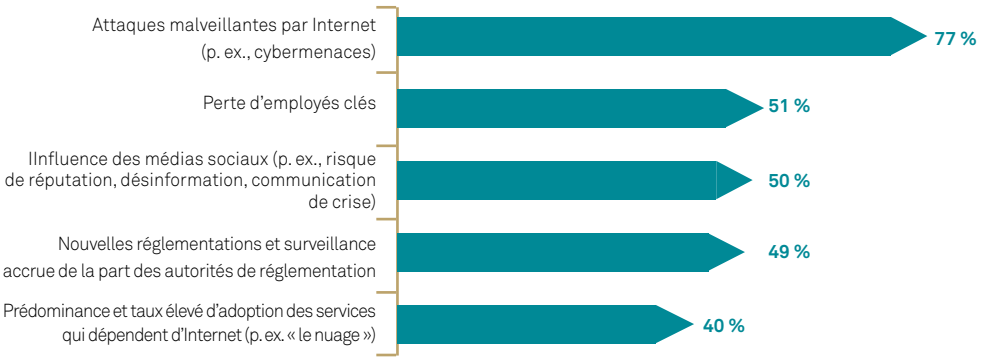
La technologie demeure en tête des préoccupations des répondants. Les événements récents comme la découverte des vulnérabilités Meltdown et Spectre rendue publique en janvier 2018 et l'attaque du logiciel rançonneur WannaCry survenue en mai 2017 ont placé la cyberrésilience et la sécurité de l'information au centre des préoccupations des organisations du monde entier.

CIBC MELLON

Nous comprenons que les cyberattaques et les violations de données soient une préoccupation majeure pour les organisations. Toutefois, on observe d'autres types de perturbations, plus fréquentes, à savoir les interruptions de service non planifiées des systèmes d'information et de télécommunication et les interruptions de services publics. En fait, il est probable que les systèmes d'information et de télécommunication de votre organisation subissent des interruptions de service non planifiées, d'une manière ou d'une autre, chaque semaine.

Cinq principales tendances et incertitudes, et mesures prises par CIBC Mellon

Ces cinq tendances et incertitudes ont été citées par plus de la moitié des répondants lors du sondage mené par BCI et trouveront probablement un large écho auprès des investisseurs institutionnels.



1. ATTAQUES MALVEILLANTES PAR INTERNET

Lors des sondages menés par le BCI en 2016, 2017 et 2018, les répondants ont placé tout en haut de leur liste de préoccupations les cyberattaques et la violation de données. Les professionnels continuent de craindre les dommages potentiels d'une cyberattaque ou d'une violation de données, sachant que les éléments hostiles ne cessent de se perfectionner.

Alors que se poursuit l'avancée vers l'interconnexion, le numérique et les technologies, les organisations continuent de placer la gouvernance des TI, la sécurité et la préparation au centre de leurs préoccupations. Des processus internes à la gestion des fournisseurs, en passant par la sensibilisation des employés, il est important que les organisations demeurent vigilantes et œuvrent à l'amélioration continue des mesures de contrôle et de sécurité mises en place pour leur propre protection et celle des parties prenantes, ainsi que de l'information placée sous leur contrôle.

La planification, la documentation et la réponse d'une organisation à un problème dépendront considérablement de la capacité de ses équipes à réagir rapidement et efficacement.

2. PERTE D'EMPLOYÉS CLÉS

Le « facteur humain », comme une pénurie de main-d'œuvre qualifiée ou la perte d'employés clés, peut avoir des répercussions sur le rendement d'une entreprise et nécessite une intervention stratégique. L'essor de toute entreprise dépend de collaborateurs clés et cet aspect est crucial pour la gestion de la continuité des activités.

Nous reconnaissons la contribution essentielle des employés à la continuité des activités. À CIBC Mellon, chaque unité d'exploitation est dotée d'un coordonnateur chargé de la planification de la reprise des activités et d'un remplaçant, qui collaborent avec l'équipe de la continuité des activités de la société pour évaluer et documenter ses besoins et ses programmes en la matière. Les programmes englobent un large éventail de facteurs, notamment la détermination des fonctions opérationnelles qui sont critiques et nécessitent une attention immédiate et des fonctions plus générales, moins prioritaires en cas de problème lié à la continuité des activités. Qu'il s'agisse du travail à distance, des sites de repli ou des exigences techniques et de connectivité liées aux fonctions et tâches de chaque employé, chaque équipe documente ses besoins, ce qui nous permet de planifier, maintenir et déployer les capacités critiques en cas d'incident.

