CIBC MELLON | BNY MELLON | CIBC

Se préparer à l'imprévu : Considérations relatives à la continuité des activités et à la sécurité de l'information

AOÛT 2021

PAR KEVIN KONDO

Vice-président adjoint, Sécurité des entreprises

Kevin Kondo est vice-président adjoint, Sécurité des entreprises chez CIBC Mellon. Kevin est responsable de la supervision de la reprise après sinistre et du programme de continuité des activités en plus de gérer les programmes de sécurité de l'information de CIBC Mellon. Il compte à son actif plus de 15 ans d'expérience dans le secteur des services financiers canadiens.

Il est probable que « sans précédent » ait été l'expression la plus utilisée en 2020, alors que la pandémie de la COVID-19 touchait les personnes, les entreprises et les marchés du monde entier. Le passage rapide au télétravail a permis aux participants du marché des services financiers de protéger la santé et la sécurité de leurs équipes, ainsi que de respecter les exigences en évolution des gouvernements et des autorités sanitaires. Au milieu de cet environnement, la continuité et la résilience des activités ont pris encore plus d'importance. De même, un nouvel ensemble de défis a été présenté aux organisations qui cherchaient à sécuriser l'information sous leur contrôle parmi une main-d'œuvre soudainement dispersée dans leur environnement domestique pendant une période prolongée.

CIBC Mellon investit depuis longtemps dans la continuité et la résilience des activités et notre équipe est fière de son rendement dans le contexte de la COVID-19. Nous avons travaillé à soutenir les clients, à collaborer avec les intervenants du marché et, surtout, à protéger nos équipes. Nous avons été heureux d'être nommés au premier rang dans le monde par Global Finance pour les opérations de trésorerie pendant la pandémie de la COVID-19. Nous demeurons néanmoins fermement engagés à nous améliorer continuellement.

TECHNOLOGIE ET RÉSILIENCE

Les incidents technologiques touchant les activités des entreprises sont fortement médiatisés, et visent les entreprises partout au Canada et dans le monde. Ils sont de plus en plus fréquents en cette ère numérique fortement branchée. Les investisseurs institutionnels, les organismes de réglementation et les intervenants de tous les services financiers et d'autres segments de l'industrie souhaitent que leurs fournisseurs et partenaires les rassurent en leur confirmant qu'ils ont mis en place des processus pour atténuer les effets des incidents imprévus, des perturbations et des menaces touchant les services essentiels. CIBC Mellon a pris et continuera de prendre des mesures pour maintenir le service de haute qualité, la stabilité et la flexibilité que les clients attendent de nous. À titre de gardien digne de confiance d'actifs d'une valeur de plus de 2,4 billions de dollars pour le compte de banques, de régimes de retraite, de fonds de placement, d'entreprises et d'autres investisseurs institutionnels, nous reconnaissons l'importance de notre résilience pour nos clients. C'est pourquoi nous cherchons constamment à renforcer notre environnement de gouvernance et de contrôle solide. Nous savons que nous devons réagir de manière rapide, organisée et efficace face à des défis imprévus, afin de continuer à offrir nos services et nos solutions à nos clients.

FAIRE PREUVE D'UN NIVEAU ÉLEVÉ DE DILIGENCE TOUT AU LONG DE LA CRISE DE LA COVID-19

Un facteur important contribuant à la capacité de CIBC Mellon de bien servir ses clients est le contrôle et la gouvernance du risque robustes que nous avons mis en place. Alors que nous sommes face à un contexte sans précédent, notre engagement à pratiquer une gouvernance appropriée et à respecter nos contrôles n'a pas changé.

NORMES ÉTABLIES PAR DES TIERS : CERTIFICATION ISO

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 certifier votre niveau de préparation auprès des autorités, des clients (potentiels ou existants) et des autres intervenants ayant un rôle essentiel dans votre secteur. La certification ISO de la British Standards Institution en est un exemple. Organisme de normalisation mondialement reconnu, l'ISO aide plus de 128 000 clients situés dans 193 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.

