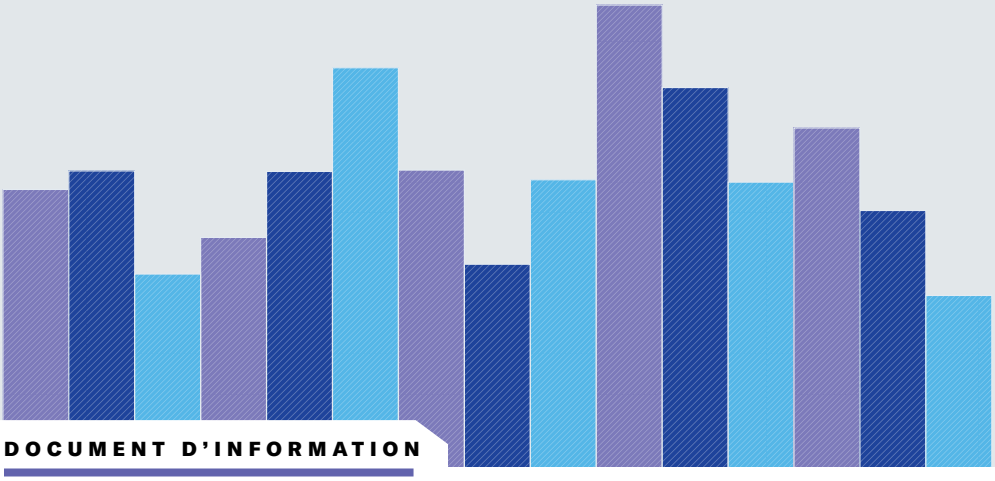
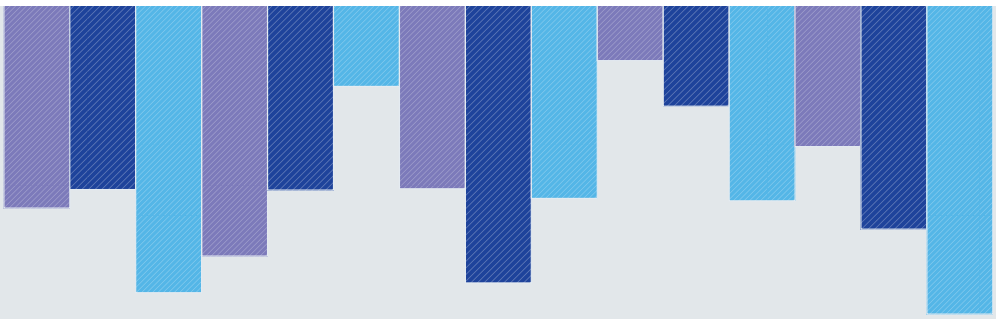
Harvard Business Review
ANALYTIC SERVICES



DOCUMENT D'INFORMATION

La cyberrésilience face aux nouvelles et rigoureuses exigences de conformité



Sponsorisé par

Commvault®

POINT DE VUE DU SPONSOR

En réponse à la complexité croissante des technologies de l'information, à l'intensification de la surveillance réglementaire et à la recrudescence des attaques par ransomware, l'investissement dans un programme de conformité d'entreprise actif, soutenu par la direction, est un indicateur clé de préparation et de cyberrésilience. Les entreprises doivent adopter une approche proactive dans leurs programmes de préparation, de récupération et de résilience pour assurer la continuité de leurs activités. Pourquoi cela est-il essentiel ?

Parce qu'il est crucial de se préparer aux situations d'urgence avant qu'elles ne surviennent. Être cyberrésilient, c'est disposer de trois équipes spécialisées prêtes à intervenir. Ces trois équipes travaillent simultanément mais de manière indépendante :

1. L'équipe d'intervention et de récupération en cas d'incident
2. L'équipe d'intervention réglementaire et juridique
3. L'équipe de préparation opérationnelle

La résilience repose sur une collaboration interfonctionnelle, des tests réguliers et des processus adaptatifs. Sans un programme de préparation solide, une entreprise reste dans une configuration réactive, jouant au chat et à la souris en cas de violation, cherchant à éliminer les acteurs malveillants de ses systèmes tout en s'efforçant de déterminer quand et comment communiquer avec les clients et le marché, le tout en respectant les exigences des organismes de réglementation. C'est un véritable raz de marée.

Ce document complet, rédigé par Harvard Business Review Analytic Services pour Commvault, propose des solutions pour remédier à ce chaos. Cette étude met en avant la nécessité d'une conformité continue pour préserver la viabilité économique et la résilience opérationnelle, tout en explorant les défis liés à la mise en œuvre d'un programme de cyberrésilience solide et l'importance de se conformer aux exigences réglementaires internationales pour protéger les données.

