Démontrer l'utilité des investissements en matière de continuité et de résilience

Réputation de l'entreprise et risque informatique : quel enjeu économique et quel impact pour les professionnels de la continuité et de la résilience ?

Implications de l'étude IBM Global Study sur l'impact économique des risques informatiques

Sommaire

Introduction

L'époque où les professionnels de la continuité se consacraient exclusivement à rétablir le fonctionnement des ordinateurs suite à un incident majeur est désormais terminée. La disponibilité continue est devenue une condition obligatoire des pratiques de continuité opérationnelle et de résilience à l'échelon de toute l'entreprise. La prévention, et non la réaction, est devenue une priorité et la reprise après incident n'est que l'un des éléments de la problématique. Les spécialistes de la continuité et de la résilience ont donc vu s'élargir considérablement la portée de leurs responsabilités : garantie de la viabilité et de la conformité du système, évaluation des fournisseurs, sauvegarde et stockage des données, gestion des budgets et définition des priorités, pour n'en citer que quelques-uns.

Et quel que soit le domaine de responsabilité concerné, le facteur coût doit toujours être surveillé. Selon les répondants spécialisés en continuité et en résilience, interrogés dans l'étude IBM Global Study sur l'impact économique du risque informatique, les interruptions d'activité et les pannes informatiques coûteront £13 millions à une entreprise au cours des 24 prochains mois.

Il s'est révélé difficile de justifier les investissements dans les initiatives de continuité et de résilience, car des données détaillées sur la durée et le coût des tests n'étaient pas disponibles. L'étude IBM Global Study sur l'impact économique des risques informatiques est la plus grande étude de cette catégorie. Elle interroge au total 2316 professionnels de l'informatique dont 1069 spécialistes de la continuité opérationnelle.

Chaque spécialiste a répondu à des questions précises sur les types de pannes subies par son entreprise, et sur leurs causes. Leurs réponses, qui figurent dans ce rapport d'analyse, vous fournissent les données de test dont vous avez besoin pour étoffer votre stratégie existante de gestion du risque informatique. Elles prouvent l'importance de la continuité et de la résilience informatiques, et vous permettent de constituer l'étude de rentabilité qui vous aidera à justifier le budget et les ressources dont vous avez besoin pour réussir.

Les menaces et leur coût

Pour aider les répondants à identifier les types de menaces qui provoquent des interruptions métier et informatiques et les types de coûts qui en résultent, l'étude IBM Global Study sur l'impact économique des risques informatiques a dressé la liste des menaces et des catégories de coût courantes à l'attention des professionnels de l'informatique. Les répondants devaient évaluer :

Six menaces courantes

1. Erreur humaine
2. Défaillance du système informatique
3. Atteinte à la cyber-sécurité ou aux données/vol de données
4. Incapacité d'un tiers à assurer la continuité ou la sécurité informatique
5. Perte de données suite à l'échec d'une sauvegarde ou d'une restauration
6. Catastrophes naturelles ou d'origine humaine

Six catégories de coûts courantes

1. Atteinte à la réputation et à l'image de marque
2. Perte de productivité en raison d'un temps d'indisponibilité ou des performances du système
3. Perte de chiffre d'affaires en raison de problèmes de disponibilité du système
4. Recherche permettant d'identifier les causes premières
5. Support technique pour la restauration des systèmes
6. Coûts entraînés par un non-respect de la conformité et des réglementations

Quelques bancs d'essais à l'appui de vos études de rentabilité

Justifier les investissements dans des projets de continuité et de résilience repose sur une vérité avérée : ces projets ont une valeur métier qui va bien au-delà du traitement des opérations. Ils ont un impact global, depuis la productivité des employés en passant par l'entreprise et son image de marque. Du point de vue financier, il est logique d'investir dans des solutions robustes de protection de la continuité et de la résilience et de les intégrer dès le départ aux systèmes informatiques. Mieux vaut prévenir que devoir payer le coût d'une correction des pannes lorsque ces dernières se produisent.

Ce rapport récapitule le retour d'informations des spécialistes en continuité en résilience sur les coûts, les causes et les facteurs de risque, tels qu'ils ont été recueillis à l'occasion de l'enquête d'IBM. Si on les ajoute à l'estimation du coût de £13 millions à payer pour atténuer et résoudre les incidents au fur et à mesure qu'ils se produisent, ces résultats sont les preuves concrètes qui faisaient défaut aux études de rentabilité précédentes.

Le coût des interruptions en fonction de leur durée

Plus longue est la durée d'une interruption métier ou informatique, plus son coût est élevé : c'est une question de bon sens. La durée permet cependant de tirer d'autres conclusions.