Deux normes qui peuvent représenter un intérêt pour la continuité de vos activités et vos efforts de sécurité de l'information sont :

ISO 22301 | ISO 27001

ISO 22301: SÉCURITÉ ET RÉSILIENCE — SYSTÈME DE GESTION DE LA CONTINUITÉ DES ACTIVITÉS

CIBC Mellon est certifiée ISO 22301. Cette norme précise que les exigences pour mettre en œuvre, maintenir et améliorer un système de gestion visant à se protéger des incidents perturbateurs, réduire leur probabilité de survenance, s'y préparer, y répondre et s'en rétablir lorsqu'ils surviennent. La norme ISO 22301 n'est pas seulement un outil de planification et de certification, mais elle peut également servir à évaluer l'aptitude d'un organisme à satisfaire ses propres besoins et obligations en matière de continuité des activités.

Le tableau ci-dessous de l'analyse prospective du BCI démontre qu'un nombre croissant d'organisations obtiennent la certification ISO 22301.

POURCENTAGE DES ORGANISATIONS CERTIFIÉES ISO 22301 OU EN CONFORMITÉ AVEC CETTE NORME

Année	Pourcentage d'organisations certifiées ISO 22301	Pourcentage d'organisations certifiées ISO 22301 OU l'utilisant comme cadre
2016	11,6 %	67,7 %
2017	9,6 %	65,8 %
2018	13,8 %	69,2 %
2019	20,5 %	71,0 %

Mise à jour de la norme ISO 22301 : À ce jour, près des trois quarts des organisations sont certifiées ISO 22301 ou l'utilisent comme cadre. 5 % des organisations prévoient obtenir la certification en 2021. Du point de vue de la sécurité de l'information, les fournisseurs ont plusieurs façons de fournir l'assurance que les données sous leur contrôle sont suffisamment protégées et qu'une organisation a la résilience nécessaire. En collaborant avec les fournisseurs, songez à obtenir l'assurance que ces facteurs sont de multiples centres de données redondants, pour confirmer la mise en place d'un plan détaillé de continuité des activités et de reprise après sinistre, et établir des normes élevées en matière de sécurité de l'information. Lors du choix des fournisseurs, les entreprises pourraient évaluer si un fournisseur respecte les normes établies par des tiers telles que la norme ISO 22301:2012 Sécurité sociétale – Systèmes de gestion de la continuité des activités. Cela permet aux organisations de se préparer aux incidents perturbateurs et de se rétablir plus rapidement, minimisant ainsi l'impact sur les employés, les clients et les fournisseurs.

ISO/IEC 27001 - Gestion de la sécurité de l'information

CIBC Mellon possède la certification 27001:2013 de l'Organisation internationale de normalisation (ISO) publiée par la British Standards Institution. ISO/IEC 27001 est un système de gestion reconnu internationalement pour la gestion des risques de gouvernance de la sécurité de l'information. La norme fournit un cadre de pratiques exemplaires, une gouvernance continue et une gestion robuste du système pour :

Identifier et minimiser les risques pour l'information sous le contrôle d'une organisation

Améliorer la réputation et la confiance des intervenants

Améliorer la sensibilisation à la sécurité de l'information

La certification ISO 27001 de CIBC Mellon confirme l'engagement de notre équipe de direction à maintenir et à faire évoluer le cadre qui aide à protéger les données financières, la propriété intellectuelle et les renseignements personnels des clients. La portée de la certification comprend, sans s'y limiter, les processus et les technologies qui soutiennent le cadre et vérifient l'efficacité des mesures de sécurité. Une évaluation continue de notre contexte de risques aide à identifier et à atténuer les risques externes et internes, et constitue une partie essentielle de la norme ISO/IEC 27001.

CIBC Mellon investit depuis longtemps dans la continuité et la résilience des activités et notre équipe est fière de son rendement dans le contexte de la COVID-19.

Un facteur important contribuant à la capacité de CIBC Mellon de bien servir ses clients est le contrôle et la gouvernance du risque robustes que nous avons mis en place.

