kyndryl

Résultats de l'enquête

Ce que les décideurs informatiques disent de l'état des risques informatiques

Les risques informatiques est devenu un sujet de discussion dans les conseils d'administration.

Dans un monde où les organisations utilisent des systèmes informatiques complexes, géographiquement dispersés et hybrides, une panne de réseau, une attaque d'un logiciel malveillant ou toute autre perturbation du système peut avoir des effets dévastateurs sur la productivité, la réputation et les résultats d'une marque.

C'est la raison pour laquelle les conseils d'administration de nombreuses entreprises demandent à leurs équipes dirigeantes des informations précises sur la préparation à un tel incident.

Compte tenu des enjeux importants, nous avons cherché à évaluer les perceptions des risques informatiques et les mesures prises par les organisations pour mettre en oeuvre la cyber-résilience. Nous avons interrogé un panel mondial de décideurs informatiques et de professionnels du risque et de la conformité pour connaître les problèmes qu'ils ont rencontré, les risques informatiques qui les préoccupent le plus et les mesures prises par leur entreprise pour anticiper les risques, s'en protéger, y résister et reprendre les opérations.

Les résultats de cette enquête constituent le rapport 2023 sur l'état des risques informatiques.

Nos résultats confirment que les systèmes informatiques des organisations sont effectivement perturbés. Nous avons identifié les obstacles les plus fréquents à l'atténuation des perturbations. Nous avons également constaté, et été surpris, par le haut niveau de confiance des responsables informatiques dans les capacités de leur organisation à gérer et à reprendre les opérations après des perturbations informatiques.

Nous vous invitons à considérer ces résultats comme une référence pour votre propre stratégie d'atténuation des risques informatiques. Outre les résultats de l'enquête, nous proposons neuf étapes vers la mise en oeuvre de la cyberrésilience.

Dans le cadre de l'émission The Progress Report, j'ai également discuté des résultats avec Ricardo Morales, RSSI de Banorte, l'une des plus grandes banques commerciales du Mexique.

Comment nous avons obtenu les données

Nous avons fait appel à une société tierce pour mener une enquête en ligne auprès de 300 décideurs informatiques de grandes entreprises (plus de 1 000 employés). Les réponses ont été collectées de mars à avril 2023.

Emplacement des répondants :

- → 65% Amérique du Nord
- → 19% Royaume-Uni
- → 16% Inde

Secteurs d'activité :

- → 18% services financiers
- → 17% administration
- → 17% Fabrication
- → 14% Ttélécommunications
- → 14% médias
- → 20% Autre

à propos de l'auteur

Kris Lovejoy est le responsable mondial de la pratique de Kyndryl pour la sécurité et la résilience.

L'informatique est au centre des processus métier critiques des organisations.

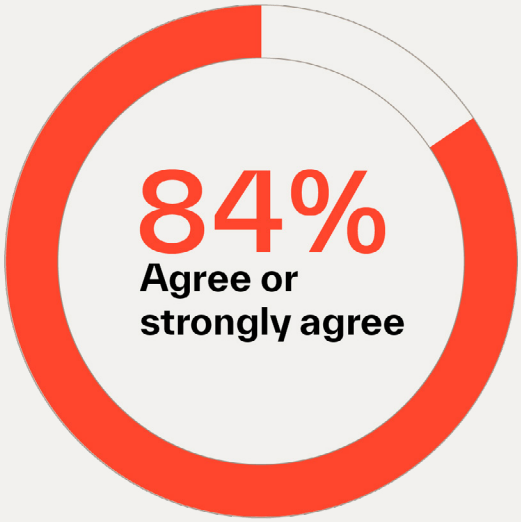
Pour ancrer la discussion sur les risques informatiques, nous avons demandé aux répondants d'indiquer dans quelle mesure leur activité quotidienne repose sur l'informatique.

84 % sont d'accord ou tout à fait d'accord sur le fait que leur organisation dépend grandement des actifs informatiques pour exécuter les processus métier critiques.

Ce résultat n'est pas surprenant, étant donné les commentaires quotidiens et systématiques sur la transformation numérique.

Ce qui est peut-être plus surprenant, c'est que la réponse n'ait pas été encore plus catégorique.

