IBM Institute for Business Value

L'évolution du rôle des directeurs et responsables des technologies de l'information

Conclusions de l'étude des risques informatiques mondiaux 2010 d'IBM

IBM Institute for Business Value

IBM Global Business Services s'appuie sur le IBM Institute for Business Value pour offrir aux exécutifs séniors des aperçus stratégiques factuels sur des enjeux critiques des secteurs publics et privés. Ce rapport est basé sur une étude détaillée réalisée par l'équipe de chercheurs de l'institut. Il s'inscrit dans un engagement continu d'IBM Global Business Services, à savoir offrir des analyses et opinions soutenant la création de valeur par les entreprises. Vous pouvez communiquer avec les auteurs ou nous envoyer un courriel à l'adresse *iibv@us.ibm.com* pour de plus amples renseignements. D'autres études du Institute for Business Value d'IBM se trouvent à l'adresse *ibm.com/iibv*

Par Linda B. Ban, Richard Cocchiara, Kristin Lovejoy, Rick Telford et Mark Ernest

L'augmentation des exigences réglementaires,

la croissance du commerce en ligne 24 heures sur 24, 7 jours sur 7 et l'ombre constante de l'instabilité de l'économie montrent l'importance de la gestion des risques sous toutes ses formes, que ce soit en relation avec les activités, les données ou les événements. L'étude des risques informatiques mondiaux 2010 d'IBM souligne les défis associés aux risques informatiques, ainsi que les mesures que les directeurs et responsables des technologies de l'information mettent en place afin de mieux comprendre ces problèmes, y faire face et les résoudre. La majorité des responsables interrogés estime que leurs responsabilités associées aux risques vont augmenter. Manifestement, la gestion des risques informatiques est un domaine très vaste, qui peut avoir une influence directe sur la compétitivité d'une entreprise, ainsi que sur sa réputation auprès de ses clients, partenaires, organismes de régulation et autres parties intéressées.

Du point de vue commercial, l'infrastructure informatique joue un rôle de plus en plus sensible, non seulement en termes de soutien et de protection des principaux actifs et de mise en place d'une gouvernance et conformité appropriées, mais également en termes de croissance. En conséquence, la gestion des risques informatiques n'est plus considérée comme une fonction strictement technique, mais comme une tâche essentielle pouvant offrir des avantages commerciaux directs pour l'ensemble de l'entreprise.

Afin de mieux comprendre comment les entreprises gèrent et atténuent les risques liés, en particulier dans le domaine informatique, IBM a lancé l'étude des risques informatiques mondiaux 2010, dans le cadre de la recherche d'IBM dans le domaine des risques informatiques, la première d'une série d'études sur ce sujet. L'objectif de cette étude réalisée en mai et juin 2010 en collaboration avec la Economist Intelligence Unit (EIU) est de mieux comprendre les domaines sur lesquels les directeurs informatiques se concentrent aujourd'hui, ainsi que les domaines dans lesquels ils entrevoient des possibilités et des défis à court terme. Une prochaine étude analysera ces questions en profondeur et examinera les options et décisions offertes à toutes les équipes en charge de la gestion des risques.

" La prépondérance acquise par les technologies de l'information dans les activités des entreprises n'a pas été accompagnée d'une croissance proportionnelle de l'importance des risques informatiques. "

Répondant, industrie du voyage et du tourisme, Europe de l'Ouest

" Bien que certaines personnes pensent que la technologie a gagné en maturité et s'est banalisée dans les entreprises, nous pensons que la révolution technologique ne fait que commencer. Nous pensons que la valeur stratégique des technologies continue à progresser. "

Brynjolfsson, Erik and Adam Saunders. Wired for Innovation: How Information Technology is Reshaping the Economy. Massachusetts Institute of Technology. 2010.

Les conclusions de cette étude sont basées sur une enquête en ligne réalisée auprès de 556 directeurs des technologies de l'information et d'autres personnes exerçant essentiellement une fonction dans ce domaine (y compris 131 directeurs des technologies de l'information). Représentant l'Amérique du Nord, l'Europe occidentale, l'Asie-Pacifique, le Moyen-Orient et l'Afrique, l'Europe de l'Est et l'Amérique latine, l'étude recoupe plusieurs industries : informatique, services financiers, santé et pharmaceutique, biotechnologies, manufacturières et gouvernementales. Les sociétés interrogées ont déclaré des chiffres d'affaires situés entre 500 millions et 10 milliards de dollars américains.