Questions à prendre en considération

1. Votre organisation a-t-elle mis en place un processus de continuité des activités actif et permanent?
2. Quels sont les engagements commerciaux ou d'affaires pris par votre organisation envers les clients et les intervenants?
3. Dans quelle mesure les plans de continuité des activités et les besoins en la matière sont-ils documentés par votre organisation?
4. Comment votre organisation compte-t-elle communiquer avec ses employés, ses clients et les autres intervenants durant une urgence ou une crise?
5. En combien de temps êtes-vous en mesure de joindre les employés en dehors des heures normales de travail?
6. Quels sont les dépendances, les technologies et les systèmes importants de votre organisation?
7. Qui sont vos employés essentiels?
8. Qui sont vos fournisseurs importants, et comment êtes-vous arrivés à vous rassurer et à rassurer les intervenants que ces fournisseurs ont pris les dispositions nécessaires pour faire face à une interruption?
9. Quelles sont les exigences réglementaires, du conseil d'administration et des intervenants en matière de déclaration que votre organisation doit respecter pour faire face aux problèmes de préparation de la continuité des activités?

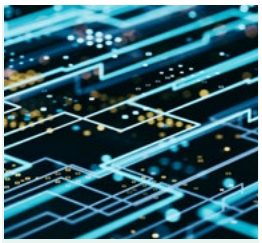
Dix principales perturbations

Incident lié à la santé

Pannes informatiques et de télécommunications non planifiées

Incident de sécurité (p. ex., blessure corporelle, décès etc.)

Manque de talents/ compétences clés



Cyberattaque et atteinte à la sécurité des données

Maladie non liée au travail

Rappel de sécurité du produit

Événements météorologiques extrêmes (p. ex., inondations, tempêtes, gel, etc.)

Interruption des services d'utilité publique

Volatilité du taux de change

Le contexte des perturbations a changé au cours de la dernière année, tandis que les effets persistants de la pandémie de la COVID-19 demeurent présents. Les autorités de santé publique continuant de surveiller la progression et la propagation de la COVID-19, les incidents liés à la santé ont éclipsé les pannes informatiques et les télécommunications et constituent ainsi la principale cause de perturbation pour les organisations au cours des douze derniers mois.

Les événements qui ont une incidence sur la continuité des activités sont très divers. Comme le montre le sondage du BCI, les entreprises ont tendance à se concentrer sur les incidents technologiques, étant donné le monde numérique dans lequel elles évoluent aujourd'hui. Un scénario relatif à la technologie peut inclure notamment les éléments suivants : une panne d'un système essentiel ou du réseau; une panne du réseau de communication, la perte de prestataires de services et de fournisseurs (externalisation), par exemple un fournisseur TI; une panne des infrastructures techniques, comme un logiciel, un élément de matériel, une base de données ou les services bancaires en ligne; ou une panne d'électricité due aux conditions météorologiques.

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.

Cybersécurité

Notre approche et notre philosophie

Chez CIBC Mellon, nous comprenons que nos clients font face à une pression croissante de la part des investisseurs institutionnels, des organismes de réglementation et des intervenants pour s'assurer que des processus sont en place afin d'atténuer les effets des perturbations inattendues et des menaces sur les services essentiels, comme les violations dues à des événements technologiques. En règle générale, la sécurité de l'information est considérée comme étant le risque de gérer la confidentialité, l'intégrité et la disponibilité des actifs informationnels. L'objectif est d'empêcher la divulgation, la modification non autorisée ou accidentelle des données ou la perte d'actifs informationnels.

Les atteintes à la sécurité de l'information sont généralement dues à des incidents technologiques qui touchent les activités de l'entreprise. Ces violations ont des répercussions sur les entreprises partout au Canada et dans le monde entier, à une fréquence plus élevée dans le monde numérique hautement connecté d'aujourd'hui. Les investisseurs institutionnels, les organismes de réglementation et les intervenants de tous les services financiers et d'autres segments de l'industrie souhaitent que leurs fournisseurs et partenaires les rassurent en leur confirmant qu'ils ont mis en place des processus pour atténuer les effets des incidents imprévus, des perturbations et des menaces touchant les services essentiels.