Q : Dans quelle mesure êtes-vous d'accord ou non : "Mon organisation s'appuie fortement sur les actifs informatiques pour mettre en oeuvre des processus commerciaux essentiels.



La plupart des organisations ont dû faire face à des perturbations de leurs systèmes informatiques.

Nous avons non seulement validé la criticité des systèmes informatiques, mais aussi le fait que les perturbations vont de pair avec le territoire. 92 % des répondants indiquent que leur organisation a subi, au cours des deux dernières années, un événement indésirable qui a compromis ou perturbé les systèmes informatiques. Oui, les affaires impliquent d'assumer les risques informatiques.

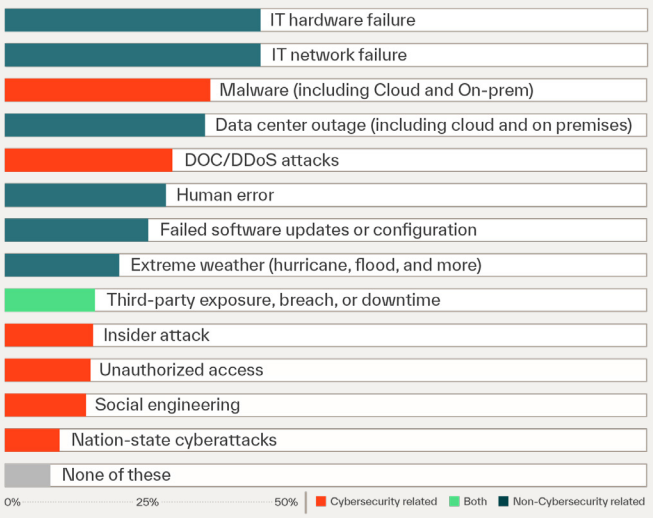
La plupart des répondants indiquent avoir été confrontés à trois ou quatre types de perturbations différentes. Si les cyber-attaques ont tendance à faire la une des journaux, les résultats montrent qu'une ouverture beaucoup plus large s'impose lorsqu'il s'agit des risques informatiques et de les traiter.

Si 71 % des répondants déclarent avoir connu un problème de cybersécurité, 88 % indiquent qu'ils ont dû faire face à un événement indésirable non lié à la cybersécurité (il ne s'agit pas d'une distinction entre les deux catégories). En fait, trois des cinq principaux événements indésirables n'étaient pas liés à la cybersécurité :

- → Dysfonctionnement du matériel informatique
- → Dysfonctionnement du réseau informatique
- → Indisponibilité du centre de données

Notamment, l'erreur humaine reste également une source clé de perturbation. Elle occupe la sixième place parmi les 13 perturbations spécifiques sur lesquelles nous avons posé des questions et elle a figure de manière constante parmi les trois premières perturbations citées par les répondants du secteur des services financiers.

Q : Au cours des 24 derniers mois, l'un des événements indésirables suivants a-t-il compromis ou perturbé vos systèmes informatiques/données ?



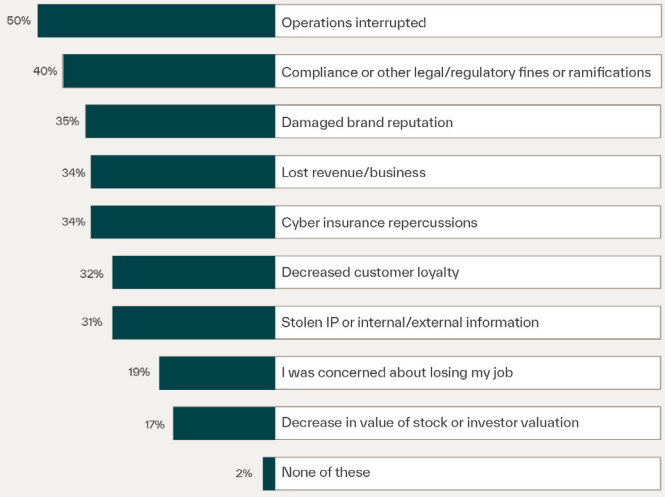
Les perturbations des systèmes informatiques ont porté atteinte à des marques et entraîné des amendes et bien d'autres déconvenues.