Les opinions des répondants diffèrent sur la définition d'une interruption, mineure, moyenne ou majeure. Ces variations sont influencées par la sophistication de la stratégie de gestion des risques de leur entreprise et des niveaux de tolérance admis, ainsi que par leur expérience personnelle (voir la Figure 1.)

Les répondants ont affecté une durée précise aux interruptions métier ou informatique mineures, moyennes ou majeures, ainsi qu'une estimation de coût sur les 24 mois à venir. Ils prévoient un coût de £681 000 pour les interruptions mineures, de £2 890 000 pour les interruptions moyennes et de £9 420 000 pour les interruptions majeures. Si le coût des interruptions majeures confirme ce que le bon sens laissait à prévoir, il est important d'observer que ces professionnels de la continuité et de la résilience ne négligent pas non plus les 28 % des coûts entraînés par des interruptions mineures et moyennes, d'autant plus qu'elles se produisent plus fréquemment et sont aussi plus faciles à éviter.

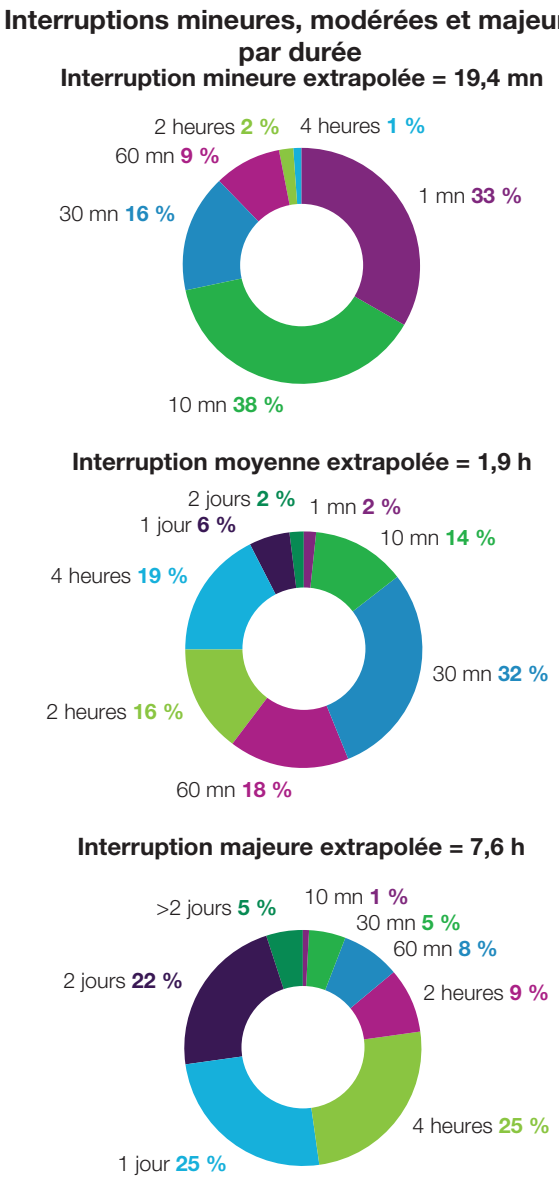


Figure 1. La variation entre la définition donnée par les répondants des interruptions mineures, moyennes et majeures est influencée par les niveaux de tolérance admis dans leur secteur d'activité, ainsi que par leur expérience personnelle.