Alors que les organisations continuent de se tourner vers la connexion, la numérisation et la technologie, la gouvernance, la sécurité et la préparation des TI sont devenues de plus en plus importantes. Qu'il s'agisse notamment de processus internes, de formation des employés et de gestion des fournisseurs, les organisations doivent chercher à demeurer vigilantes et œuvrer à l'amélioration continue des contrôles et des mesures de sécurité mis en place pour se protéger, protéger les intervenants et l'information sous leur contrôle.

Assurez-vous de recevoir de l'information sur la sécurité concernant les menaces potentielles de la part de nos pairs et d'une grande partie du secteur des services financiers ainsi que de la part des organismes d'application de la loi et d'une variété de sources publiques et privées. De nombreuses industries travaillent ensemble sur le cyberrenseignement – une violation dans une organisation a un impact sur l'ensemble de l'industrie.

Cybersécurité et atténuation des cyberrisques

CIBC Mellon est bien placée grâce au soutien d'organismes chefs de file des services financiers mondiaux – CIBC Mellon et BNY Mellon – qui accordent tous les deux un grand intérêt à la cybersécurité. CIBC, BNY Mellon et CIBC Mellon surveillent continuellement l'environnement informatique pour déterminer les risques potentiels et les préoccupations. Elles œuvrent à renforcer davantage leurs mesures de sécurité et de gouvernance.

CIBC Mellon et ses sociétés mères disposent de plusieurs niveaux de protection contre les menaces liées aux technologies de l'information. En outre, elles ont mis en œuvre – et cherchent à améliorer en permanence – un large éventail de mesures de sécurité visant à protéger notre société, nos clients, nos employés et l'information sous notre contrôle.

Nos évaluations des risques et des contrôles sont généralisées à nos fournisseurs de services externes. Nous avons établi des exigences obligatoires pour que nos partenaires protègent les actifs des clients. Nous effectuons des contrôles préalables planifiés de nos ententes d'externalisation de matériel et des fournisseurs de technologie et de services commerciaux essentiels, y compris des ententes de sous-traitance connexes, pour garantir qu'ils répondent à nos exigences en matière de niveau de service et qu'ils soutiennent nos engagements commerciaux et de protection des données envers nos clients et nos organismes de réglementation.

QUELLES SONT LES QUESTIONS SUR LA CYBERSÉCURITÉ QUE LES CLIENTS DEVRAIENT SE POSER?

- Dans quelle mesure vous documentez, comprenez et saisissez la portée des données sous votre contrôle?
- Quelles mesures avez-vous mises en place pour protéger les données? Quelles sont les politiques?
- Chiffrez-vous les données? Si c'est le cas, à quel moment vous le faites?
- Comment rendez-vous la transmission des données plus sûre?
- Comment tenez-vous les employés informés et préparés aux procédures de cybersécurité les plus récentes ainsi qu'à d'autres aspects similaires?
- Comment vous assurez-vous que les employés, du tout nouvel employé aux plus hauts dirigeants, sont bien préparés?
- Quels sont les dépendances, les technologies et les systèmes importants de votre organisation?
- Quels sont les événements à risque potentiels et comment réagiriez-vous si vous avez fait l'objet d'une violation?
- Par exemple, paieriez-vous une rançon ou dans quelles circonstances envisageriez-vous de la faire?
- Que peuvent faire ou non mes employés avec les données dont ils se soucient? Comment cet accès aux données est-il contrôlé?
- Quelles mesures de protection avez-vous mises en place pour prévenir les pertes de données, les violations de données et les attaques par déni de service? Comment détectez-vous les logiciels malveillants et les attaques par hameçonnage et comment protégez-vous?
- Dans quelle mesure faites-vous confiance aux principes fondamentaux de votre organisation? Par exemple, la capacité de surveiller l'évolution du contexte des menaces, des correctifs, de la gestion des vulnérabilités et des programmes de gestion des accès?