Principaux objectifs de l'étude :

- Analyser un échantillon d'entreprises afin d'évaluer avec précision le niveau actuel de la gestion des risques informatiques.
- Déterminer les facteurs susceptibles de faire progresser (ou ralentir) les stratégies de gestion des risques des entreprises.
- Étudier dans quelle mesure les entreprises mettent de nouvelles stratégies, programmes et politiques de gestion des risques en place.
- Comprendre comment les progrès informatiques, tels que l'informatique dématérialisée, sont alignés aux stratégies globales de gestion des risques des entreprises.
- Analyser l'évolution du rôle des responsables et directeurs des technologies de l'information.

De façon générale, les conclusions de l'enquête se recoupent entre les différentes régions, ainsi qu'en fonction de l'importance de l'industrie et des rôles (toutes les régions représentées dans l'étude reconnaissent l'importance de la gestion des risques informatiques et cherchent à renforcer ce domaine). Dans l'ensemble, les participants à l'étude ont confiance en leur gestion des risques et efforts de conformité (voir la figure 1).

Toutefois, bien que 50 pour cent des répondants déclarent que leurs budgets sont restés identiques ou ont été renforcés, 36 pour cent éprouvent toujours des difficultés à obtenir suffisamment de financement pour s'attaquer aux défis liés aux risques. En dépit de la reconnaissance des avantages que peut offrir la gestion des risques informatiques, le soutien de la direction reste un réel problème. Les

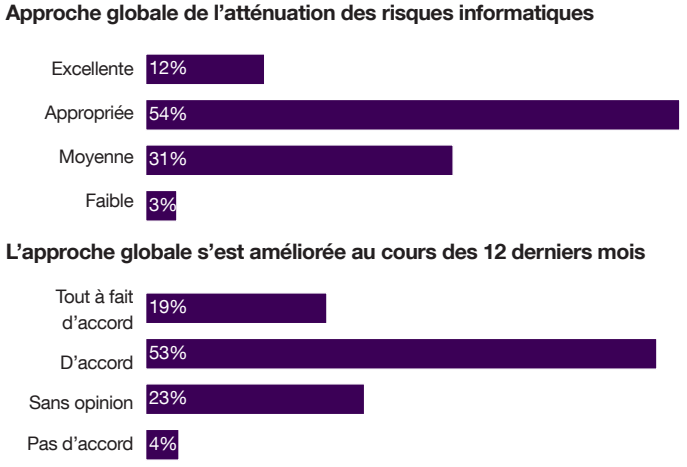

Figure 1 : **Les entreprises classent leur approche de l'atténuation des risques informatiques comme satisfaisante.**

répondants indiquent un écart entre la perception de la direction générale du coût du renforcement de la gestion des risques informatiques et la valeur qu'elle peut en tirer.

Faciliter les améliorations

Reconnaissant les retours possibles d'une gestion efficace des risques informatiques, de nombreux participants à l'enquête envisagent d'étendre leurs programmes liés aux risques au cours des trois à cinq prochaines années. D'importantes divergences sont toutefois à noter. Près de la moitié seulement des sociétés interrogées ont mis en place un service dédié à la gestion des risques (46 pour cent) ou une stratégie commerciale adaptée (54 pour cent). En outre, les branches d'activité et les autres risques opérationnels (stratégie financière et commerciale par exemple) ne représentent pas un centre d'attention de premier plan.

" Les départements informatiques réalisent généralement de nombreux tests avant d'introduire de nouveaux services, dans l'objectif d'éviter tout défaut de fonctionnement. Les directeurs des technologies de l'information doivent comprendre le coût réel de ces tests pour l'entreprise. Il ne s'agit pas seulement des coûts informatiques, mais également d'occasions perdues en raison du délai de mise en service. Chaque journée de test correspond à une journée de chiffre d'affaires et de bénéfices perdus. Quel est le risque encouru en cas de panne de service par rapport à l'avantage d'un service en exploitation ? "

Mark Ernest, ingénieur chez IBM

Interrogés sur l'approche globale de leur entreprise en matière d'atténuation des risques informatiques, 66 pour cent des répondants l'estime appropriée ou excellente. Bien que ce résultat représente la majorité des sociétés, plus de 30 pour cent considèrent leur entreprise comme médiocre dans ce domaine. Toutefois, 72 pour cent des répondants déclarent que l'approche de leur société s'est améliorée au cours des 12 derniers mois.

Il n'est donc par étonnant que 75 pour cent des répondants déclarent que la planification des risques informatiques représente principalement une fonction discrète réalisée dans des structures distinctes. Il semble donc très difficile de faire collaborer les différents services d'une entreprise sur ce défi considérable. Autre élément révélateur, de nombreux répondants ont déclaré que bien qu'ils soient engagés dans plusieurs activités de gestion des risques et de mise en conformité, ils souhaiteraient participer davantage (alors qu'environ la moitié des répondants déclare que leur société dispose d'un service de gestion des risques, nombre d'entre eux estime que l'entreprise ne répond pas à leurs attentes en termes de formation et de communication aux employés des politiques et défis liés à la gestion des risques).