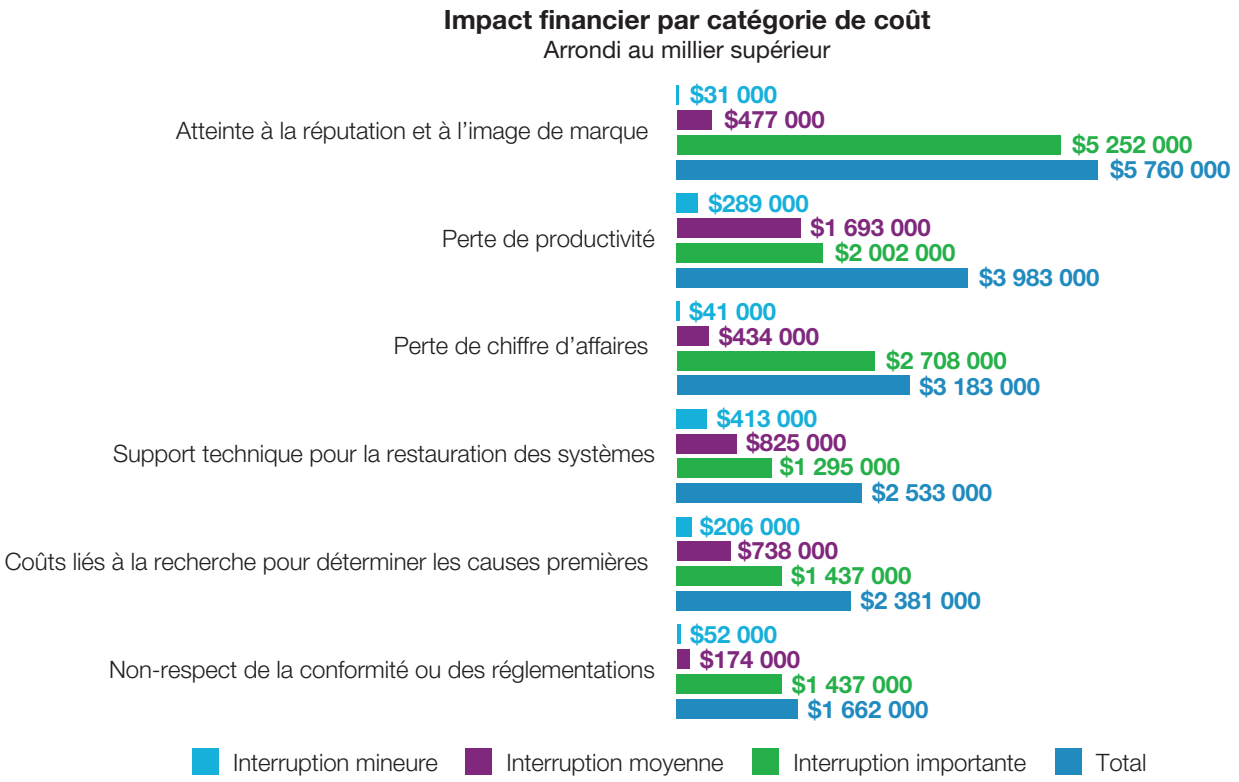


Figure 2. Il a été demandé aux professionnels de la continuité et de la résilience d'évaluer le coût des pannes informatiques en affectant un montant à six catégories courantes. L'atteinte à la réputation et à l'image de marque est globalement la catégorie la plus onéreuse, et en particulier la plus coûteuse dans le cas d'incidents de longue durée.

Coûts par catégorie

L'enquête d'IBM demandait aussi aux répondants d'évaluer le coût des pannes informatiques en affectant un montant en dollars à chacune des six catégories de coût courantes, qui ont été ensuite été comparées avec la durée de l'interruption.

Comme on l'a vu dans la Figure 2, la catégorie la plus onéreuse est globalement l'atteinte à la réputation et à l'image de marque, suivie de la perte de productivité et la perte de chiffre d'affaires. La catégorie la plus onéreuse des incidents de courte durée est le support technique. La catégorie la plus onéreuse des incidents de durée moyenne est la perte de productivité ; en ce qui concerne les incidents de longue durée, c'est l'atteinte à l'image de marque.

Il est intéressant d'observer que la perte de chiffre d'affaires, qui est la troisième catégorie la plus onéreuse, n'est pas l'un des principaux facteurs si l'on examine les résultats du point de vue de la durée. Cela ne signifie pas que les coûts attribués à une perte de chiffre d'affaires soient dépourvus d'importance. En fait, c'est tout le contraire et ces coûts peuvent être très élevés quelle que soit la durée d'une panne informatique. Lorsque la perte du chiffre d'affaires est combinée aux autres coûts (atteinte à la réputation et à l'image de marque, perte de productivité et non-respect des réglementations), ces coûts représentent au total 75 % (soit £9,5 millions) des coûts totaux encourus, chiffre qui vient valider un peu plus encore l'étude de rentabilité.

La continuité opérationnelle est avant tout une question de disponibilité continue et de techniques proactives chargées de protéger cette disponibilité dans toutes les circonstances.

– Paige A Poore, Directrice, Worldwide IBM Business Continuity

Pourquoi les interruptions se produisent : les facteurs du risque informatique

Aucun examen des coûts des pannes informatiques ne serait complet s'il ne répond pas à la question suivante : « Quelle est la cause de ces pannes ? » Dans la Figure 3, les professionnels de la continuité et de la résilience ont évalué six facteurs de risques informatiques courants, classés par impact économique, atteinte à la réputation et probabilité de l'incident.

L'erreur humaine est la cause la plus fréquente des interruptions métier et informatiques, et celle qui a l'impact économique le plus important. Cela est vrai à la fois au sein du service informatique et pour le reste des utilisateurs. L'erreur humaine est aussi à 82 % plus souvent responsable des atteintes à la réputation que les répondants ne l'avaient prévu.