Risques qui vont au-delà des risques technologiques en cas de cyberattaque :

Traitement des transactions - ce qui pourrait entraîner un risque de perte résultant de défaillances dans le traitement ou l'exécution d'une tâche si vous ne pouvez pas accéder aux systèmes et traiter les transactions.

Risque de continuité des activités - résultant d'un cyberévénement, il peut évidemment avoir un impact négatif sur la poursuite des processus opérationnels d'une entreprise.

Risque juridique - une entreprise pourrait courir le risque de négligence dans la protection de ses données, ce qui pourrait entraîner un litige potentiel avec des clients, des fournisseurs ou d'autres sociétés affiliées.

Risques liés à la réglementation et à la conformité - en raison d'infractions potentielles ou de non-respect des lois, des règles, des politiques, des règlements, des pratiques prescrites ou des normes éthiques en matière de sécurité de l'information.

Risque d'atteinte à la réputation - qui entraîne la perte d'affaires en raison d'une diminution de l'image publique de votre organisation aux yeux des clients, des employés, des organismes de réglementation, des intervenants concernés comme les membres du régime ou des investisseurs, et d'autres intervenants dans les marchés ou encore des communautés où vous exercez vos activités. Le risque d'atteinte à la réputation a une incidence sur la capacité de l'organisation à établir de nouvelles relations ou de nouveaux services ou à continuer à servir les clients existants. Un problème de risque d'atteinte à la réputation peut souvent entraîner une perte de revenus, une augmentation des coûts d'exploitation ou réglementaires, une diminution de la valeur pour les actionnaires. La réputation est également à risque si un scénario n'est pas géré efficacement.

Les dommages à la réputation peuvent être minimisés grâce à l'intervention d'une organisation en cas de perturbation. Selon le Business Continuity Institute, la meilleure pratique d'une entreprise est d'être transparente. L'honnêteté avec les intervenants renforce la confiance et donne l'assurance que votre organisation a la capacité de reprendre ses activités et de revenir à la normale après un événement.

Évolution du contexte des menaces dans le cadre d'un fonctionnement à distance soutenu