3. INFLUENCE DES MÉDIAS SOCIAUX

L'influence croissante des médias sociaux, surtout en ce qui concerne la réputation des entreprises, occupe le troisième rang, cette année, puisque 50 % des répondants la considèrent comme une menace majeure. Outre les préoccupations liées à la réputation et à l'image de marque des entreprises, les médias sociaux présentent des risques en ce qui a trait au respect des exigences juridiques et réglementaires, à la sécurité des données et à la protection des renseignements personnels, ainsi qu'aux questions relatives aux ressources humaines.

Les médias sociaux ne représentent pas que des défis. Ils permettent aussi aux organisations de rester à l'affût des menaces et défis potentiels et peuvent servir de moyen de communication lorsqu'un événement se produit. À CIBC Mellon, nous utilisons également les médias sociaux pour mettre en avant la qualité de notre milieu de travail, ce qui nous permet de recruter de brillants collaborateurs et d'alimenter un solide bassin de talents afin de gérer le roulement du personnel naturel auquel toute organisation doit faire face.

4. NOUVELLES RÉGLEMENTATIONS ET SURVEILLANCE ACCRUE DE LA PART DES AUTORITÉS DE RÉGLEMENTATION

Aujourd'hui, les participants au marché des services financiers accordent beaucoup d'attention au respect des exigences des divers organismes sectoriels et autorités de réglementation du Canada. Qu'il s'agisse des lignes directrices des Autorités canadiennes en valeurs mobilières (ACVM) ou des exigences relatives à la conservation de dossiers de la Commission des services financiers de l'Ontario (CSFO), les organisations font face à un resserrement des exigences réglementaires, qui vise à rassurer les clients concernant les risques pour la continuité des activités et la capacité des organisations à les gérer adéquatement. Dans cette optique, CIBC Mellon fournit à ses clients des rapports détaillés sur les mesures de contrôle, les pratiques et les efforts de gouvernance et leur donne un aperçu des mesures prises par CIBC Mellon pour assurer la continuité des activités.

5. PRÉDOMINANCE ET TAUX ÉLEVÉ D'ADOPTION DES SERVICES QUI DÉPENDENT D'INTERNET

La gestion des risques liés aux services par Internet passe par un examen approprié des prestataires de services. Important pour la sélection et le recrutement des fournisseurs, cet examen est également impératif pendant toute la durée de la relation d'affaires. L'engagement des fournisseurs peut prendre bien des formes : plusieurs centres de données redondants, procédure détaillée de reprise après sinistre (ou de continuité des services) et normes élevées en matière de sécurité de l'information.

CIBC Mellon table sur les infrastructures puissantes et robustes de CIBC et de BNY Mellon, ainsi que sur des processus étendus de gestion des fournisseurs pour consolider la confiance à l'égard des services impartis. Nous évaluons avec soin nos fournisseurs pour confirmer qu'ils se conforment bien à nos normes, et nous nous appuyons sur l'expertise et l'envergure de nos deux sociétés mères pour surveiller l'environnement informatique. Tous nos employés bénéficient d'une formation annuelle détaillée portant sur la sécurité de l'information. De plus, nous assurons un suivi permanent des menaces émergentes.

Pour bien gérer la continuité des activités, vous devez planifier et préparer la continuité opérationnelle de votre entreprise en cas d'incidents graves et de sinistres, ainsi que le rétablissement des conditions d'exploitation normales dans un délai raisonnablement court.

Éléments à considérer pour une gestion robuste et résiliente de la continuité des activités

EXAMINER LES SCÉNARIOS

Les événements qui ont une incidence sur la continuité des activités sont très divers. Comme le montre le sondage de BCI, les entreprises ont tendance à se concentrer sur les incidents technologiques, étant donné le monde interconnecté dans lequel elles évoluent. Il est toutefois important d'examiner toute une gamme de situations possibles pour s'y préparer. Nous présentons ci-dessous les trois grandes catégories d'incidents à prendre en compte.