Du côté positif, notons que dans un environnement économique difficile, la gestion des risques informatiques et la conformité ont été généralement épargnées par les réductions budgétaires et des coûts. Interrogés sur le budget 2010 de leur entreprise dédié à la gestion des risques, 14 pour cent (80 répondants à l'enquête) anticipaient une croissance importante du financement, et 39 pour cent une croissance. Trente-six pour cent déclaraient que le budget de la gestion des risques resterait inchangé.

Les répondants à l'enquête reconnaissent que l'investissement dans la gestion des risques informatiques peut apporter d'importants avantages commerciaux, en particulier dans les domaines de la continuité des activités (74 pour cent) et de la réputation (32 pour cent, voir la figure 2). Selon les répondants, la gestion des risques informatiques devrait être davantage perçue comme une tactique défensive. Elle peut augmenter l'agilité des sociétés (19 pour cent) et les occasions de croissance (12 pour cent) tout en réduisant les coûts (18 pour cent). Toutefois, la majorité des responsables des technologies de l'information (57 pour cent) se consacre aux risques liés à l'infrastructure.

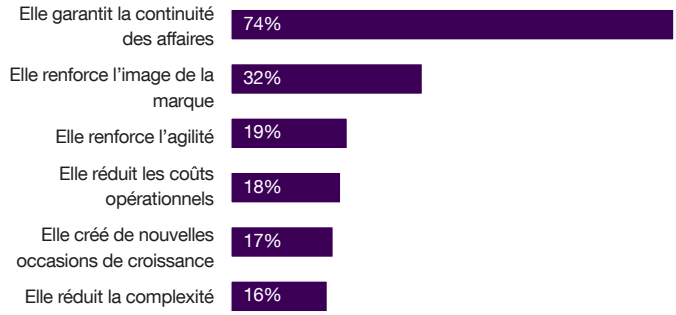

Figure 2 : **Avantages de l'amélioration de la gestion des risques informatiques**

La sécurité informatique reste la principale préoccupation

Bien que les risques informatiques concernent tous les processus, toutes les activités et tous les systèmes, la sécurité informatique (vulnérabilité vis-à-vis des pirates et de l'accès/l'utilisation frauduleuse des systèmes de la société) reste la première préoccupation de 78 pour cent des professionnels interrogés. Le dysfonctionnement matériel et du système arrive en seconde position, cité par 63 pour cent des répondants, suivi de près par les pannes d'alimentation et la sécurité physique (40 pour cent) puis le vol, la qualité du produit, la conformité, les catastrophes naturelles, les requêtes de preuve électronique, les dysfonctionnements de la chaîne logistique et le terrorisme dans cet ordre.

Les responsables des technologies de l'information ont des opinions bien définies de l'importance de la gestion des risques, ainsi que des domaines les plus problématiques. Néanmoins, des écarts considérables existent en termes de confiance dans la capacité de leur entreprise à s'attaquer et à réagir efficacement aux risques. À titre d'exemple, seulement 22 pour cent des personnes interrogées estiment que leur entreprise est bien préparée en termes de sécurité informatique. Vingt-trois pour cent des répondants pensent la même chose en termes de préparation aux pannes matériels et systèmes. La protection contre les pannes d'alimentation bénéficie de plus de soutien, 32 pour cent des répondants déclarant que leur entreprise est bien préparée dans ce domaine. Toutefois, un écart important se dessine entre la reconnaissance des répondants de l'importance de s'attaquer aux risques informatiques et la confiance qu'ils ont en la capacité de leur société à gérer et à atténuer correctement ces risques.

" La continuité des affaires est bien plus large que la planification des catastrophes naturelles ou prévues. Elle englobe l'établissement d'une culture des risques, garantissant que les outils, processus et méthodes nécessaires sont en place, et que chaque employé de l'entreprise est conscient de sa responsabilité vis-à-vis de la protection et de l'intégrité des données. Enfin, lors de la mise en œuvre d'outils et de processus, il est essentiel de trouver un équilibre entre délais de commercialisation et risques acceptables. "

Jessica Carroll, directrice générale des technologies de l'information, United States Golf Association

Étude de cas

Au cours du premier semestre de 2010, l'équipe de recherche et de développement d'IBM a étudié 4,396 nouvelles vulnérabilités, soit une augmentation de 36 pour cent par rapport à la même période l'an dernier. Selon le rapport, les vulnérabilités des applications Web représentent toujours la menace la plus importante, comptant pour plus de la moitié de toutes les divulgations d'informations. Néanmoins, le rapport souligne que les entreprises cherchent davantage à identifier et divulguer les failles de sécurité qu'auparavant. Ce phénomène a un impact positif sur l'industrie, car il dynamise la collaboration ouverte en matière d'identification et de suppression des vulnérabilités avant que les cybercriminels ne puissent les exploiter.[1]