Enrichi par les perspectives de leaders et d'experts du secteur, ce rapport sert de guide pour toute organisation évoluant dans le paysage complexe des cybermenaces et des obligations réglementaires.

Nous espérons que ce rapport vous incitera à adopter une approche proactive en matière de conformité et de résilience : Nous sommes tous sur le même bateau lorsqu'il s'agit de protéger les données et les systèmes dans le monde numérique actuel.

Danielle Sheer
Directrice de la confiance
Commvault

La cyberrésilience face aux nouvelles et rigoureuses exigences de conformité

LE CLIMAT EST CLAIR : les professionnels du risque, de la conformité et de la sécurité sont en état d'alerte. Les risques liés aux données et aux cyber-perturbations sèment la peur. Selon le Rapport d'enquête sur les risques et la conformité de Thomson Reuters 2023, publié en octobre 2023, le conglomérat d'informations de Toronto a constaté que 82 % des professionnels du risque et de la conformité estiment que les préoccupations liées aux données et à la cybersécurité constituent le plus grand risque pour leur organisation, presque deux fois plus que la deuxième préoccupation la plus importante.[1] **FIGURE 1** En parallèle, l'enquête mondiale sur la crise et la résilience 2023 de PwC, publiée par le cabinet londonien en décembre 2023, indique que 96 % des organisations ont connu des perturbations au cours des deux dernières années, et pour 76 % d'entre elles, la perturbation la plus grave a eu un impact moyen à élevé sur leurs opérations.[2]

Cette perception reflète une compréhension profonde des professionnels du risque, de la conformité et de la sécurité : Les entreprises ne peuvent négliger la cyberrésilience, d'autant que la préparation aux cyber-incidents est aujourd'hui plus complexe que jamais. Bienvenue dans l'ère de la conformité continue, où la viabilité économique mondiale exige des services cloud disponibles en permanence et une protection des données sans compromis. Alors que de nombreuses entreprises découvrent encore l'importance croissante de l'IA pour assurer cette sécurité, les organismes de réglementation de divers continents imposent des mesures numériques strictes assorties de lourdes sanctions en cas de non-conformité.

Selon Michael Rasmussen, analyste en gouvernance, risques et conformité chez GRC 20/20 Research, un cabinet de conseil international basé à Milwaukee, la cyberrésilience repose essentiellement sur la quasi-éradication des perturbations commerciales majeures, un objectif où l'IA aura un rôle essentiel à jouer. « D'ici trois à cinq ans, les services alimentés par l'IA devraient atteindre un niveau de sophistication inédit, avec des avancées en machine learning permettant une sécurité prédictive, capable d'anticiper et de neutraliser les menaces avant qu'elles ne se concrétisent ».

Les organisations connaissent déjà sans doute les projets de loi visant à protéger les données (le Règlement général sur la protection des données, la Loi sur la gouvernance des données, la Loi européenne sur les données), à garantir la sécurité des systèmes et de l'information (la Directive 2 sur la sécurité des réseaux et des informations (NIS2),

POINTS CLÉS

La résilience, selon de nombreuses définitions, exige des organisations la capacité d'**anticiper les catastrophes, qu'elles soient naturelles ou causées par l'homme**, de **survivre aux perturbations avec des dommages limités**, et de **restaurer données et opérations presque** instantanément.

L'intégration de nouvelles fonctions de conformité dans les flux de travail existants est **particulièrement difficile pour les organisations qui ne cultivent pas une culture de la conformité et qui n'investissent pas suffisamment dans la surveillance et l'amélioration continues**.

Les avancées de la recherche en IA pourraient jouer un rôle important en **aidant les organisations à gérer les menaces, et en facilitant la production automatique de rapports** de conformité répondant aux normes réglementaires mondiales.

« D'ici trois à cinq ans, les services alimentés par l'IA devraient atteindre un niveau de sophistication inédit, avec des avancées en machine learning permettant une sécurité prédictive, de sorte à pouvoir anticiper et neutraliser les menaces avant qu'elles ne se concrétisent », affirme Michael Rasmussen, analyste gouvernance, risque et conformité chez GRC 20/20 Research.

la Loi sur la cyberrésilience, la Directive sur la résilience des entités critiques), ou à cibler des cas d'utilisation spécifiques (la Loi sur l'IA de l'UE). Ces réglementations préparent le terrain pour l'un des défis de conformité les plus redoutables : la loi sur la résilience opérationnelle numérique (DORA) de l'Union européenne, qui instaure des cadres stricts pour la gestion des risques, les tests de résilience et les rapports d'incidents.

