Cyberrésilience

Donner aux organisations les moyens d'anticiper les cybermenaces, de s'y adapter, d'y résister et de s'en remettre.

96 % des chefs de la direction considèrent la cybersécurité comme essentielle à la croissance et à la stabilité de l'entreprise, et 74 % soulignent leurs préoccupations quant à la préparation organisationnelle en vue de réduire les dommages en cas de cyberattaque.

Source : SentinelOne Cyber Resilience, 2025

Malgré un plus grand contrôle diligent des fournisseurs, 43 % des organisations ont subi des perturbations de leur chaîne d'approvisionnement en raison de défaillances de tiers.

Source : BCI Supply Chain Resilience Report 2024

Pourquoi la cyberrésilience est-elle importante?

Les perturbations sont inévitables. Des événements comme des catastrophes naturelles, des pannes de courant, des pannes de systèmes ou des attaques sophistiquées par hameçonnage ou hypertrucage peuvent perturber les activités essentielles d'une organisation. La cyberrésilience vous aide à protéger et à soutenir ce qui compte le plus en rendant votre organisation plus forte, plus adaptable, plus résistante et prête à se relever de ces défis. Il s'agit d'assurer la continuité et l'agilité de l'organisation, et ce, malgré les cyberincidents.

Pourquoi en avez-vous besoin?

Dans le contexte numérique actuel, les cybermenaces sont plus sophistiquées, plus fréquentes et plus perturbatrices que jamais. Les organisations doivent non seulement se défendre contre les attaques, mais aussi assurer une reprise rapide pour maintenir leurs opérations sous pression. Contrairement à la cybersécurité traditionnelle, qui vise à prévenir les atteintes, la cyberrésilience suppose que des atteintes se produiront et accorde la priorité à la continuité et à l'adaptabilité. La cyberrésilience est un élément essentiel de la résilience opérationnelle, qui comprend la continuité des activités et la gestion des crises et des risques. Elle intègre des défenses techniques, une gouvernance solide et une culture axée sur la sécurité. Cette approche globale renforce votre organisation à tous les niveaux, vous aidant à résister à tout cyberincident et à vous en remettre.

Modèle de cyberrésilience

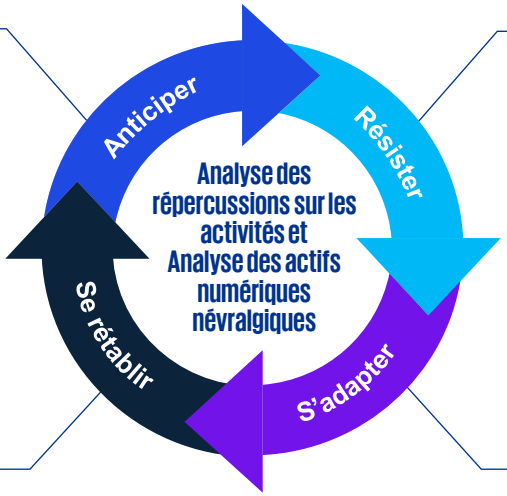
Le modèle de cyberrésilience de KPMG décrit les principaux domaines qui permettent aux organisations de maintenir leurs objectifs stratégiques et opérationnels même dans des environnements cybernétiques très convoités. Au cœur de ce modèle se trouvent l'analyse des répercussions sur les activités et l'analyse des actifs numériques névralgiques qui guident les organisations dans l'établissement des priorités et le renforcement continu des pratiques de résilience.

Anticiper

Évaluer de façon proactive le contexte des cybermenaces, effectuer des évaluations des risques et former les utilisateurs pour cerner les menaces potentielles et s'y préparer avant qu'elles ne surviennent.

Se rétablir

Rétablir efficacement les activités en tirant parti des plans d'intervention en cas d'incident établis, validés par des simulations régulières et soutenus par des stratégies de sauvegarde solides.



Résister

Concevoir des systèmes et des réseaux résilients qui utilisent une protection et des processus coordonnés pour se défendre contre les attaques et maintenir le déroulement des opérations.

S'adapter

Mettre en œuvre une reconfiguration et une redondance dynamiques pour permettre à l'organisation d'ajuster rapidement les systèmes, les privilèges des utilisateurs et les processus en réponse à l'évolution des menaces.

Nos services de cyberrésilience

Nous offrons une gamme de services qui aident les organisations à demeurer fortes et à poursuivre leurs activités, même lorsqu'elles sont confrontées à des cybermenaces. Notre approche s'articule autour de quatre axes : anticiper, résister, s'adapter et se rétablir. Notre équipe Cyberrésilience dirige ces efforts, mais nous faisons également appel à des spécialistes d'autres domaines au besoin pour nous assurer que chaque solution s'inscrit dans notre modèle éprouvé de cyberrésilience.