TECHNOLOGIE

Exemples d'incidents technologiques :

- Panne d'un système essentiel ou du réseau
- Panne du réseau de télécommunication
- Perte de prestataires de services et de fournisseurs (impartition), par exemple un fournisseur TI
- Panne des infrastructures techniques, comme un logiciel, un élément de matériel, une base de données ou les services bancaires en ligne
- Panne d'électricité due aux conditions météorologiques

Exemple de scénario : La rigueur de l'hiver canadien peut causer des pannes d'électricité, des perturbations de l'approvisionnement et des risques pour la sécurité pouvant mettre des vies en danger et empêcher l'accès à des infrastructures essentielles. Il est possible de prévoir bien à l'avance la marche à suivre en cas d'événements de ce type. La planification devrait consister notamment à :

- Former et sensibiliser, en particulier aux procédures et au trajet d'évacuation
- Coordonner les activités avec les équipes d'intervention locales et gouvernementales
- Communiquer les trajets d'évacuation recommandés
- Fournir les trousses d'urgence
- Suivre les bulletins à la radio et/ou à la télévision
- Sécuriser les locaux
- Sauvegarder et mettre en sécurité les fichiers électroniques critiques

FINANCES

Un événement susceptible de nuire à la continuité des activités peut avoir des répercussions financières, mais il est possible de se préparer à certains scénarios :

- Bénéfice inférieur aux prévisions
- Rétablissement des gains
- Baisse des cours boursiers
- Perte de clients
- Turbulence des marchés
- Troubles sociopolitiques

Exemple de scénario : Amorcées en 2017 et se poursuivant en 2018, les négociations de l'ALENA et d'autres accords commerciaux internationaux ont créé des tensions grandissantes. Le Dow et le Nasdaq ont subi les effets des changements et de l'adoption de tarifs douaniers entre les États-Unis et l'UE, le Canada, le Mexique et la Chine, entre autres. En fait, selon un article de CNNMoney[1], le Dow a chuté de 400 points et le Nasdaq a perdu 2 % lorsqu'il a été annoncé que le président Trump prévoyait s'attaquer aux investissements chinois visant des technologies stratégiques aux États-Unis. Même si beaucoup d'incertitude persiste à cet égard, c'est un scénario qui exige une soigneuse préparation et une réflexion, pour que votre entreprise soit en mesure de réagir efficacement.

ATTEINTE À LA RÉPUTATION

Il semblerait que le risque de réputation soit fréquemment ignoré des organisations. Pourtant, il peut souvent entraîner une perte de revenus, une hausse des coûts d'exploitation ou des coûts liés à la réglementation, une baisse de la valeur actionnariale, voire une enquête criminelle. La réputation peut aussi être entachée lorsqu'un des scénarios décrits ci-dessus n'est pas géré efficacement. Exemples d'événements portant atteinte à la réputation et pouvant nuire à la continuité des activités :

- Activité illégale
  - Extorsion
  - Corruption
  - Fraude
  - Enquête criminelle
- Manquement de la part d'un employé

Il est possible d'atténuer les dommages causés en organisant une riposte. Selon le Business Continuity Institute[2], la transparence est la meilleure approche. En misant sur la transparence auprès des parties prenantes, l'organisation renforce la confiance et montre qu'elle est en mesure de reprendre ses activités et d'opérer un retour à la normale après un incident.

INSISTER SUR LA MOBILISATION ET LE SUIVI

Pour que l'entreprise se prépare adéquatement à tout incident éventuel, il est important de nommer un responsable qui fera activement valoir l'incidence des événements liés à la continuité des activités sur l'exploitation, l'expérience des employés et des clients et, potentiellement, les résultats de l'entreprise. Un suivi régulier des incidents, mineurs et majeurs, permet d'en déterminer la fréquence, ainsi que les avantages d'être préparé.

VÉRIFICATION PAR UN TIERS

Pour donner suite à l'examen de scénarios, le recours à des intervenants externes spécialisés dans la continuité des activités peut aider votre société à détecter les occasions, à renforcer vos programmes et à attester de votre niveau de préparation auprès des autorités, des clients (potentiels ou existants) et des autres parties prenantes ayant un rôle essentiel dans votre secteur. La certification ISO 22301 en est un exemple. Organisme de normalisation mondialement reconnu, l'ISO aide plus de 80 000 clients situés dans 182 pays à comprendre, évaluer et élaborer de nouvelles normes pour accroître leur rendement dans des situations très diverses. L'ISO offre toute une gamme de certifications, allant de la gestion de l'énergie à la santé et la sécurité au travail. Les deux normes applicables à la continuité des activités et à la sécurité de l'information sont l'ISO 22301 et l'ISO 27001, respectivement.