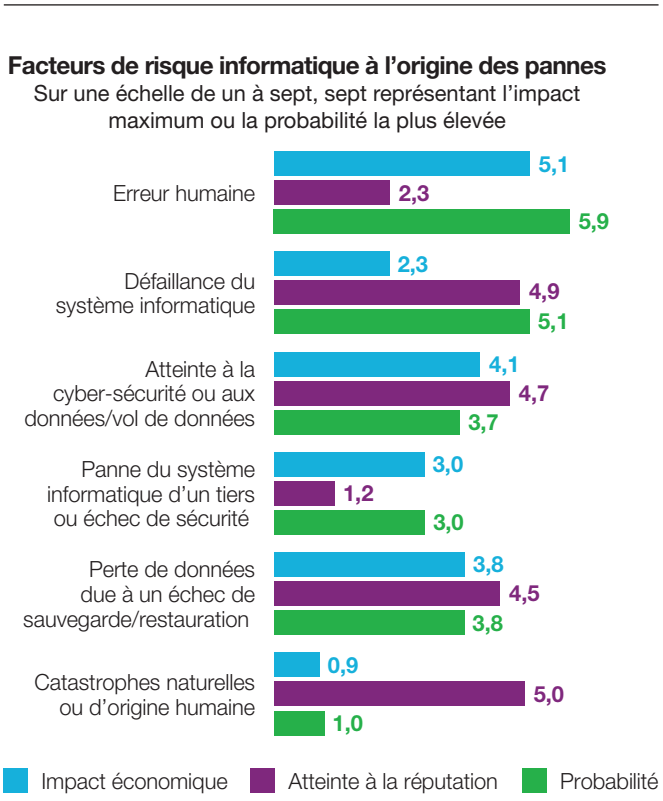


Figure 3. L'erreur humaine est le facteur de risque informatique ayant le plus grand impact économique et la plus grande probabilité de se produire, selon les répondants à l'étude IBM Global Study sur l'impact économique des risques informatiques.

La seule bonne solution pour empêcher l'erreur humaine est d'appliquer l'automatisation dans toute l'entreprise. La solution peut être la virtualisation, une sauvegarde managée ou l'accès via le cloud aux ressources du système, aux logiciels et aux données. Une sauvegarde automatisée pour les utilisateurs individuels, ainsi que la distribution des logiciels et de données sur le cloud, permettent aussi de limiter les interruptions métier et informatiques provoquées par une perte de données ou un codage incorrect des données. Elles peuvent évidemment aussi réduire les coûts du support technique.

La panne d'un système informatique est le deuxième facteur cité par les répondants, à la fois en termes de probabilité d'occurrence et d'impact pour la réputation. Le facteur numéro un responsable de l'atteinte à la réputation est une catastrophe naturelle ou d'origine humaine, mais ces événements se classent toutefois bons derniers sur le plan de l'impact économique et de la probabilité.

La dichotomie entre les estimations chiffrées de l'atteinte à la réputation, de l'impact économique et de la probabilité appliquées aux catastrophes est un bon exemple qui démontre pourquoi il est important de faire figurer ces trois aspects dans l'analyse destinée à l'étude de rentabilité. Les médias sont prompts à dénoncer les problèmes majeurs rencontrés par les systèmes informatiques d'une entreprise, qu'ils soient causés par une tempête ou par une panne informatique grave. La conséquence est que les sinistres sont perçus comme des facteurs à fort impact pour la réputation. Toutefois, comme ils se produisent rarement, ils nécessitent sans doute un budget moins important que celui qui leur était alloué traditionnellement.

L'état des lieux de la continuité opérationnelle aujourd'hui

Un changement majeur s'est opéré dans les initiatives de continuité et de résilience des dernières années. La priorité n'est plus la reprise après incident ou la réaction rapide aux problèmes. La reprise après incident n'est qu'une composante parmi d'autres de la continuité et de la résilience, et la réactivité a cédé la place à la prévention.

Dans de nombreuses entreprises, les programmes de continuité et de résilience ont encore un long chemin à parcourir pour s'améliorer. 20 % seulement des professionnels de la continuité et de la résilience jugent que ces programmes sont pleinement arrivés à maturité, et 13 % ne parviennent pas à déterminer leur degré de maturité. L'atteinte à la réputation et à l'image de marque est la catégorie de coût la plus importante, mais 35 % seulement des répondants déclarent que leurs dirigeants sont conscients de l'impact du risque informatique sur l'image de marque.