Les organisations souhaitant prospérer dans une économie numérique mondialisée doivent gérer ce foisonnement de réglementations complexes et bâtir une résilience leur permettant de résister aux erreurs et attaques qui perturbent non seulement leurs chaînes d'approvisionnement, centres de données, réseaux et opérations dans le cloud, mais aussi leurs partenaires, clients et actionnaires. Quelle que soit la région ou le secteur, l'approche réglementaire se fonde généralement sur un principe fondamental : Renforcer chaque maillon de la chaîne numérique, des organisations les plus riches aux plus modestes en ressources, et exiger des comptes de toutes les parties impliquées.

« Je pense que nombre de ces réglementations visent à s'assurer que la société, face à notre interdépendance économique croissante, ne soit pas mise en péril par des entités qui ne saisissent pas ou ne prennent pas en charge leurs propres risques », explique Jonathan Fairtlough, directeur chez KPMG, cabinet de conseil en stratégie basé à Londres. Le risque cybernétique, autrefois délégué aux équipes informatiques, est devenu « un pilier de la planification des activités, de la continuité des opérations et de l'évaluation des risques », explique M. Fairtlough. « C'est pourquoi de plus en plus de conseils d'administration s'organisent pour superviser et comprendre le cyber-risque, car celui-ci touche au cœur de leur mission dans l'entreprise ».

Face à ces réglementations actuelles et à venir, les organisations en Amérique du Nord, en Europe et en Asie-Pacifique subissent une pression accrue pour mettre en place des programmes de cyberrésilience solides et investir dans les outils et talents adéquats, afin d'assurer la bonne gestion et la protection des données sensibles concernant leurs produits, services, clients, partenaires et employés. Répondre à ces exigences n'est pas une mince affaire. Mettre en place une cyberrésilience constitue un objectif ambitieux. Selon de nombreuses définitions, la résilience exige que les organisations puissent anticiper les catastrophes naturelles ou humaines, résister aux perturbations avec des dommages limités, et rétablir presque immédiatement leurs données et opérations. Pour atteindre ces niveaux élevés de résilience opérationnelle, les organisations doivent adopter des pratiques exemplaires, comme des tests de récupération fréquents, des environnements cybernétiques isolés (protégés des menaces externes), des capacités de signalement renforcées et des cyberdéfenses robustes intégrées au cloud.

Ce document analyse les éléments clés de la conformité réglementaire et de la cyberrésilience à l'ère numérique, en mettant en lumière les défis majeurs auxquels les organisations du monde entier sont confrontées pour renforcer leur résilience face à des menaces puissantes et en constante évolution, y compris les nouvelles menaces. Il met également en avant la surveillance réglementaire accrue, qui expose les organisations à de lourdes sanctions en cas de mauvaise gestion des données ou de négligences impactant les marchés et les chaînes d'approvisionnement. En outre, il explore la façon dont les organisations peuvent optimiser et renforcer leur résilience opérationnelle sans compromettre leur agilité commerciale.

Des perturbations commerciales coûteuses

L'ampleur sans précédent des nouvelles réglementations à venir, replacée dans un contexte économique, reflète l'engagement général et coordonné des gouvernements à réduire, voire à éliminer les risques de perturbations commerciales coûteuses. Parmi les problèmes récurrents se trouvent les centres de données cloud mal gérés et les applications cloud défaillantes des fournisseurs de logiciels, susceptibles de provoquer des pannes de système préjudiciables et des interruptions d'activité, comme la panne généralisée de CrowdStrike survenue le 19 juillet 2024. Un rapport de Parametrix, un cyber-assureur new-yorkais, publié peu après cette panne de plusieurs jours, a estimé que l'incident avait coûté 5,4 milliards de dollars aux entreprises américaines du classement Fortune 500, sans compter les potentielles atteintes à la réputation de la marque, les frais juridiques, les sanctions réglementaires ou la perte de valeur pour les actionnaires.[3]

Pour prévenir les interruptions de service et répondre aux exigences de plus en plus strictes en matière de protection des données, les entreprises doivent développer une stratégie globale qui renforce leur résilience opérationnelle face aux perturbations, qu'elles soient d'origine naturelle ou humaine, y compris en cas de

mauvaise gestion des données. La situation est urgente. Le rapport Global Cybersecurity Outlook 2023 du Forum économique mondial à Cologny (Suisse) a révélé que « les cyberattaquants sont plus susceptibles de cibler l'interruption des activités et l'atteinte à la réputation ». Plus de neuf dirigeants et experts en cybersécurité sur dix ayant participé à cette étude estiment qu'un « cyber-événement catastrophique de grande ampleur est au moins assez probable dans les deux prochaines années »[4]

Selon M. Rasmussen de GRC 20/20, « dans un monde où les risques d'entreprise deviennent de plus en plus complexes et interconnectés, être conforme et résilient nécessite que votre organisation soit capable de répondre aux pressions réglementaires, de protéger ses actifs critiques et d'assurer la continuité et sa résilience au milieu du chaos du changement qui touche son activité.»