Sur la base de l'importance de l'informatique pour les opérations quotidiennes, les répondants citent les perturbations opérationnelles comme l'impact le plus courant causé par des incidents informatiques défavorables, la conformité ou les autres sanctions financières ou conséquences juridiques ou réglementaires étant le deuxième plus fort impact. C'est particulièrement vrai pour les répondants des secteurs des services financiers, de l'administration et des médias.

Non seulement les perturbations opérationnelles et les catégories de conformité sont les plus courantes, mais les répondants les classent également parmi les deux catégories d'impacts les plus préoccupants en cas d'indisponibilité ou de compromission future des actifs informatiques. Les interruptions par déni de service et les violations de données, par exemple, peuvent entraîner de lourdes amendes.

35 % des répondants déclarent que la réputation de la marque de leur organisation a été ternie par des perturbations informatiques. Ce résultat est particulièrement vrai parmi les répondants des organisations du secteur des médias, 63 % ayant noté un tel impact. Le cycle de l'information en continu et l'activité des clients sur les médias sociaux rendent tout événement indésirable plus visible que jamais.

Q : Parmi les impacts suivants, quels sont ceux que votre organisation a subis à la suite d'événements indésirables [au cours des 24 derniers mois] ?



Alors, qu'est-ce qui empêche les décideurs informatiques d'anticiper les risques informatiques ?

Nous pensions que la pénurie mondiale de compétences informatiques figurerait en bonne place parmi les facteurs d'atténuation, mais elle n'est pas tout à fait en tête de liste. L'incapacité de restaurer les systèmes et les données à partir d'une sauvegarde chiffrée et propre est apparaît le plus souvent comme l'un des principaux défis auxquels les répondants ont dû faire face pour gérer l'impact des événements indésirables. C'est également ce que nous constatons souvent dans les organisations qui nous demandent des services. Nous les encourageons à :

- → Investir dans l'automatisation et l'orchestration des processus de reprise
- → Évaluer et déterminer la meilleure façon de limiter les erreurs humaines lors de la restauration à partir des sauvegardes
- → Tester les plans de réponse aux incidents de manièrerépétée et fréquente

Les trois principaux défis rencontrées par les répondants pour atténuer les risques figurent l'expansion des espaces informatiques et la capacité à se tenir informé sur les nouvelles menaces. Le manque de personnel informatique qualifié arrive en quatrième position.

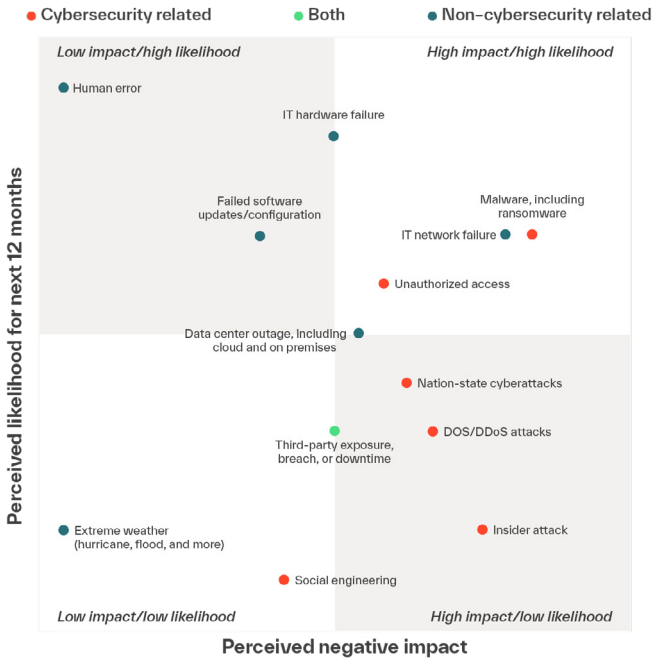
Pour les 12 prochains mois, les incidents provoqués par des logiciels malveillants sont considérés comme le risque informatique le plus probable et le plus négatif.

Pour les 12 prochains mois, les incidents provoqués par des logiciels malveillants sont considérés comme le risque informatique le plus probable et le plus négatif.