La stratégie, un facteur essentiel

Tout programme mature de continuité et de résilience nécessite une stratégie solide et cohérente. 17 % seulement des répondants déclarent que leur entreprise a une stratégie formelle appliquée globalement. 29 % n'ont aucune stratégie. La création ou l'optimisation de votre stratégie de continuité et de résilience peuvent être difficiles, mais il existe des outils qui vous facilitent la tâche.

Un de ces outils est l'Index IBM de continuité des opérations. Cet Index vous guide en vous posant en ligne une série de questions sur les initiatives actuelles de continuité et de résilience dans votre entreprise. Il vous fournit ensuite une analyse des domaines dans lesquels votre stratégie de continuité métier est mature et indique les aspects que vous devez retravailler.

La menace informatique : distinguer la perception de la réalité

Il est fondamental que votre étude de rentabilité et votre stratégie de continuité et de résilience soient basées sur la réalité et confirmées par des faits.

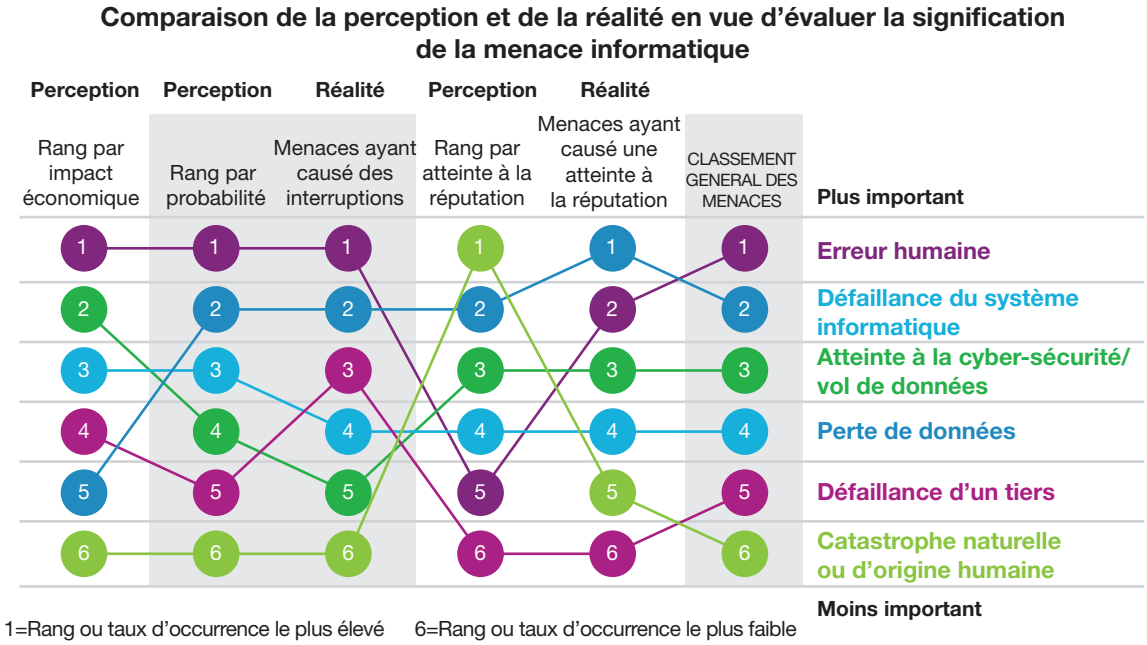


Figure 4. La comparaison des classements affectés par les répondants aux différentes menaces informatiques avec la fréquence réelle de l'occurrence de chaque menace donne une image plus vraie de l'importance des menaces.

Comme nous l'avons vu à la Figure 4, les six menaces informatiques courantes sont comparées en fonction de la perception de leur impact économique, de leur probabilité et de leur capacité d'atteinte à la réputation, mais également de la fréquence à laquelle les menaces ont réellement causé des interruptions et porté atteinte à la réputation de l'entreprise au cours des 24 derniers mois. Ces comparaisons confirment que l'erreur humaine et les pannes du système informatique sont les deux principales menaces informatiques. En même temps, la comparaison met en évidence l'écart énorme entre la perception de l'impact que les catastrophes naturelles ou d'origine humaine ont sur la réputation, et leur impact réel au vu de la classification des menaces, puisqu'elles sont en réalité les moins importantes.

L'avènement des intervenants tiers

La participation des tiers à une grande diversité de fonctions métier de l'entreprise continue à se développer. Mais si leur contribution comporte des avantages, elle entraîne aussi de nouveaux risques informatiques. A l'heure où les entreprises créent des macrocosmes de partenaires, de sous-traitants, de fournisseurs et de consultants de plus en plus vastes et de plus en plus connectés, il va devenir indispensable d'exiger que ces intervenants offrent le même degré de protection contre le risque informatique que l'entreprise avec laquelle ils collaborent.