Selon lui, la capacité à maîtriser cette complexité revêt une importance stratégique. « D'un point de vue stratégique, cet effort de conformité place l'organisation en tant qu'entité de confiance, capable de fournir une valeur durable à ses clients et à ses parties prenantes, tout en réduisant les perturbations et les coûts associés ».

La résilience : un enjeu majeur

Cédric Burton, coprésident mondial et associé chargé des données, de la confidentialité et de la cybersécurité au bureau de Bruxelles du cabinet d'avocats Wilson Sonsini, basé à Palo Alto (Californie), recommande aux multinationales de considérer la cyberrésilience comme une nécessité absolue. « Aujourd'hui, pour prospérer, une entreprise doit maintenir des pratiques cybersécuritaires solides, ce qui implique d'être cyberrésiliente », explique-t-il. « Sans cela, la confiance est perdue ».

Il est indiscutable que la cyberrésilience constitue un pilier de l'économie mondiale. Cependant, les règles du jeu ont changé. l n'y a pas si longtemps, les organisations visaient avant tout à se rétablir rapidement après les catastrophes, plutôt qu'à les prévenir. Avant l'avènement du cloud, les entreprises envoyaient leurs données sur des bobines de bandes magnétiques vers des entrepôts externes pour stockage. Ces sauvegardes sur bande n'étaient ni indestructibles ni facilement accessibles, à l'opposé des exigences modernes en matière de résilience d'entreprise. Bien que le cloud offre aux entreprises de nombreuses options intéressantes de récupération, telles que la redondance globale des données, il complique également la gestion des risques avec des cyberattaques omniprésentes, notamment les ransomwares, qui forcent parfois les organisations à payer des millions de dollars pour récupérer leurs données volées et chiffrées.

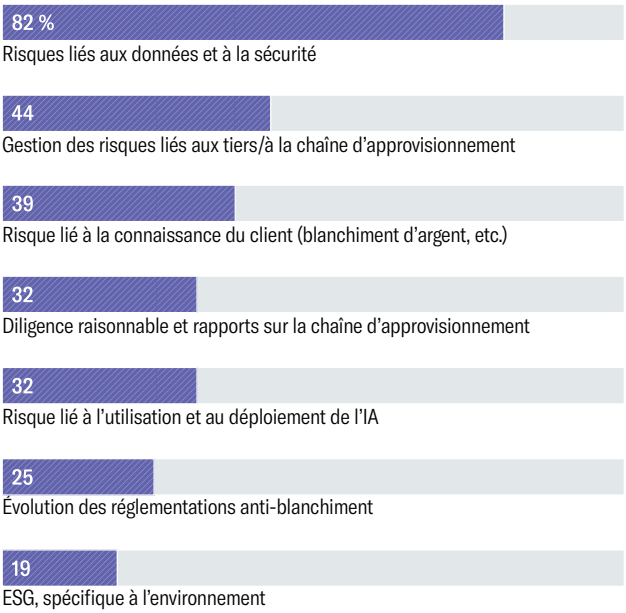
Opérer dans le cloud public n'équivaut pas à se décharger de sa responsabilité de résilience opérationnelle. Les entreprises qui utilisent des services cloud doivent également adopter le « modèle de responsabilité partagée », où la sécurité est une responsabilité conjointe : le fournisseur gère l'infrastructure et les réseaux, tandis que le client assure la sécurité de ses données et applications. Les clients opérant dans le cloud doivent mettre au point des stratégies de protection des données et de cyberrésilience en tenant compte du modèle de responsabilité partagée.

FIGURE 1

Le risque rencontre la conformité

Les organisations considèrent que les données représentent leur risque le plus important

Parmi les concepts suivants, lequel constitue le plus grand risque pour votre organisation ?



Les entreprises, notamment dans les secteurs réglementés, font face à la menace de sanctions financières et d'atteinte à la réputation en cas de violation de la confidentialité des données, dans un contexte de réglementation mondiale de plus en plus stricte. Les clouds et les chaînes d'approvisionnement logicielles se sont transformés en véritables terrains minés pour la gestion des données et la conformité réglementaire. M. Rasmussen observe malheureusement que « le modèle de responsabilité partagée en matière de sécurité dans le cloud peut engendrer une confusion quant aux responsabilités, augmentant ainsi les risques de mauvaises configurations et de violations de données »

La résilience représente un investissement de taille, nécessitant l'adoption de cadres technologiques fiables et une évaluation rigoureuse des risques et opportunités actuels. « La résilience opérationnelle va bien au-delà de la seule conformité réglementaire », souligne M. Rasmussen. « Chaque organisation devrait examiner les risques d'intégration et évaluer son niveau de conformité ainsi que ses capacités de résilience », ajoute-t-il. « Cette évaluation inclut la cartographie des chaînes d'approvisionnement, l'identification des dépendances critiques et l'analyse de l'impact potentiel des perturbations ».