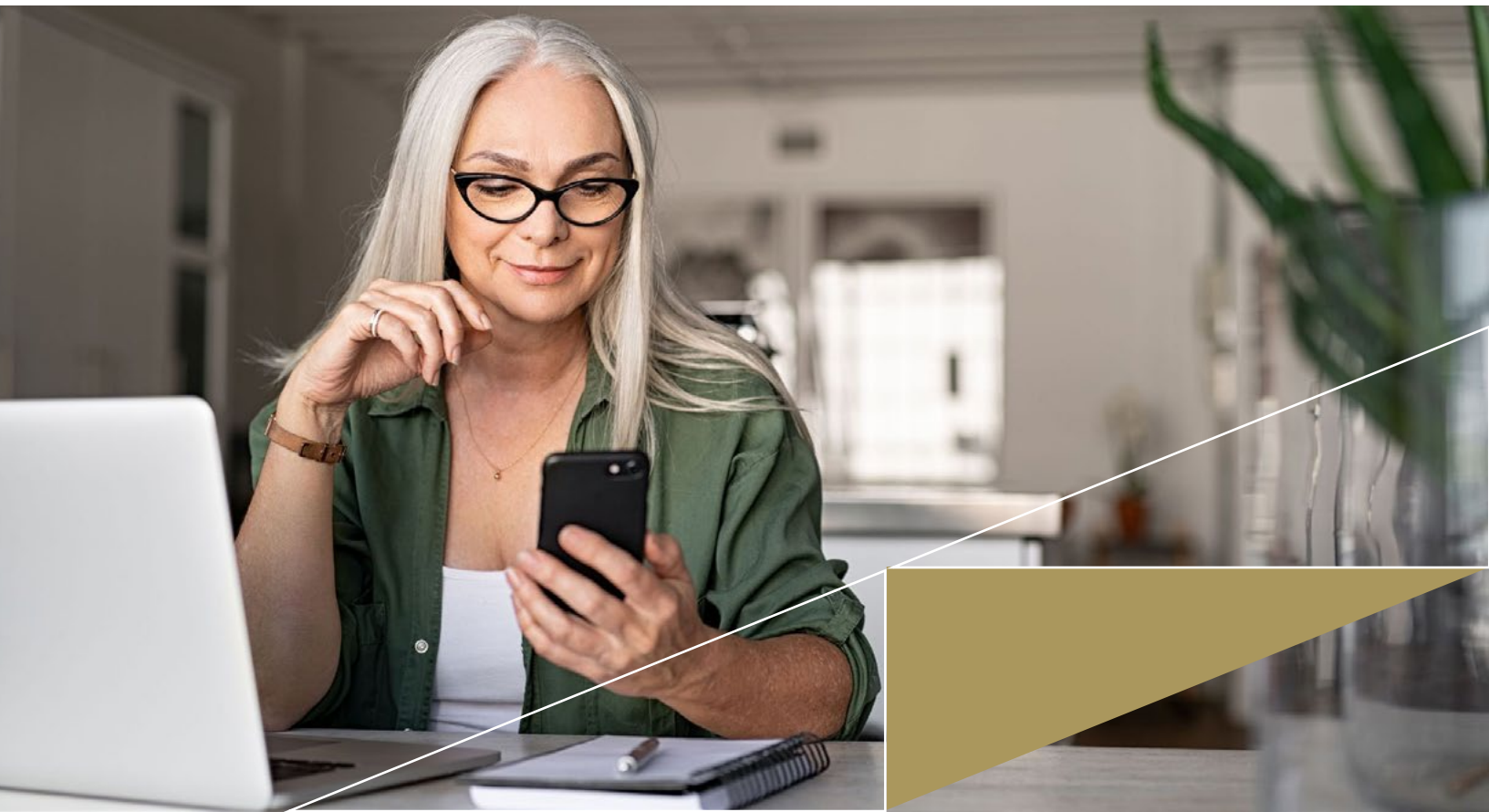
Particulièrement dans le cadre d'un transfert où la majorité des employés travaillent à distance, la diligence des employés et leur sensibilisation aux bonnes pratiques sont des éléments essentiels dans les efforts d'une société pour maintenir des contrôles solides. Le travail à domicile pendant de longues périodes peut entraîner des changements dans le contexte des menaces et créer de nouveaux risques et de nouvelles occasions.

LE TRAVAIL SE FERA DE PLUS EN PLUS À DISTANCE À L'AVENIR

Même si les organisations envisagent leur position opérationnelle dans un environnement post-pandémique, dans de nombreux cas, cette position comprend une partie de la main-d'œuvre travaillant à distance au moins une partie du temps. CIBC Mellon continue de promouvoir ses efforts stratégiques « Futures façons de travailler », qui reconnaissent que les opérations à distance ont produit des résultats soutenus et, dans certains cas, avantageux pour nos clients, nos employés et notre organisation. Pour en savoir davantage, veuillez communiquer avec votre directeur des relations.

Un contexte de menaces en constante mutation nécessite un programme pour les employés qui évolue en permanence. Mettre à la disposition des employés les moyens nécessaires pour détecter les menaces et y réagir est un thème prévalent dans l'industrie financière. Les vulnérabilités technologiques non protégées peuvent entraîner des conséquences désastreuses, comme des systèmes non affectés, des portes arrière et un accès non révoqué. Le personnel doit comprendre le caractère essentiel des données. Cela peut se faire en rendant les classifications de données disponibles, comme le traitement interne ou confidentiel, afin que les employés sachent les dispositions nécessaires à prendre en lien avec chaque ensemble d'informations. Les domaines clés sur lesquels former les employés sont, entre autres, les suivants : comment gérer les données, déplacer les données, identifier les courriels d'hameçonnage et savoir si un bureau a été piraté. Il ne suffit pas d'enseigner à un employé comment déterminer s'il a été piraté ou remarquer un mauvais lien – vos employés doivent également savoir comment réagir et signaler un incident.

Le mouvement de l'information sécurisée vers des parties externes à l'extérieur de nos organisations comme les clients et les fournisseurs représente un domaine où l'industrie peut continuer à évoluer.