Formation des administrateurs et des dirigeants

Nous offrons des séances d'information sur mesure pour les conseils d'administration et la haute direction sur la gouvernance des cyberrisques, les attentes réglementaires et la planification stratégique de la résilience. Ces séances permettent aux dirigeants de prendre des décisions éclairées, de s'acquitter de leurs responsabilités de surveillance et de renforcer la résilience organisationnelle de haut en bas.

Planification de la cyberrésilience

Nous prenons en charge l'élaboration de documents sur la résilience et les améliorations organisationnelles, y compris l'analyse des actifs numériques névralgiques, les plans de reprise après sinistre, les plans de poursuite des activités, les plans de résilience précis et les guides d'intervention en cas d'incident. Notre approche fait en sorte que ces plans sont pratiques, testés et alignés sur vos priorités d'affaires.

Évaluation de la maturité en matière de cyberrésilience

À l'aide du cadre de cyberrésilience de KPMG, nous fournissons des évaluations complètes et personnalisées au moyen d'une approche unifiée, évolutive et reproductible. Ce cadre est conforme aux normes sectorielles et aux exigences réglementaires, offre des points de comparaison et aide les organisations à composer avec l'incertitude. Le résultat donne lieu à des renseignements exploitables et à des recommandations pratiques pour réduire les risques et renforcer la résilience.

Formation de sensibilisation à la sécurité

Nous offrons des services ciblés de sensibilisation et de formation en matière de sécurité. Ceux-ci tirent parti de plateformes fondées sur l'IA de nouvelle génération et aident les employés à reconnaître les vecteurs de cybermenace courants, comme l'hameçonnage, l'hameçonnage par texto et les hypertrucages, et à y réagir. Cette formation permet aux utilisateurs finaux d'acquérir des compétences pratiques pour détecter les activités suspectes, éviter les attaques et signaler rapidement les incidents.

Exercices de table

Nous concevons et animons des exercices de table et des ateliers de simulation personnalisés pour renforcer la préparation organisationnelle aux cyberincidents. Ces séances interactives font appel à des équipes spécifiques ou à des groupes interfonctionnels, y compris des dirigeants et du personnel technique, pour tester les protocoles d'intervention, améliorer la prise de décision sous pression et développer la mémoire musculaire pour des scénarios réels. KPMG offre des formules souples qui répondent aux besoins de votre organisation (virtuel seulement, en personne ou hybride), améliorées par des outils avancés comme notre simulateur 4Di pour accroître le réalisme et l'efficacité.

Ce qui distingue KPMG?

KPMG au Canada rassemble des professionnels en cyberrésilience et en sécurité de l'information de partout au pays, de Vancouver à Halifax, qui s'appuient sur un savoir-faire mondial. Nous pensons à l'échelle mondiale, agissons à l'échelle locale et offrons une connaissance approfondie du secteur pour vous aider à vous concentrer sur ce qui compte le plus : protéger vos actifs essentiels et assurer une posture de cyberrésilience.

Méthodologies exemplaires

Nous allons au-delà des cadres sectoriels en tirant parti du cadre de cyberrésilience de KPMG et en l'améliorant continuellement. Notre approche s'appuie sur les pratiques réglementaires émergentes pour fournir des évaluations complètes et une orientation fondée, et veiller à ce que votre organisation soit évaluée de façon globale.

Axé sur la collaboration

Avec plus de 300 professionnels en résilience partout au Canada, nous misons sur l'amélioration des capacités de résilience. Nous travaillons main dans la main avec votre équipe et collaborons avec nos groupes Renseignements sur les cybermenaces et Intervention en cas d'incident et d'autres spécialistes pour vous fournir des conseils pratiques qui renforceront votre organisation.

Engagement éprouvé

Nos relations reposent sur la confiance et un partenariat à long terme, et nous offrons des solutions efficaces et efficientes qui évoluent avec vos besoins commerciaux. Nous sommes profondément investis dans votre réussite, tout comme nous le sommes au Canada depuis 1869. Nous combinons le savoir-faire du réseau mondial de KPMG et nos connaissances locales pour vous aider à vous concentrer sur ce qui compte le plus.

Communiquez avec nous

Vivek Jassal
Associé
KPMG au Canada
416-777-3723
vjassal@kpmg.ca

Tarek Habib
Associé
KPMG au Canada
902-292-2091
tarekhabib@kpmg.ca

Ivana Lukic-Miloloza
Directrice principale
KPMG au Canada
416-777-8545
ilukic-miloloza@kpmg.ca