CIBC Mellon est certifiée ISO 22301 et ISO 27001. Tiré du rapport d'analyse prospective du BCI, le tableau ci-dessous montre qu'un nombre croissant d'organisations obtiennent la certification ISO 22301.

Année	Certification ISO 22301
2016	51 %
2017	63 %
2018	70 %

INCLURE LES PARTENAIRES, LES FOURNISSEURS ET LES TIERS

Au moment d'élaborer vos programmes de gestion de la continuité des activités et les efforts entourant la sécurité de l'information, il est important de tenir compte des partenaires, fournisseurs et tierces parties qui font partie de votre entreprise élargie. Ils sont souvent une extension de vos activités d'exploitation et en cas d'incident, leur capacité à réagir et à rétablir leurs activités dans les meilleurs délais est tout aussi importante. Veuillez lire la section ci-après, qui présente plusieurs questions essentielles à poser pour évaluer le niveau de préparation des fournisseurs.

GESTION À L'INTERNE

Vos employés sont votre première ligne de défense. Ils peuvent participer à la détection de situations potentiellement graves dans le cadre de leurs activités quotidiennes, mais ils sont aussi votre porte d'entrée la plus vulnérable. Une sensibilisation continue, comprenant une formation approfondie et un partage régulier des connaissances, est essentielle pour doter vos employés de l'information nécessaire à la protection de l'intégrité de vos activités quotidiennes. La section sur les tendances et incertitudes présentée plus haut examine des éléments clés du point de vue de la continuité des activités.

La planification, la documentation et la réponse d'une organisation à un problème dépendront considérablement de la capacité de ses équipes à réagir rapidement et efficacement.

CYBERSÉCURITÉ ET GESTION DES DONNÉES

CIBC Mellon est bien placée, grâce au soutien de deux chefs de file mondiaux du secteur des services financiers, CIBC et BNY Mellon, qui attachent beaucoup d'importance à la cybersécurité. CIBC Mellon, CIBC et BNY Mellon surveillent l'environnement des TI, à l'affût de menaces potentielles et d'éléments préoccupants. Elles s'emploient à renforcer leurs mesures de sécurité et de gouvernance.