TOUJOURS TENIR COMPTE DES DEUX QUESTIONS SUIVANTES :

Mon entreprise effectue-t-elle ses activités en utilisant des approches cohérentes en matière de diligence – dans toutes les fonctions et au fil du temps?

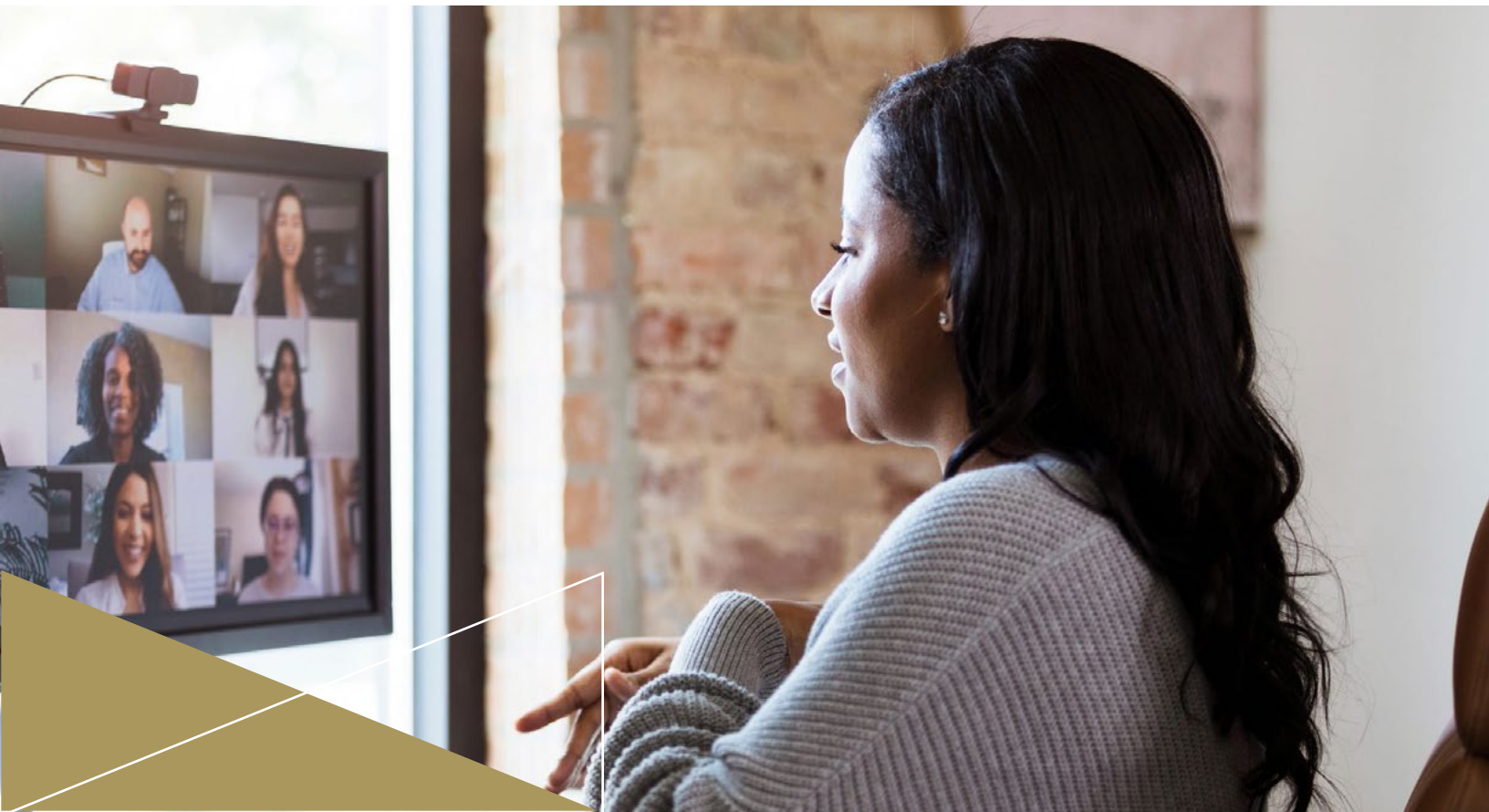
Envoyons-nous des données chiffrées en tout temps (p. ex. courriels)?