Le défi de la communication

Il ne fait aucun doute que la gestion des risques informatiques peut apporter de véritables avantages commerciaux. Toutefois, en dépit des différentes méthodes de diffusion des informations liées aux risques que les entreprises peuvent utiliser, la communication émerge comme une réelle barrière. Selon 25 pour cent des répondants, le soutien de la direction générale reste un défi. La communication des politiques et procédures aux employés représente également un problème pour 30 pour cent des répondants.

De nombreuses entreprises adoptent une approche passive plutôt que proactive de la gestion et l'atténuation des risques informatiques. Souvent, l'information est diffusée sur l'intranet de la société, où les employés doivent la rechercher. Certaines entreprises intègrent leurs politiques de gestion des risques dans les documents de formation des nouveaux employés, sans prendre en compte le besoin de les communiquer à tous (seulement 22 pour cent des responsables des technologies de l'information déclarent que les politiques de gestion des risques sont intégrées à la formation de tous les employés. Plus surprenant, moins de 15 pour cent des répondants ont incorporé un plan de gestion des risques intégré à l'infrastructure physique et technique de leur entreprise.

" Nous luttons pour faire évoluer le comportement de la direction et du personnel dans le but de renforcer la sécurité. "

Répondant, industrie manufacturière, Europe de l'Ouest

" Le financement nécessaire à la gestion des risques informatiques est de plus en plus difficile à obtenir, y compris lorsque les coûts encourus par l'absence de prise en charge des risques sont clairement exposés à la direction. Nous assistons souvent à une réticence à investir. "

Répondant, industrie aérospatiale et défense, Amérique du Nord

Étant donnée la diversité des canaux de communication et de formation disponibles pour sensibiliser aux risques, les sociétés devraient adopter une approche mieux organisée et plus détaillée pour se tenir informées des risques, communiquer ces défis aux employés et intégrer la gestion des risques informatiques à tous les services. En réponse à la question " De quelle manière votre société se tient-elle informée des risques ? ", la majorité des répondants déclare que les menaces sur la sécurité sont prises en charge par des ressources internes et externes (38 pour cent), une équipe interfonctionnelle de cadres dirigeants (26 pour cent) ou un service dédié à la gestion des risques (19 pour cent).

" Généralement, les utilisateurs, la direction et les partenaires envisagent les risques à partir de points de vue différents, dont je dois tenir compte de manière raisonnable. "

Répondant, industrie manufacturière, Europe de l'Ouest

Évaluation des nouvelles technologies

Les répondants ont été interrogés sur la position de leur entreprise en matière d'acquisition et de déploiement de cinq technologies émergentes (voir la Figure 3) :

- Réseaux sociaux (ex. : forums intranet et internet, messagerie instantanée, bibliothèques, blogues et wikis)
- Plateformes mobiles (ex : Windows® Mobile, BlackBerry OS et Google Android OS)
- Informatique dématérialisée
- Virtualisation
- Architecture orientée services (SOA)

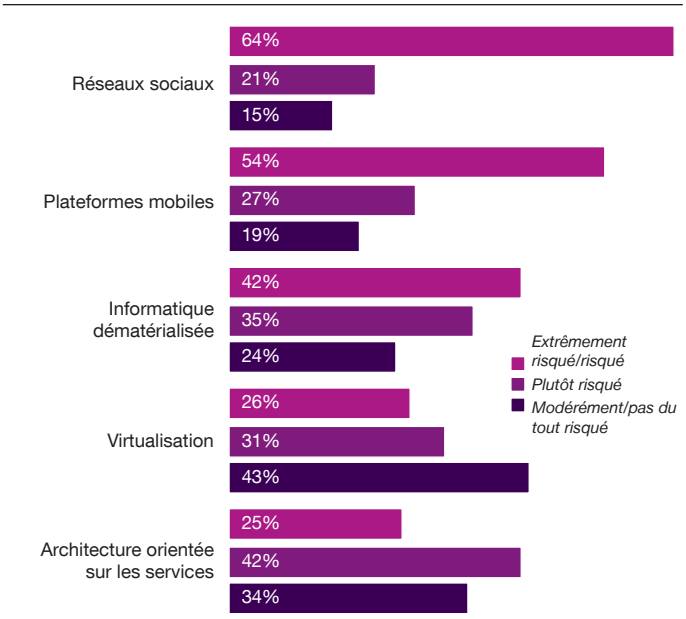

Figure 3 : **Les réseaux sociaux, les plateformes mobiles et l'informatique dématérialisée présentent les principaux risques.**