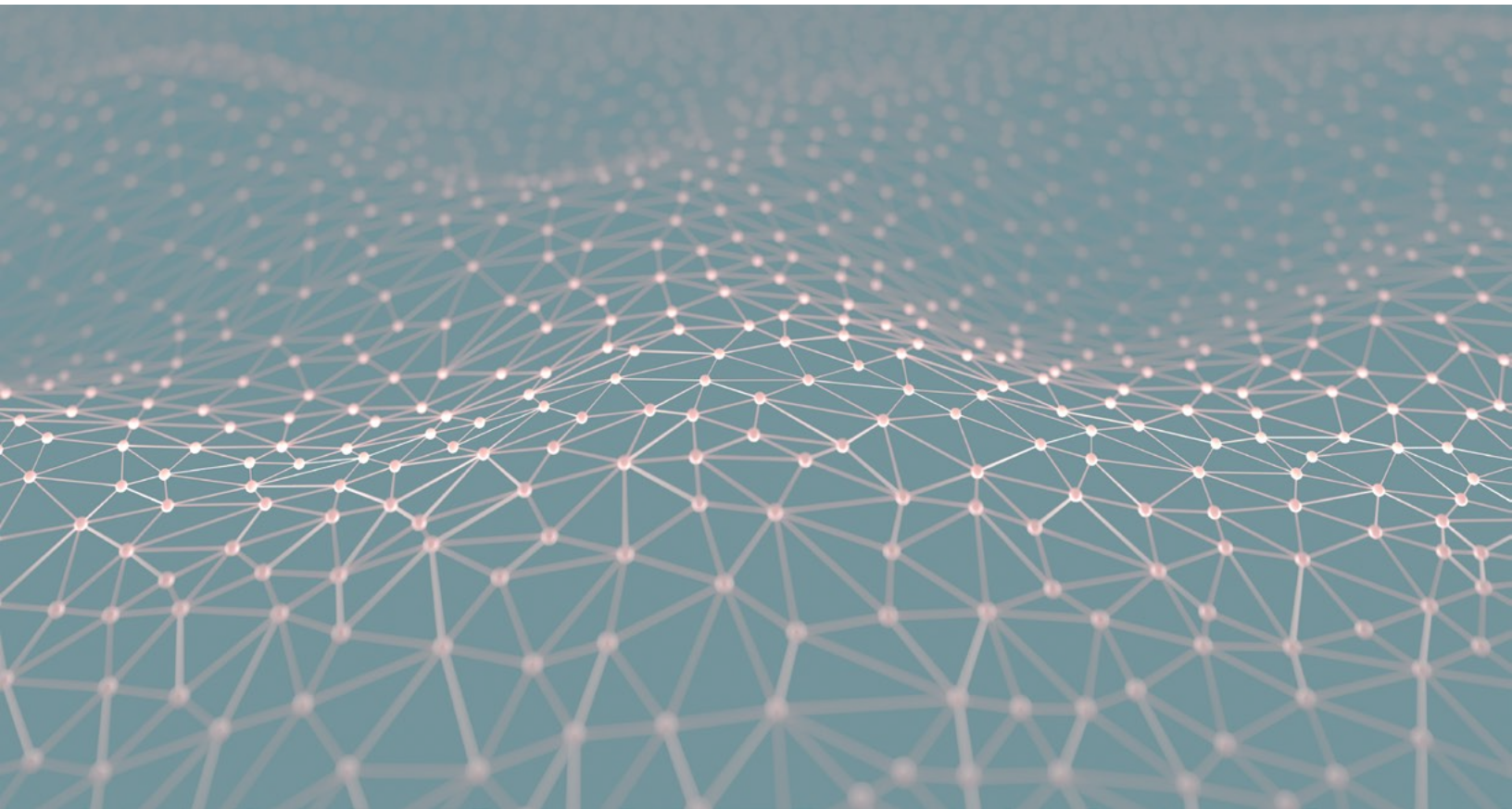
CIBC Mellon et ses sociétés mères disposent de plusieurs niveaux de protection liés aux technologies de l'information. En outre, elles ont mis en place – et s'emploient à renforcer en permanence – un large éventail de mesures de sécurité pour protéger notre société, nos clients, nos employés et l'information placée sous notre contrôle. Nous recevons régulièrement de l'information sur les menaces potentielles de la part de nos pairs et du reste du secteur des services financiers, ainsi que de la part de nos clients, des forces de l'ordre et de diverses sources, publiques et privées. CIBC Mellon et ses sociétés mères surveillent et analysent nos environnements informatiques pour détecter les vulnérabilités et menaces potentielles. Elles continuent d'investir dans des moyens de protection et de les mettre en œuvre si elles le jugent nécessaire.

À CIBC Mellon, nous intervenons régulièrement auprès des employés afin de les sensibiliser aux mesures à prendre pour protéger la société, ses clients et l'information placée sous son contrôle, dont le signalement des tentatives d'hameçonnage et le renforcement des contrôles entourant le traitement de l'information. Nous savons que la diligence des employés et leur connaissance des pratiques exemplaires sont essentielles au maintien de contrôles solides.

GOUVERNANCE RELATIVE AUX FOURNISSEURS

CIBC Mellon s'est dotée d'un programme de gouvernance relative aux fournisseurs, en vertu duquel elle assure un suivi de ses fournisseurs externes. Ce programme prévoit la documentation, ainsi que la responsabilisation des fournisseurs relativement à des critères de rendement au moyen de contrôles préalables et d'obligations de divulgation de l'information. Dans le cas des fournisseurs dont les services sont jugés critiques pour CIBC Mellon (notamment dans le domaine des TI), nous appliquons des contrôles et un suivi supplémentaires pour obtenir l'assurance que les risques associés à nos fournisseurs et à notre chaîne d'approvisionnement sont gérés conformément aux exigences de CIBC Mellon. Cela s'inscrit dans notre démarche d'excellence en matière de gouvernance et d'exploitation.

CIBC Mellon et ses sociétés mères disposent de plusieurs niveaux de protection liés aux technologies de l'information. En outre, elles ont mis en place – et s'emploient à renforcer en permanence – un large éventail de mesures de sécurité pour protéger notre société, nos clients, nos employés et l'information placée sous notre contrôle.