Lorsque des vulnérabilités potentielles sont identifiées, une organisation doit mener une analyse des écarts entre ses pratiques

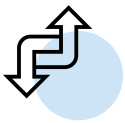
actuelles et les exigences des cadres réglementaires en place, explique M. Burton de Wilson Sonsini. « Une fois l'écart identifié, tentez de le combler en élaborant ou en adoptant un cadre qui permette la conformité et la réduction de ces lacunes », conseille-t-il.

Après ces étapes, M. Burton recommande de réaliser des audits, des tests et un « suivi continu du plan pour s'assurer de son amélioration constante ». La seule façon de se préparer, c'est de s'entraîner ». Une approche consiste à organiser des exercices sur table, simulant le rôle de chaque membre de l'équipe lors d'une cyber-urgence. Les organisations peuvent évaluer leurs progrès grâce à des indicateurs clés de performance, comme le délai moyen de récupération, la disponibilité des systèmes, la formation des équipes, et la fréquence des mises à jour du plan d'intervention en cas d'incidents. Une autre forme de préparation est de réaliser des tests en salle blanche, une technique permettant d'identifier et d'éliminer les failles qui rendent les logiciels vulnérables aux cybermenaces. Les tests en salle blanche constituent une pratique émergente, souvent coûteuse et complexe, permettant aux organisations de démontrer aux organismes de réglementation qu'elles prennent des mesures adéquates pour protéger les données.

Cependant, la majorité des entreprises tend à compartimenter la gestion de la conformité et de la résilience, observe M. Fairtlough de KPMG. Une telle approche peut créer un « manque de compréhension de l'interconnexion des éléments ». À l'inverse, ceux qui adoptent une vision globale des risques peuvent démontrer à leur conseil d'administration que la gestion des risques, bien qu'ayant un impact significatif sur l'activité, « s'intègre dans les plans de continuité des activités et de récupération après sinistre ». Il ajoute que l'intégration d'une vision holistique des risques dans la planification organisationnelle améliore la capacité d'une organisation à « répondre à ses impératifs de production et contractuels », en décloisonnant l'information et en diffusant ainsi les meilleures pratiques de conformité et de cyberrésilience.

L'obtention du soutien et du parrainage des cadres dirigeants pour des projets organisationnels d'envergure est depuis longtemps reconnue pour favoriser la mise en cohérence des unités opérationnelles disparates. L'intégration de nouvelles fonctions de conformité dans les flux de travail existants est particulièrement difficile pour les organisations qui ne cultivent pas une culture de la conformité et qui n'investissent pas suffisamment dans la surveillance et l'amélioration continues. L'adaptation aux exigences d'une architecture de cloud complexe et d'un environnement réglementaire en perpétuelle évolution face aux cybermenaces ne peut pas simplement être déléguée à l'équipe conformité. Il s'agit d'une initiative globale nécessitant une planification approfondie, des investissements, une formation adaptée, ainsi qu'un contrôle et des tests rigoureux.

D'après M. Rasmussen, instaurer un programme de conformité et de résilience efficace exige un engagement constant de la part du conseil d'administration. Il est également indispensable d'avoir « une compréhension approfondie de l'évolution de l'environnement commercial et du panorama des risques et des menaces, ainsi qu'une culture qui valorise la gestion des risques et la résilience à tous les échelons de l'organisation », précise-t-il. « La difficulté réside rarement dans la technologie elle-même, mais plutôt dans la promotion de l'état d'esprit et de l'alignement autour de la conformité continue au sein des différentes fonctions de l'entreprise, ainsi que dans la mise à jour constante au sein d'un environnement commercial dynamique et changeant ».



Jonathan Fairtlough, directeur chez KPMG, indique que les organisations qui adoptent une vision globale des risques peuvent démontrer à leur conseil d'administration que la gestion des risques, bien qu'impactante, « s'intègre dans les plans de continuité des activités et de récupération après sinistre ».