Parmi ces cinq technologies, les réseaux sociaux, les plateformes mobiles et l'informatique dématérialisée représentent les principales préoccupations. Les réseaux sociaux représentent la principale inquiétude en termes de risques pour 64 pour cent des personnes interrogées, suivis de près par les plateformes mobiles et l'informatique dématérialisée (54 et 43 pour cent respectivement). La majorité des risques concernent l'accès, l'utilisation et le contrôle des données, en particulier en ce qui concerne les réseaux sociaux, et le danger de l'accès non autorisé aux informations confidentielles et sensibles (de nombreuses entreprises n'ont pas encore mis en place de méthodes et processus pour intégrer les réseaux sociaux dans leurs infrastructures et flux).

Interrogés sur les deux risques les plus importants qu'ils associent à l'informatique dématérialisée, la majorité des répondants cite la protection des données et le respect de la vie privée (voir la figure 4). La continuité des affaires préoccupe plus de la moitié des répondants, tandis que 44 pour cent estiment que les nuages privés représentent davantage de risques que les services informatiques traditionnels, et 77 pour cent expriment des inquiétudes vis-à-vis du respect de la vie privée.

" La dématérialisation représente uniquement une option permettant de résoudre un problème lorsque vous pouvez en tirer des avantages. Elle doit donc être prise en compte. "

Répondant, industrie des technologies de l'information, Amérique du Nord

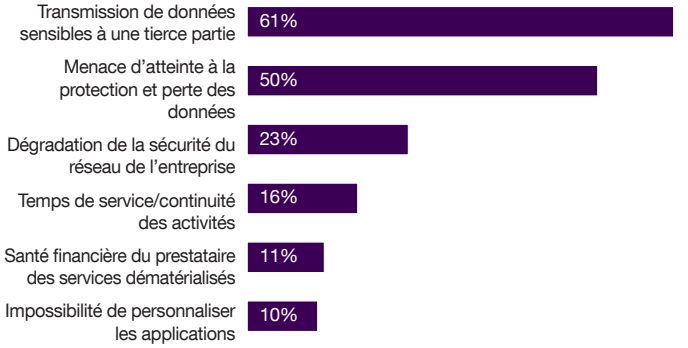

Figure 4 : **Risques associés à l'informatique dématérialisée.**

La transmission de données à une tierce partie est également considérée comme risquée par 61 pour cent des répondants, tandis que seulement 23 pour cent citent les brèches de sécurité du réseau.

Seulement 26 pour cent des répondants pensent que la virtualisation représente un risque important pour leur entreprise. De façon similaire, l'architecture orientée sur les services (SOA) représente un défi pour seulement 25 pour cent.

Le choix de la dématérialisation

Les responsables des technologies de l'information ressentent la pression de la baisse des dépenses liées à l'infrastructure, l'augmentation des efficacités et l'amélioration des niveaux de service dans l'ensemble de l'entreprise. Nombre d'entre eux se tournent vers l'informatique dématérialisée pour atteindre ces objectifs. L'informatique dématérialisée représente un progrès majeur des modèles informatiques, à l'instar de ces prédécesseurs, à savoir l'infrastructure client/serveur et l'informatique centralisée. Le traitement est géré par un réseau de ressources distribué et mondialement accessible, diffusées sur demande en tant que service. L'informatique dématérialisée offre une alternative extrêmement automatisée et dynamique pour l'acquisition et l'offre de services informatiques, permettant aux utilisateurs d'exploiter des nuages publics, privés et hybrides de ressources et services sans avoir à gérer directement la technologie sous-jacente. Aujourd'hui, les sociétés tirent profit de l'incroyable extensibilité et des capacités de collaboration de l'informatique dématérialisée pour résoudre les problèmes de manière différente. Elles déploient également de nouveaux services plus rapidement, sans investissement de capitaux supplémentaire. Néanmoins, les entreprises doivent rester prudentes et se tenir informées lors de la sélection d'un prestataire, en particulier en raison des questions liées aux risques.

Implications pour les directeurs des technologies de l'information

La majorité des directeurs des technologies de l'information interrogés estime que leurs responsabilités – de l'exécution des politiques et procédures, de la définition des stratégies d'atténuation des risques au soutien à la mise en place et à la supervision des stratégies de gestion des risques informatiques dans l'entreprise – vont augmenter au cours des trois prochaines années (voir la figure 5). Plus de 65 pour cent des répondants estiment que l'atténuation des risques fait de plus en plus partie de leurs fonctions, tandis que 83 pour cent estiment que les responsables des technologies de l'information devraient être davantage impliqués dans ce domaine.