QUESTIONS IMPORTANTES

Questions importantes en matière de continuité des activités

- Votre organisation dispose-t-elle d'un processus actif et à jour pour la continuité des activités?
- Quels sont les engagements prioritaires pris par votre organisation envers ses clients et parties prenantes concernant ses activités ou services?
- Comment les programmes de continuité des activités et les besoins en la matière sont-ils documentés par votre organisation?
- Comment votre organisation compte-t-elle communiquer avec ses employés, ses clients et les autres parties prenantes durant une urgence ou une crise?
- En combien de temps êtes-vous en mesure de joindre les employés en dehors des heures normales de travail?
- Quels sont les dépendances, technologies et systèmes critiques de votre organisation?
- Qui sont vos employés clés?
- Qui sont vos fournisseurs essentiels et quelles mesures avez-vous prises pour vous assurer et donner à vos parties prenantes l'assurance que ces fournisseurs sont prêts à faire face à une perturbation?
- Quelles dispositions réglementaires et exigences du conseil d'administration ou des parties prenantes en matière de divulgation de l'information votre organisation doit-elle respecter pour assurer la continuité des activités?

Suggestions de questions à poser aux fournisseurs

- Avez-vous un processus actif et à jour pour la gestion de la continuité des activités?
  - Si oui, en quoi consiste-t-il?
- Quelles mesures avez-vous prises pour protéger mes données?
- Chiffrez-vous vos données?
- Comment sécurisez-vous les transferts de données?
- En tant que client, comment et quand serai-je avisé d'un incident?
- Qui sont les employés clés chargés de mon compte et quelles sont leurs coordonnées?
- Qui sont vos fournisseurs critiques et quelles mesures avez-vous prises pour vous assurer et donner à vos parties prenantes l'assurance que ces fournisseurs sont prêts?
- Quelles certifications, réglementations et/ou mesures utilisez-vous pour mesurer votre niveau de préparation aux incidents?
- Comment tenez-vous vos employés informés de l'évolution des processus de continuité des activités, des procédures de cybersécurité et d'autres questions connexes, et comment les préparez-vous? Quelles politiques avez-vous mises en place?

Les efforts déployés par CIBC Mellon en matière de continuité des activités et de sécurité de l'information visent à donner à nos clients l'assurance que les risques qui menacent la continuité de nos activités et les données placées sous notre contrôle sont évalués, surveillés, gérés et atténués de manière appropriée.

Pour obtenir de plus amples renseignements

Nous nous engageons à prendre des mesures, et ce, en collaboration avec nos clients, pour protéger l'information placée sous le contrôle de CIBC Mellon. Pour obtenir de plus amples renseignements auprès de CIBC Mellon, notamment les commentaires de notre société à propos d'une question de sécurité des TI (par exemple un virus ou un logiciel malveillant mentionné dans les médias), pour faire le point sur vos mesures et besoins technologiques pouvant avoir une incidence sur CIBC Mellon, ou pour parler des mesures de cybersécurité prises par CIBC Mellon, CIBC et BNY Mellon, veuillez communiquer avec votre directeur de service ou votre gestionnaire de relations.

Notes:

1 http://money.cnn.com/2018/06/25/investing/dow-jones-stock-market-trade-war/index.html

2 https://www.thebci.org/news/what-are-the-effects-of-reputational-damage.html

À propos de CIBC Mellon

CIBC Mellon est une société canadienne qui se concentre exclusivement à répondre aux besoins en services de placement des investisseurs institutionnels canadiens et des investisseurs institutionnels étrangers qui investissent au Canada. Fondée en 1996, CIBC Mellon est détenue à parts égales par The Bank of New York Mellon (BNY Mellon) et la Banque Canadienne Impériale de Commerce (CIBC). Les solutions de services de placement de CIBC Mellon sont offertes aux institutions et aux sociétés en étroite collaboration avec nos sociétés mères et comprennent des services de garde, de comptabilité en devises multiples, d'administration de fonds, de tenue des dossiers, de retraite, de prêt de titres, de règlement en monnaies étrangères et de trésorerie. Au 30 juin 2018, CIBC Mellon détenait plus de 2 billions de dollars canadiens d'actifs sous administration au nom de banques, de caisses de retraite, de fonds de placement, de sociétés, de gouvernements, de compagnies d'assurance, de fiducies d'assurance étrangères, de fondations et d'institutions financières mondiales dont les clients investissent au Canada. CIBC Mellon fait partie du réseau mondial de BNY Mellon qui, au 30 juin 2018, avait 33,6 billions de dollars américains d'actifs sous garde et sous administration.

Pour obtenir de plus amples renseignements, consultez le site www.cibcmellon.com.

CIBC MELLON

UNE COENTREPRISE DE BNY MELLON ET CIBC[SM]

000 - KL29 - 07 - 18