Il existe quelques étapes simples qui peuvent favoriser une résilience accrue. Par exemple, les organisations devraient envisager d'utiliser le plus récent protocole de sécurité de la couche transport (TLS) pour envoyer des données à l'extérieur de leurs environnements informatiques aux clients, aux contreparties et aux fournisseurs. Le TLS se compose de protocoles cryptographiques qui fournissent une méthode sécurisée pour transmettre des données et des informations sur un réseau informatique.

Réfléchissez à la façon dont vous gérez vos fournisseurs externalisés : leurs programmes de sécurité sont-ils aussi bien rodés que vos programmes de sécurité?

Du point de vue de la technologie, CIBC Mellon dispose de plusieurs niveaux de contrôles préventifs et de détection, peu importe le lieu de travail des employés. Le cyberprogramme d'aujourd'hui doit s'étendre au-delà des murs de briques du siège social et jouer un rôle dans chaque maison de nos employés et dans les appareils avec lesquels ils travaillent.

Travaillant à l'échelle de notre entreprise mondiale, en collaborant avec les fournisseurs et en veillant à surveiller les mises à jour de la communauté du cyberrenseignement, nos équipes mettent l'accent sur les principes fondamentaux de la sécurité technologique – en protégeant l'infrastructure de travail à distance, les environnements RPV et Citrix, en sécurisant nos terminaux par le biais de corrections de programmes et en mettant en place des correctifs, tout en surveillant étroitement les vulnérabilités et les menaces renouvelées.



Conclusion

Les participants au marché financier à l'échelle mondiale continuent de se concentrer sur la gestion des risques, la gouvernance et l'assurance des risques. Le marché canadien peut offrir des renseignements et des outils aux participants mondiaux qui cherchent à fournir une assurance, en particulier lorsque l'accent est mis sur la protection des données gérées à l'interne et à l'externe par les fournisseurs.

La pandémie oblige les entreprises à se concentrer davantage sur le risque pour les personnes, par exemple, la planification de la main-d'œuvre en cas d'absentéisme et les mesures d'intervention contre la COVID-19. La même planification et la même préparation doivent se faire au niveau de la technologie. Équipement de bureau de secours, accès à vos données et aux dossiers, sans oublier les fournisseurs de services Internet résidentiels et des services cellulaires; et en allant encore plus loin, la résilience et la préparation des principaux fournisseurs de services. L'approche holistique de la planification de la continuité au niveau des personnes, de la technologie et des processus est essentielle, car les organisations cherchent à maximiser leur résilience pendant la pandémie et au-delà.

Encourager une culture du risque durable et faire preuve d'une grande résilience est un élément essentiel de la réussite dans le paysage technologique et l'industrie des services financiers en évolution.

Pour plus d'informations

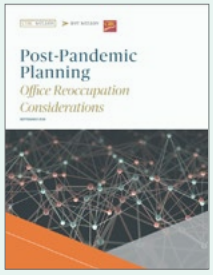
Pour en savoir plus, communiquez avec votre directeur des relations, votre directeur de service ou le service des communications d'entreprise à corporate_communications@cibcmellon.com

Ressources supplémentaires

Pour obtenir de plus amples renseignements sur la planification de la continuité des activités et le leadership éclairé de CIBC Mellon concernant la COVID-19, nous sommes heureux de vous fournir les ressources suivantes :

Énoncé de CIBC Mellon sur les préparatifs concernant le coronavirus 2019 (COVID-19)

Considérations sur la continuité des activités : Préparation aux situations de pandémie



Considérations relatives à la planification post-pandémique et à la réoccupation des bureaux

CIBC MELLON

UNE COENTREPRISE DE BNY MELLON ET CIBC[SM]

BNY MELLON

www.bnymellon.com

CIBC

www.cibc.com/fr/

000 - KL43 - 08 - 21