L'augmentation de l'interdépendance des activités et de l'informatique justifie ces réponses. En effet, les directeurs et responsables des technologies de l'information interrogés estiment que leurs fonctions engloberont le soutien à la stratégie commerciale globale et à la marque de l'entreprise (par exemple dans le marketing et le service à la clientèle). En maintenant ou renforçant leurs stratégies, processus et procédures de gestion des risques, les sociétés pourraient sous-traiter la responsabilité de l'infrastructure à un fournisseur ou partenaire pour permettre aux responsables des technologies de l'information de se concentrer davantage sur la sécurité, la résilience et la continuité des activités.

Il est également intéressant de noter que les réponses des 131 directeurs des technologies de l'information interrogés pour l'enquête et celles des responsables restent proches.

Bien que l'importance de la gestion des risques informatiques et de la conformité soit largement reconnue par les entreprises de toutes les industries, et que nombre d'entre elles cherchent à améliorer ces aspects de leurs activités, rares sont les entreprises entièrement préparées pour toutes les situations liées aux risques et à la conformité.

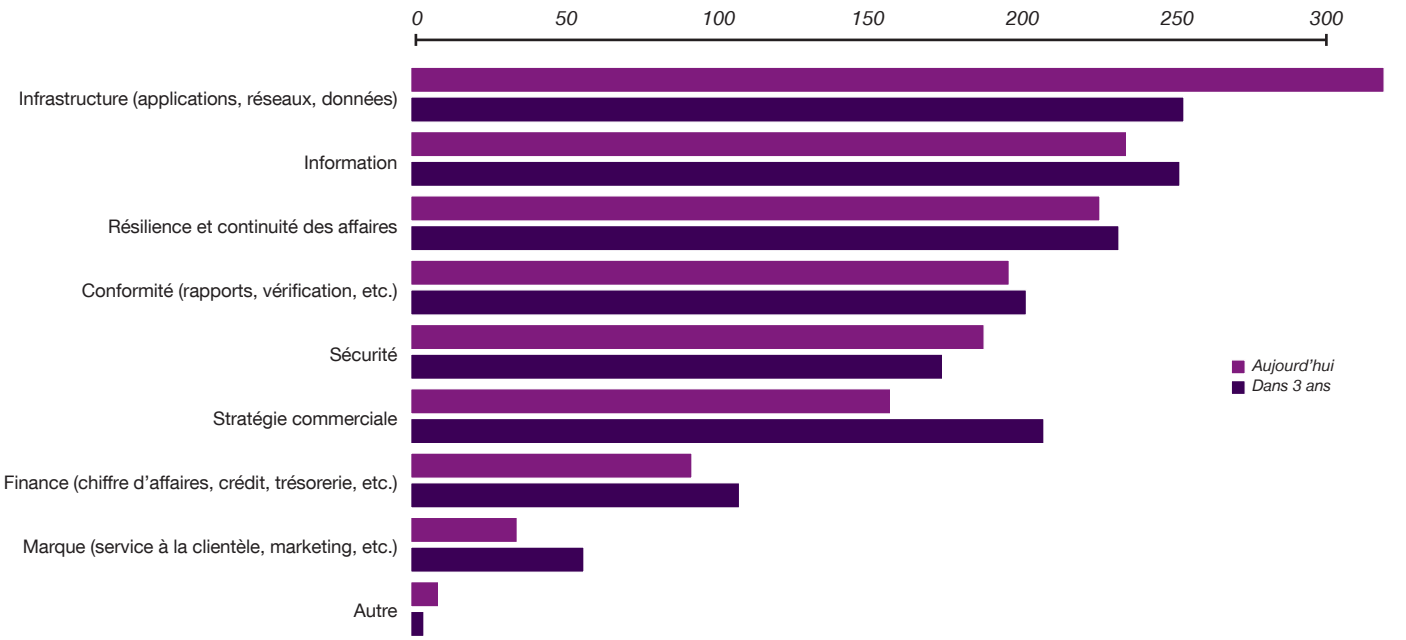

Figure 5 : **Les responsables des technologies de l'information s'attendent à une évolution de leurs domaines de responsabilité au cours des trois prochaines années.**

L'étude des risques informatiques mondiaux 2010 d'IBM a permis de mettre l'accent sur les domaines pouvant permettre aux responsables des technologies de l'information d'évaluer la maturité des risques, de déterminer les points faibles, d'établir des priorités et d'élaborer des stratégies dans plusieurs domaines :

- Dans une entreprise, la sensibilisation aux risques relève de la responsabilité de tous. Toutefois, si les politiques et procédures liées aux risques ne sont pas incorporées à la culture d'entreprise, de nombreux programmes de gestion et d'atténuation des risques informatiques n'atteindront pas les résultats escomptés, voire échoueront. Les résultats de l'étude confirment que les entreprises doivent insister sur la formation, la communication et le soutien aux programmes de gestion des risques et de conformité dans leur entreprise.
- Les données représentent un défi pour tous les aspects de la gestion des risques informatiques, de la sécurité, l'efficacité et la continuité des activités jusqu'à la disponibilité, la gestion des catastrophes, les pirates, la gestion des données et de l'infrastructure. Dans ce cadre, les sociétés doivent adopter une approche unifiée et holistique des risques informatiques, en prenant en compte tous ses éléments dans l'objectif de renforcer les retours et l'efficacité.