Nous avons demandé aux répondants de nous indiquer les événements indésirables les plus susceptibles de se produire au cours des 12 prochains mois et l'impact qu'ils pourraient avoir sur leur organisation.

Ils considèrent l'erreur humaine comme la plus probable, mais son impact possible est moins fort que celui de la plupart des autres événements. En revanche, les logiciels malveillants constituent, selon eux, le risque informatique le plus élevé et le plus menaçant.

Compte tenu de l'augmentation des logiciels malveillants, en particulier les ransomwares, les résultats ne sont pas surprenants. Si l'on tient compte des difficultés évoquées plus haut liées à la récupération des données à partir de sauvegardes chiffrées propres, on peut également y voir une raison de l'attention particulière apportée à la question. Que votre organisation soit ou non confrontée à des problèmes de sauvegarde, le ciblage croissant des sauvegardes par les auteurs de ransomwares complique les choses. Dans ces scénarios, lorsque les sauvegardes sont compromises, les organisations ne peuvent pas restaurer les systèmes ni vérifier la présence de logiciels malveillants. Par conséquent, les risques et les impacts potentiels augmentent de manière exponentielle.



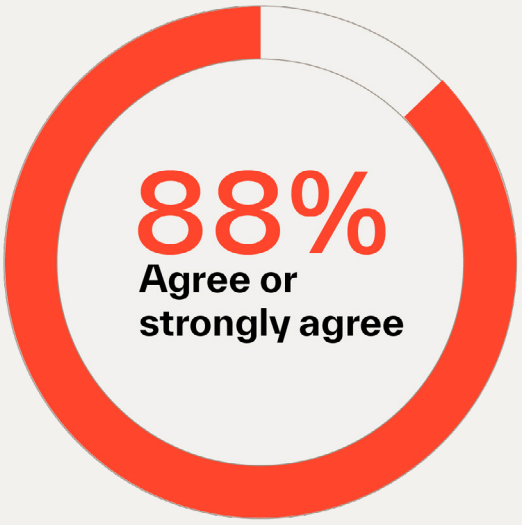
Un autre risque très redouté et potentiellement important, les accès non autorisés, est également considéré comme ayant des conséquences négatives importantes. Les principes Zero Trust continueront d'occuper une place majeure dans la gestion des accès non autorisés. Ces principes exigent que les organisations identifient leurs actifs de grande valeur, déterminent les accès avec privilèges et utilisent des technologies, telles que l'authentification multifacteur, pour les valider.

Malgré les risques que les décideurs informatiques perçoivent, ils restent confiants.

Nous avons mentionné dans ce rapport notre surprise quant à la confiance des décideurs informatiques, compte tenu des événements mondiaux et des défis relevés. En fait, 88 % des répondants s'accordent à dire que leur organisation est bien préparée pour gérer et rependre les opérations à la suite d'événements défavorable, d'attaques ou de compromissions qui perturbe les actifs informatiques de leur organisation.

Lorsqu'on leur demande de se situer par rapport à leurs pairs, 65 % des répondants estiment que leur organisation est mieux préparée que les autres organisations à faire face à des événements indésirables. Seuls 8 % d'entre eux se considèrent moins bien préparés. Ce niveau élevé de confiance a particulièrement attiré notre attention étant donné que 92 % des répondants, comme nous l'avons vu, indiquent également que leur organisation a connu des événements indésirables. Cette dualité est pour le moins surprenante, si ce n'est une raison de s'interroger sur le bienfondé d'une telle confiance.

Q : Dans quelle mesure êtes-vous d'accord ou non : Mon organisation est bien préparée à gérer et à récupérer les conditions défavorables, les attaques ou les compromissions qui perturbent ses actifs informatiques.



9 étapes à suivre par les responsables informatiques vers la cyber-résilience

Nous avons effectué cette enquête pour évaluer la façon dont les décideurs informatiques perçoivent l'état actuel des risques informatiques et les mesures prises par leurs organisations pour atténuer ces risques, en s'appuyant sur les quatre piliers de la cyberrésilience.