Le risque à travers le prisme culturel

Il est tentant, mais également risqué, de supposer que la conformité réglementaire et la cyberrésilience sont interprétées de façon identique par les organismes de réglementation du monde entier. M. Fairtlough avance que les entreprises américaines voient souvent la conformité comme une condition binaire. « Nous nous focalisons sur des termes comme « conformité », où l'on se réfère à des normes telles que le NIST (National Institute of Standards and Technology) [Institut national des normes et de la technologie], en travaillant pour les respecter et en documentant méticuleusement ce respect ». D'après lui, la conformité dans l'UE s'inscrit dans une approche différente : il s'agit de prouver une analyse approfondie des risques et l'existence d'un plan d'atténuation. « Il ne s'agit pas de simples cases à cocher, mais bien d'une analyse des risques. « Ce qui est requis pour démontrer la conformité diffère subtilement », explique M. Fairtlough. « Peu s'en rendent vraiment compte. Ce fossé culturel représente l'un des défis les plus complexes pour les entreprises ».

La mise en place de cadres opérationnels distincts pour chaque pays ou réglementation n'est ni pratique ni rentable, même pour les géants mondiaux. « Les entreprises ne peuvent pas aborder l'UE de manière isolée », affirme M. Burton. « Il est impossible d'établir un cadre de protection des données uniquement pour un pays ou un continent. Les menaces se jouent des frontières, tout comme les données. Cela accroît donc considérablement la complexité pour les entreprises ».

« Il est impossible d'établir un cadre de protection des données uniquement pour un pays ou un continent. Les menaces se jouent des frontières, tout comme les données. Cela accroît donc considérablement la complexité pour les entreprises », déclare Cédric Burton, co-président mondial et associé en charge des données, de la confidentialité et de la cybersécurité chez Wilson Sonsini.

« Le volume de données disponible aujourd'hui peut submerger les organisations mal préparées. Il est donc essentiel de disposer des bons outils et de l'expertise pour tirer parti de l'IA et du big data », déclare Rasmussen, analyste chez GRC 20/20 Research.

D'autre part, M. Rasmussen recommande aux organisations de créer un « cadre unifié de gestion des risques et de la résilience, aligné sur les réglementations nationales et internationales ». Il précise que cela devrait inclure « l'utilisation de la technologie pour une surveillance continue et la promotion d'une culture de la conformité à tous les niveaux de l'organisation ». À titre de mesure concrète, M. Rasmussen recommande à ses clients d'« intégrer la conformité dans leurs opérations quotidiennes ». Cela permet aux organisations d'éviter les sanctions, de renforcer leur posture de sécurité globale, et d'être mieux préparées face aux menaces ».

Les entreprises présentes en Asie-Pacifique, notamment en Chine, doivent également se conformer aux nouvelles réglementations en matière de protection des données, de respect de la vie privée et de lutte contre le blanchiment d'argent. Burton et Fairtlough relèvent que la deuxième puissance économique mondiale présente des défis de conformité pour toutes les entreprises qui y opèrent. « Le cadre juridique chinois est particulièrement complexe à appréhender », déclare Burton. Il illustre cela par les restrictions sur le transfert de données : « Lorsque vous touchez à certains types de données en Chine, une autorisation réglementaire est obligatoire ». En Chine, par exemple, les organisations ne peuvent recourir au chiffrement que si le gouvernement dispose également d'une clé d'accès.

Malgré des divergences régionales, M. Fairtlough observe une certaine uniformité dans les protections, technologies, et processus déployés par les entreprises à l'échelle mondiale. « Les processus techniques employés pour protéger vos données sont, dans l'ensemble, similaires », déclare-t-il. « La différence est dictée par des exigences réglementaires ou légales, comme la localisation des données, c'est-à-dire leur lieu de stockage ». Ces divergences réglementaires influent aussi sur les autorisations nécessaires à la mise en place de certaines mesures de protection technique. Par exemple, certains contrôles de données qu'une entreprise peut appliquer de manière autonome aux États-Unis peuvent nécessiter l'approbation d'un comité d'entreprise en Allemagne ou en France. Vous devez tenir compte de cette [approbation] dans l'analyse globale des risques ».

L'IA : un véritable changement de paradigme

La cyberrésilience ne se limite pas à surmonter les incidents. Elle vise à garantir la continuité des opérations et une récupération rapide en cas d'incident.

L'IA peut s'avérer un atout précieux dans ce contexte. « L'IA joue un rôle clé dans la sécurisation des entrepôts de données cloud, en renforçant la détection des menaces, en automatisant les réponses aux incidents et en identifiant les vulnérabilités avant qu'elles ne soient exploitées par des acteurs malveillants », précise M. Rasmussen. Les outils propulsés par l'IA, explique-t-il, ont « indéniablement » transformé les complexités de la gestion des cyber-risques et de la conformité réglementaire. « Ces technologies requièrent également des cadres de gouvernance robustes pour gérer les risques qu'elles engendrent, comme les biais algorithmiques et les questions de confidentialité des données », observe-t-il. « Par ailleurs, le volume de données disponible aujourd'hui peut submerger les organisations mal préparées. Il est donc essentiel de disposer des bons outils et de l'expertise pour tirer parti de l'IA et du big data ».