- Au moment de l'adoption de nouvelles technologies, architectures et stratégies, du développement de nouvelles applications ou de l'intégration aux systèmes existants, l'atténuation des risques devrait représenter l'un des principaux points de débats. La prise en compte des risques positifs (ceux que la société accepte car le risque s'accompagne d'occasions) et des risques négatifs (incidents possibles pouvant avoir des conséquences sur l'entreprise) peuvent ajouter de la valeur et augmenter le chiffre d'affaires, mais uniquement si la gestion des risques informatiques est correctement financée.

  Les nouvelles technologies sont toutes différentes, mais certaines, telles que la virtualisation et l'informatique dématérialisée, peuvent offrir de nombreux avantages en termes de soutien et d'options d'atténuation des risques. Bien que l'informatique dématérialisée exige de l'attention en matière de sécurité des données, lorsqu'elle est correctement déployée, la dématérialisation peut favoriser la réduction des coûts ainsi que les risques associés à la résilience. Toutefois, il est indispensable de mettre des processus en place pour s'attaquer aux risques associés aux nouvelles technologies.

" Nous avons tendance à envisager un projet trop simplement en fonction de ce que nous pensons connaître des risques, puis nous affectons les ressources sur cette base. "

Répondant, industrie des technologies de l'information, Moyen-Orient et Afrique

Un processus bien défini

Une gestion efficace des risques informatiques comprend plusieurs facettes. Les responsables des technologies de l'information doivent prendre les éléments suivant en compte au moment de sa mise en place :

Étude et évaluation des risques informatiques de l'entreprise

- Mettre en place une planification interentreprise de toutes les catégories de risques (données, sécurité, résilience et nouvelles technologies).
- Étudier les défis posés par les risques et confirmer la mise en place d'un plan afin de s'attaquer à tous ces défis (établissement de priorités et atténuation de l'extensibilité des risques : défaillances systèmes et brèches du système de sécurité) et rechercher des moyens de tirer profit des risques les plus importants (raccourcissement du délai de commercialisation et nouveaux points de contact pour les nouveaux clients).

Identifier des experts parmi les cadres

- Devenir un conseiller digne de confiance et une ressource de valeur pour le directeur des technologies de l'information. Formuler les avantages que le directeur et les autres apportent en s'attaquant aux risques informatiques.
- " Vendre " les avantages de l'atténuation des risques, tels qu'une croissance plus élevée, le renforcement de l'agilité et de l'image de marque.

Chercher à sensibiliser aux risques à tous les niveaux, et dans la culture de l'entreprise

- Sensibiliser aux risques dans les processus informatiques et commerciaux quotidiens. Mettre en place différentes méthodes de formation dans l'ensemble de la société.
- Créer une stratégie permettant de communiquer régulièrement l'étendue de la gestion des risques, ainsi que les questions liées à la conformité afin de souligner qu'il ne s'agit pas d'une activité ponctuelle.

Rechercher des procédures de gestion des risques innovantes

- Établir des procédures de gestion des risques dans l'infrastructure informatique, plutôt que de les inclure dans des applications de manière fragmentaires.
- Étudier les processus commerciaux à la recherche de risques possibles et établir un plan de gouvernance des risques informatiques spécifique pouvant être exécuté dans l'ensemble de l'entreprise.

Garantir la mise en place de mesures de protection contre les accès non autorisés aux données et dans les systèmes de la société

- Réviser les plans de continuité des affaires. La continuité des affaires est plus vaste que la gestion des catastrophes naturelles, elle englobe un large spectre de scénarios d'interruption des activités, de la panne du serveur aux pandémies.
- Informer tous les employés de leur responsabilité en matière de protection des données et les sensibiliser à l'exécution de cette responsabilité.
- Déterminer des outils, processus et méthodes afin de protéger les données. De nombreux outils et processus sont d'ores et déjà disponibles (contrôle de l'accès, gestion des données de référence, gestion du cycle des informations, processus de gestion des données).