De nos jours, les pires dangers restent les catastrophes à grande échelle, mais les plus grandes menaces sont les événements banaux tels que les erreurs humaines ou l'arrêt d'un système.

– Laurence Guihard-Joly, directrice générale internationale, Services IBM de continuité opérationnelle et de résilience

Les risques informatiques affectent la réputation

La réputation et l'image de marque d'une entreprise sont pour elles des éléments vitaux. L'informatique joue désormais un rôle important dans leur protection. Les répondants à l'étude IBM Global Study sur l'impact économique des risques informatiques déclarent que les pannes système est la menace informatique qui a eu le plus fort impact sur leur réputation au cours des 24 derniers mois. Venant renforcer ce fait, des données collectées lors de la même étude réalisée en 2012 montrent que l'atteinte à la réputation est le dommage le plus durable que puisse subir une entreprise. Six mois ou plus – soit la moitié de l'exercice – sont nécessaires pour que l'entreprise puisse s'en relever. La menace d'une panne système informatique peut être atténuée grâce à une planification adaptée et des tests fréquents, ainsi que l'automatisation de tâches telles que la sauvegarde et la mise à jour des systèmes d'exploitation et des logiciels.

Evaluez vos pratiques en matière de risque réputationnel

Concernant l'impact du risque informatique pour votre réputation et et votre image de marque, votre entreprise est-elle exposée, consciente ou capable de le gérer ? L'Indice IBM de Risque Réputationnel vous donne la réponse. Répondez à quelques questions. Cet outil IBM en ligne, rapide et simple, vous fournit alors une évaluation globale de vos opérations de gestion du risque réputationnel et informatique, ainsi que des scores dans différentes catégories importantes dans ce domaine, plus des suggestions d'amélioration.

L'externalisation, une force positive

L'externalisation et le conseil sont en passe de devenir des ressources de plus en plus importantes pour une continuité et une résilience métier robustes. La raison pour laquelle les services informatiques recherchent une aide extérieure est claire : ils ont besoin de compétences supplémentaires et/ou de davantage de bande passante. Cela apparaît clairement dans les réponses de 49 % des répondants à l'enquête, selon lesquels leur entreprise a échoué à un audit interne ou externe. A l'heure où cette étude est publiée, 34 % des répondants externalisaient leur gestion de la continuité opérationnelle, tandis que 18 % envisageaient de le faire dans les 18 prochains mois. L'externalisation et le conseil sont en outre plus séduisants que jamais, grâce à un éventail d'options de plus en plus large qui peut être adapté aux besoins particuliers d'une entreprise. Ces options vont des ateliers de stratégie et de planification en passant par les évaluations et le conseil, jusqu'à l'externalisation intégrale.

Un plan d'action pour les professionnels de la continuité opérationnelle

Vous-même et votre entreprise avez tout à gagner à vous ériger en porte-paroles de l'impact économique et réputationnel du risque informatique. L'entreprise se dote d'une nouvelle perspective intéressante lui permettant de filtrer la stratégie et la tactique du risque informatique. En ce qui vous concerne, vous vous positionnez comme un responsable technologique sensibilisé aux aspects financiers, ce qui signifie presque toujours une meilleure visibilité.

Sur la base des résultats de cette étude, IBM propose six étapes qui vous aident à justifier les investissements dans la continuité opérationnelle et la résilience et à obtenir des résultats mesurables. Certaines d'entre elles sont des recommandations que nous avons formulées au cours des cinq dernières années, au cours desquelles nous avons étudié le risque informatique et publié des rapports. D'autres sont fondées sur les nouvelles perspectives et les données plus détaillées de cette étude. Nous espérons ainsi vous aider à pousser plus loin le débat sur la continuité et la résilience dans votre entreprise, et vous fournir des informations essentielles sur le risque réputationnel et l'erreur humaine que vous pourrez communiquer à votre direction.

Faites passer le message du risque réputationnel aux dirigeants de l'entreprise

Près des deux tiers des répondants pensent que leurs dirigeants ne se rendent pas compte que les interruptions métier et informatiques nuisent à la réputation et à l'image de marque de l'entreprise et que ces atteintes impliquent un coût élevé. Aidez les dirigeants à comprendre les conséquences des pannes informatiques sur la réputation et, au passage, créez pour vous-même et vos homologues une image de professionnels informatiques soucieux de protéger cette ressource.