Malgré ses avantages, l'IA introduit également de nouveaux cyberrisques et expose les organisations à des vulnérabilités susceptibles de nuire à leurs relations avec leurs clients et partenaires. Bien que les équipes de sécurité et réseau utilisent des outils de surveillance basés sur l'IA pour repérer les cybermenaces, les « acteurs malveillants disposent de la même technologie », observe Burton. « D'un côté, l'IA est censée à sécuriser le réseau d'une entreprise, mais elle est également exploitée par des acteurs malveillants pour lancer de nouvelles attaques ». Les « deepfakes », qui manipulent numériquement le visage et le corps d'une personne à des fins malveillantes, sont désormais « un des principaux défis pour les entreprises », ajoute-t-il. « Il est aujourd'hui très facile de créer un deepfake avec la technologie IA actuelle ». M. Burton souligne que les réglementations actuelles sont « rapidement dépassées par l'évolution accélérée de la technologie ».

La récente loi européenne sur l'IA propose de réglementer l'usage des systèmes d'IA au sein de l'UE. Comme d'autres réglementations européennes telles que DORA et NIS2, cette loi adopte une « approche basée sur le risque », classant les systèmes d'IA selon les risques qu'ils peuvent présenter. Plus l'application est risquée, plus les contrôles sont stricts. Par exemple, la loi interdit la manipulation des individus et les « jouets vocaux incitant les enfants à des comportements dangereux ».[5] Entre autres mesures, la loi impose des normes de transparence et exige que les organisations informent les clients qu'ils interagissent avec un chatbot et non pas avec un être humain. Les dispositions de cette loi seront appliquées progressivement sur trois ans, et les amendes pour non-conformité pourraient atteindre 35 millions d'euros ou entre 1 % et 7 % du chiffre d'affaires annuel, selon le montant le plus élevé.

« L'IA est actuellement le sujet le plus brûlant en matière de réglementation. Tous les organismes de réglementation mondiaux tentent de s'emparer de ce sujet : cela concerne l'antitrust, les régulateurs de la vie privée en UE, et maintenant les régulateurs de l'IA avec les nouvelles réglementations relatives à l'IA », observe M. Burton de Wilson Sonsini.

M. Fairtlough, de KPMG, conseille aux organisations de définir comment et où leurs données seront analysées, ainsi que ce qu'elles savent de leur utilisation en matière de confidentialité.

« L'IA est actuellement le sujet le plus brûlant en matière de réglementation », affirme M. Burton. Tous les organismes de réglementation mondiaux tentent de s'emparer de ce sujet : cela concerne l'antitrust, les régulateurs de la vie privée dans l'UE, et à présent les régulateurs de l'IA avec les nouvelles réglementations ». Il avertit qu'il sera « extrêmement complexe pour une organisation d'identifier chaque réglementation et de garantir sa conformité ».

Une planification proactive est nécessaire pour éviter les écueils réglementaires. M. Fairtlough souligne que, pour établir des fondations solides à l'utilisation de l'IA, il est essentiel de bien comprendre sa situation financière. « Comment peut-on envisager une planification financière à long terme sans savoir précisément quels fonds on possède, quels comptes sont ouverts, ce qui est dû et quelles créances sont en cours ? », interroge-t-il. « En pratique, les données et la technologie permettent de générer de la valeur ». M. Fairtlough conseille aux organisations de définir comment et où leurs données seront analysées, ainsi que ce qu'elles savent de leur utilisation en matière de confidentialité. Il recommande d'évaluer les impacts potentiels d'interruptions de service, de problèmes techniques ou d'obstacles réglementaires.

Pour M. Fairtlough, une fois cette évaluation réalisée, les organisations seront en mesure d'utiliser pleinement des grands modèles de langage, « car je sais où cibler mes données et je connais celles qui m'appartiennent », précise-t-il. « Cela me permet d'établir une gouvernance sur ces données, en ayant la certitude d'utiliser des données collectées légalement, intégrées à mon ensemble d'analyses, et dont les résultats sont fiables ». Enfin, il se poserait la question : « Quelles mesures ai-je prises pour sécuriser ces données en fonction des risques qu'elles représentent pour mon entreprise ? » Les avancées en recherche IA pourraient grandement aider les organisations, depuis la prévention des menaces jusqu'à la génération automatique de rapports de conformité répondant aux exigences mondiales. Rasmussen estime que l'IA et le machine learning offriront des solutions pratiques aux organisations dans les trois à cinq prochaines années. « L'IA jouera un rôle crucial pour garantir la conformité, automatiser les audits et fournir des informations en temps réel sur la posture de sécurité d'une organisation », explique-t-il.