- → **Anticiper:** actions qui visent à évaluer et à comprendre le degré d'exposition aux risques informatiques, afin d'atténuer plus efficacement les menaces potentielles et de maîtriser les réglementations éventuelles.
- → **Protéger:** actions qui visent à renforcer les protections des actifs informatiques, afin de s'assurer qu'ils sont à l'abri d'événements indésirables.
- → **Surmonter:** actions qui visent à gérer les perturbations et à en réduire l'impact.
- → **Rétablir:** actions qui visent à atténuer l'impact d'une perturbation et à rétablir rapidement les environnements informatiques essentiels.

Les répondants considèrent systématiquement que leur organisation est performante, d'où les scores de confiance élevés. En moyenne, pour l'ensemble des activités, 75 % des répondants considèrent que leurs performances sont très bonnes, voire excellentes. Nous avons relevé un point intéressant dans la mesure où les répondants qui font état d'un fort soutien de la direction pour investir dans la sécurité sont plus enclins à s'attribuer de très bonnes notes pour les activités liées à la cyber-résilience.

Pour vous aider à obtenir cette adhésion, nous vous proposons neuf étapes fondamentales vers la cyber-résilience.

1 **Engagez l'entreprise dès le début.**

Les services informatiques fonctionnent trop souvent en vase clos, à l'écart des autres secteurs de l'entreprise. La voie la plus sûre pour mener à bien une stratégie de cyber-résilience consiste à briser le cloisonnement. Invitez des personnes extérieures aux services informatiques à la table de discussion et fixez les conversations sur la cyber-résilience dans la mission de l'organisation. Intégrez-la dans la culture organisationnelle.

2 **Alignez-la sur la tolérance aux risques.**

Un niveau de tolérance aux risques est souvent dicté par secteur d'activité. Par exemple, le niveau de tolérance d'une institution financière hautement réglementée serait probablement très bas. Quel que soit le niveau, définissez la tolérance aux risques de votre organisation et communiquez-la à vos équipes.

3 **Définissez votre société minimale viable.**

Une entreprise minimale viable représente les éléments de l'organisation qui sont essentiels au maintien des activités et à la réalisation des objectifs de l'entreprise. Votre stratégie de cyber-résilience doit non seulement identifier les éléments critiques, mais aussi les tolérances d'impact.

4 **Faites un inventaire.**

Comme le montrent les résultats de l'enquête, de nombreuses organisations sont confrontées à un espace informatique en expansion perpétuelle. Identifier et cartographier les actifs informatiques qui sont essentiels à votre entreprise minimale viable. Ces actifs devront être protégés en priorité et, dans le pire des cas, rétablis à la suite d'un événement indésirable.

5 **Passez à un framework Zero Trust.**

Nous recommandons d'adopter le refus par défaut pour que seuls ceux qui doivent accéder aux systèmes puissent le faire, et que ceux pour lesquels ce n'est pas nécessaire ne puissent pas le faire.

6 **Établissez un plan gestion des crises.**

Il arrive que des événements indésirables soient inévitables. (Exemple concret : l'erreur humaine est la cause la plus probable des perturbations). La définition des rôles et des responsabilités au sein des équipes, l'établissement d'un processus de communication, la documentation des processus et l'amélioration de la transparence contribuent généralement à réduire l'impact d'un événement indésirable.

7 **Entraînez-vous à faire face à une perturbation.**

Les plans sont trop souvent élaborés, puis mis de côté et rarement mis en pratique. Lorsqu'un événement indésirable se produit, un plan non testé entraîne une certaine confusion et une lenteur de réaction, et l'impact devient plus grave.