Justifiez les investissements informatiques

Avec en main une preuve irréfutable démontrant que plus de 75 % des coûts liés aux pannes informatiques sont imputables à l'atteinte à la réputation et aux performances métier, vous avez une base de départ concrète qui vous permet de justifier le financement de la continuité et de la résilience. Les directeurs financiers et les responsables des unités commerciales sont habitués à ce que les demandes d'allocation de budget leur soient présentées en termes de projets et de coûts. Adoptez une approche différente. Soulignez le lien entre les investissements en rapport avec la continuité et les objectifs métier quantifiables, tels que l'augmentation de la productivité et des revenus et la protection de la réputation et de la valeur de la marque.

Développez des mesures d'atténuation du risque informatique

Pour continuer à faire progresser votre argument, élaborez des mesures qui établissent un lien entre les résultats des initiatives d'atténuation des risques et l'amélioration des résultats métier. Il est vrai que cette tâche est plus complexe qu'elle ne le paraît au premier abord, car il est difficile de mesurer le résultat de la prévention ou de faire les choses mieux et plus rapidement. Notre stratégie est une approche qui procède de « l'extérieur vers l'intérieur ». Elle consiste à identifier d'abord les objectifs métier que vos dirigeants souhaitent atteindre, puis à déterminer ce que vous pouvez mesurer et comment, afin de pouvoir visualiser les résultats de vos initiatives d'atténuation.

Réduisez le risque d'erreur humaine

L'erreur humaine est la principale cause des interruptions métier et informatiques. Soyez proactifs et évaluez des solutions d'automatisation dans la perspective d'une réduction des erreurs humaines et non d'une réduction des coûts informatiques. Par exemple, l'automatisation de la sauvegarde sur toutes les plates-formes utilisateur et serveur permet d'éviter toute une gamme d'erreurs humaines dont les conséquences sont multiples : perte de données, configuration incorrecte d'un logiciel de sauvegarde, omission de sauvegarde, voire perte d'un ordinateur personnel.

Mettez en place la collaboration

Selon 41 % des répondants, la collaboration entre les différentes fonctions de l'entreprise en matière de gestion de la continuité métier est médiocre, voire inexistante. Alors même que les technologies deviennent plus complexes et que les domaines du risque informatique se recoupent, la collaboration est extrêmement importante.

Demandez une aide extérieure

Une collaboration avec des spécialistes externes qui ont un point de vue différent permet d'aborder les anciens problèmes sous un nouvel angle, et d'identifier les nouveaux défis qui surgissent avec l'arrivée des nouvelles technologies. Les consultants informatiques vous aident à déterminer une stratégie d'atténuation du risque informatique et à élaborer un plan de mise en œuvre, et vous aident aussi à monter une étude de rentabilité. Ils aident aussi les entreprises à définir les aspects de la continuité opérationnelle et de la résilience qu'il est préférable de confier à un fournisseur de services informatiques possédant davantage de compétences, de ressources ou de technologies. Pour les entreprises de taille modeste qui ont du mal à recruter des spécialistes ou certains secteurs d'activité ou industries tels que la santé dans lesquels les équipes informatiques sont relativement réduites, l'utilisation de services managés pour toutes les activités de gestion de la continuité métier peut être un choix judicieux.

Comment IBM peut vous aider

A condition d'être planifiées et implémentées efficacement, la stratégie et la gestion de la continuité opérationnelle peuvent devenir des avantages concurrentiels vitaux. En protégeant votre entreprise des risques et en les atténuant, vous pouvez améliorer sa valeur de marque vis-à-vis des clients, des partenaires et des analystes. De plus, votre entreprise peut être plus attractive pour de nouveaux clients, peut retenir des clients existants et générer des revenus plus importants.

Pour vous faire une idée globale des risques auxquels votre entreprise est exposée, nous vous conseillons de commencer par un Atelier de gestion du risque informatique. Les consultants IBM collaborent avec vous et vous fournissent une évaluation globale des risques dans toutes les couches de l'entreprise : processus, technologies, applications et données, ainsi que votre infrastructure informatique physique et vos sites. Un Atelier CORE (Évaluation des Risques liés aux Opérations Continues) aide à déterminer la capacité de votre entreprise à assurer la continuité des opérations. Concernant la résilience à l'échelle de toute l'entreprise, les Services IBM SmartCloud Resilience proposent des services cloud managés à la demande. Ils constituent une solution économique pour protéger les données, les applications et les opérations en cas d'indisponibilité. Ils permettent aussi de restaurer rapidement les données et les opérations suite à une interruption.