M. Burton anticipe que les outils IA renforceront considérablement la détection des menaces, permettant une analyse en temps réel des dangers imminents pour les organisations. « La restauration des systèmes sera plus efficace, car de nombreuses tâches seront automatisées », précise-t-il. Il prévoit également un « chiffrement IA automatisé, permettant d'adapter le modèle de chiffrement en temps réel selon le type de menace ».

Conclusion

La voie vers la cyberrésilience et la conformité réglementaire débute par l'implication de la direction, souvent avec le soutien du conseil d'administration. Les organisations présentes sur les marchés mondiaux doivent respecter un nombre croissant de réglementations visant à protéger les données et à éviter les perturbations des chaînes d'approvisionnement et du commerce numérique, afin de les rendre responsables de leurs actions ou manquements.

Cependant, la menace de lourdes amendes n'est pas le seul facteur incitant les entreprises à renforcer leur résilience et leurs défenses cyber. Les interruptions de service imprévues, comme les pannes de réseau ou de cloud, les attaques par ransomware et les pertes de données, représentent également un coût et mettent en péril la confiance des clients, partenaires et parties prenantes. La principale raison qui pousse les conseils d'administration à investir dans la résilience, selon 49 % des sondés dans l'enquête de PwC de décembre 2023, est de « réduire les pertes dues aux futures perturbations ».[6]

Comment les organisations répondront-elles aux exigences strictes des réglementations comme la directive NIS2 de l'UE, axée sur la sécurité, et la DORA, centrée sur la résilience ? Des tests rigoureux, l'utilisation de salles blanches et une gestion accrue des risques peuvent renforcer la cyberrésilience. Cependant, l'IA ne constituera pas une solution immédiate et universelle. Un nombre croissant d'outils IA aide les entreprises à détecter les menaces, mais les gouvernements et les acteurs économiques s'inquiètent des risques cybernétiques liés aux erreurs et aux deepfakes générés par l'IA. Les nouvelles réglementations de l'UE, ainsi que la législation californienne en préparation, cherchent à réduire les biais algorithmiques et à limiter les atteintes à la confidentialité des données.

Si la réglementation DORA, parmi d'autres, peut encourager certaines organisations à renforcer leur résilience cybernétique, il reste essentiel de gérer données et opérations cybernétiques avec la plus grande intelligence. « Ces réglementations obligent les organisations à revoir leurs stratégies de gestion des risques, en mettant davantage l'accent sur la surveillance continue, la réponse aux incidents et les capacités de récupération », précise M. Rasmussen. « Les organisations doivent ajuster leur posture non seulement pour se conformer, mais pour aller au-delà des exigences réglementaires. En procédant ainsi, elles protègent leurs opérations contre des défis nouveaux et imprévus, garantissant ainsi leur conformité, leur robustesse et leur adaptabilité face aux risques émergents ».

Notes de fin

1 Thomson Reuters, « The 2023 Thomson Reuters Risk & Compliance Survey Report », 13 octobre 2023. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/risk-compliance-survey-report-2023/.

2 PwC, « PwC's Global Crisis and Resilience Survey 2023 », décembre 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

3 Parametrix, « CrowdStrike's Impact on the Fortune 500 », 24 juillet 2024. https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

4 Le Forum économique mondial, « Global Cybersecurity Outlook 2023 », janvier 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.

5 Le Parlement européen, « EU AI Act : first regulation on artificielle intelligence », 8 juin 2024. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

6 PwC, « PwC's Global Crisis and Resilience Survey 2023 », décembre 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

Harvard Business Review
ANALYTIC SERVICES

À PROPOS DE NOUS

Harvard Business Review Analytic Services est une unité de recherche commerciale indépendante au sein du groupe de la Harvard Business Review qui effectue des recherches et des analyses comparatives sur les principaux problèmes de gestion et les nouvelles opportunités commerciales. Chaque rapport est publié en fonction des conclusions de recherches et d'analyses quantitatives et/ou qualitatives originales, dans le but de fournir des informations commerciales et les perspectives d'un groupe de pairs. Les enquêtes quantitatives sont réalisées avec le conseil consultatif de HBR, le panel de recherche mondial de HBR, et la recherche qualitative est menée avec des hauts dirigeants d'entreprises et des spécialistes du domaine issus de la communauté des auteurs de la *Harvard Business Review. Envoyez-nous un e-mail à hbranalyticservices@hbr.org.*

hbr.org/hbr-analytic-services

MCCRE54701024