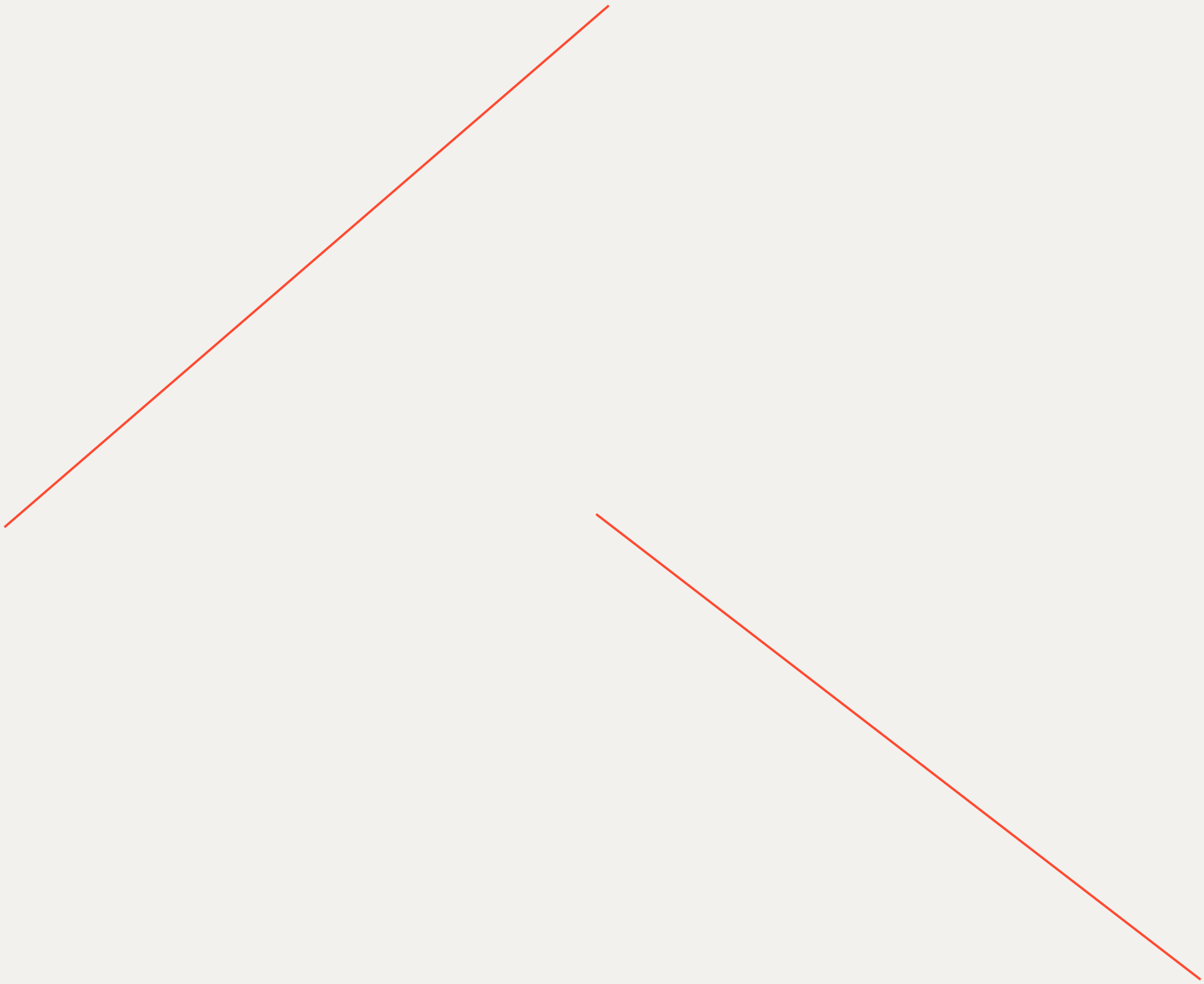
8 **Modernisez continuellement votre stratégie cyberrésilience.**

Les organisations sont des entités vivantes. Les objectifs de l'entreprise évoluent, le parc informatique devient plus complexe et des forces extérieures (les réglementations, par exemple) peuvent exiger des changements. Pour que votre stratégie de cyber-résilience soit efficace, ces étapes doivent faire l'objet d'une discussion permanente.

9 **Sensibilisez jusqu'au conseil d'administration.**

Nous terminons ce rapport d'enquête là où nous l'avons commencé, en attirant l'attention sur le fait que la cyber-résilience est devenue un sujet de discussion au niveau des conseils d'administration dans le monde entier.

Informer le conseil d'administration des risques informatiques et des plans d'atténuation de ces risques peut contribuer à l'alignement organisationnel de haut en bas et fournir une protection pour les changements nécessaires, afin de garantir que les systèmes cybernétiques puissent rester opérationnels.



kyndryl