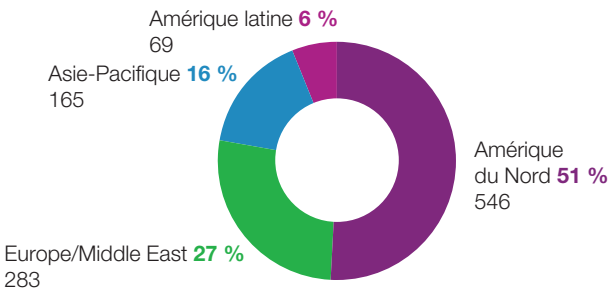
À propos de l'étude

L'étude IBM Global Study sur l'impact économique des risques informatiques est la plus grande étude indépendante réalisée à ce jour, dans le but de mesurer les conséquences financières et réputationnelles des interruptions métier ou informatiques, suite à des incidents de continuité opérationnelle ou de sécurité informatique. Cette étude, qui fait suite à celle conduite en 2013 sur les risques liés à la réputation (intitulée l'« IBM Reputational Risk and IT Study »), a été commandée par IBM et réalisée indépendamment par le Ponemon Institute® en juillet 2013.

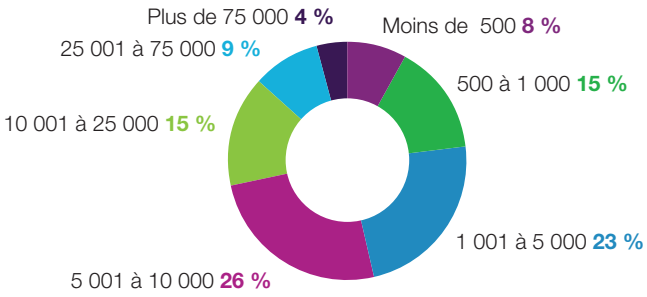
L'étude s'est limitée aux professionnels de l'informatique dont l'activité se concentre sur la continuité des opérations, la sécurité informatique ou les deux, et dont les responsabilités sont liées à la prise de décisions ou aux performances. Dans le cadre de la présente analyse, seules les réponses des professionnels de la continuité opérationnelle ont été intégrées aux données.

Nombre total de répondants spécialisés en continuité opérationnelle : 1069

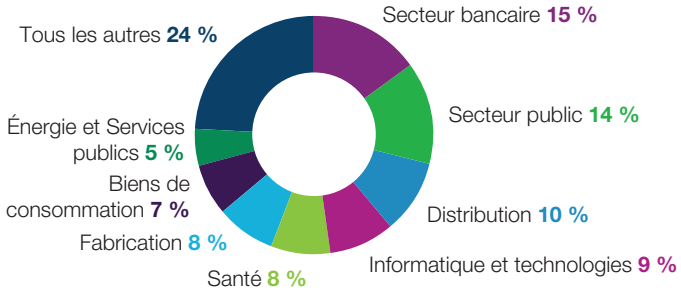
Lieu (35 pays)



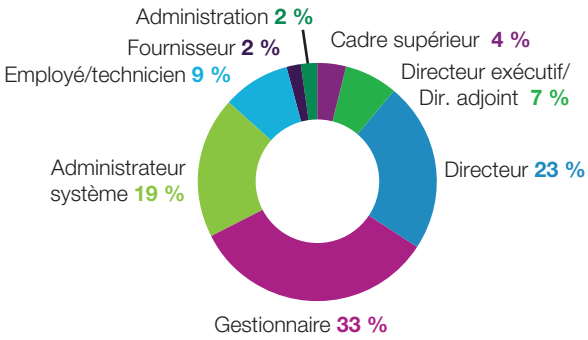
Taille des entreprises (employés)



Secteurs



Fonction



L'étude IBM Global Study sur l'impact économique des risques informatiques, conduite indépendamment par le Ponemon Institute, publiée en septembre 2013, a recueilli les informations de 1039 professionnels de la continuité des opérations et de la résilience à travers le monde.

Pour plus d'informations

Pour mieux comprendre comment IBM peut vous aider à protéger votre entreprise en renforçant la continuité opérationnelle et la résilience, prenez contact avec votre interlocuteur ou votre partenaire commercial IBM ou consultez le site Web suivant :

ibm.com/services/fr/continuity

Rejoignez la conversation sur la continuité des opérations

Pour en savoir plus sur l'étude IBM Global Study sur l'impact économique des risques informatiques, visitez le site suivant : **ibm.com**/services/fr/riskstudy

Index IBM de continuité des opérations ibmbusinesscontinuityindex.com

Indice IBM de Risque Réputationnel ibmriskindex.com

Compagnie IBM France
17 Avenue de l'Europe
92 275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse :
ibm.com

Pensez à recycler ce document

RLW03026-FRFR-01