La question n'est plus de savoir si de nouvelles technologies seront introduites dans une entreprise, mais quand. Tel qu'il est indiqué ci-dessus, les nouvelles technologies sont toutes différentes, mais certaines peuvent offrir de nombreux avantages en termes de gestion des risques informatiques. Les dernières technologies, telles que la virtualisation, offrent d'impressionnantes options d'atténuation des risques et de réduction des coûts.

Êtes-vous bien préparé?

- **Comment votre société évalue-t-elle la maturité des risques et gère-t-elle les risques en termes d'activité et d'infrastructure et d'actifs informatiques?**
- **Quelles stratégies votre société a-t-elle mises en place dans le cadre des meilleures pratiques informatiques de l'industrie dans le but d'atténuer les risques (sécurité, résilience et continuité des affaires)?**
- **De quelles manières les programmes liés aux risques de votre société permettent d'améliorer la visibilité et le contrôle, et facilitent-ils la conformité aux contrats, normes de l'industrie, réglementations et contrôles internes?**
- **Comment votre infrastructure informatique soutient-elle les objectifs de rendement en termes de flexibilité, sécurité, disponibilité, gouvernance, extensibilité et résilience?**
- **Quel type de programme votre entreprise a-t-elle mis en place afin de garantir que son capital humain, ses processus et systèmes soient en mesure de répondre à une perturbation puis de reprendre les activités?**

Une gouvernance énergique et cyclique de la gestion des risques informatiques, du point de vue technologique et commercial, évalue en permanence la vulnérabilité d'une entreprise aux risques informatiques et établit une priorité de ces risques tout en ayant un impact sur ceux-ci. En conséquence, les protocoles de gestion des risques doivent être incorporés dans les nouvelles technologies dès leur mise en œuvre.

Enfin, il est essentiel d'étudier les besoins de l'entreprise lors de la mise en œuvre d'outils et de processus, d'équilibrer le délai de commercialisation et les risques acceptables. En adoptant une approche proactive de la gestion des risques informatiques, les sociétés peuvent se positionner de façon à devancer leur vulnérabilité, et à être davantage protégées et résilientes vis-à-vis des incidents anticipés ou non anticipés.

Plus d'informations

Pour en savoir plus sur cette étude du IBM Institute for Business Value, veuillez communiquer avec nous au *iibv@us.ibm.com*. Pour obtenir le catalogue complet de nos recherches, visitez :

ibm.com/iibv

Pour obtenir plus d'informations sur la gestion des risques informatiques, veuillez visiter :

ibm.com/smarterplanet/security

Auteurs

Linda Ban est directrice du programme d'études CxO et directrice AIS du IBM Institute for Business Value. Dans le cadre de ses fonctions, elle dirige l'équipe mondiale en charge du développement, du déploiement et du soutien du leadership éclairé d'IBM dans le cadre du programme CIO, ainsi que de l'organisation de l'Application Innovation Services (AIS). L'expérience de Linda comprend une vaste expérience des technologies émergentes et collaboratives, de la stratégie commerciale et opérationnelle, du développement de systèmes et de la gestion opérationnelle. Outre sa fonction auprès des clients, elle a publié de nombreux travaux sur un large spectre de thèmes, défis et solutions. Vous pouvez communiquer avec Linda à l'adresse *lban@us.ibm.com*.

Richard Cocchiara est ingénieur chez IBM et directeur des technologies pour les services de continuité des activités et de résilience d'IBM Global Services. Il dispose d'une expérience de plus de 28 ans en IS et a conseillé de nombreuses sociétés du Fortune 500, en particulier dans l'industrie de la finance et de la sécurité. Richard est actuellement responsable de la recherche et du développement des solutions et services de continuité des activités et de résilience d'IBM Global Technology Services. Vous pouvez communiquer avec lui à l'adresse *rmcocch@us.ibm.com*.

Kristin Lovejoy est vice-présidente de la stratégie de sécurité d'IBM. Elle a été désignée comme l'une des 25 premières directrices de la technologie par InfoWorld en 2005, et comme l'une des 25 directrices de la sécurité les plus influentes par Security Magazine en 2006. Elle détient des brevets européens et américains pour un modèle et une méthode de gestion des risques orientée objets. Kristin peut être jointe à l'adresse *klovejoy@us.ibm.com*.

Ric Telford est vice-président des services dématérialisés d'IBM, en charge de la définition de nouvelles occasions et nouveaux services dans le cadre du portefeuille des offres dématérialisées d'IBM. Chez IBM, Ric Telford a exercé plusieurs fonctions clés dans plusieurs programmes logiciels et de services, y compris un système de gestion de documents, réseautage, gestion de systèmes et services d'infrastructures informatiques. Auparavant, Ric Telford a exercé la fonction de vice-président d'Autonomic Computing, en charge du développement de systèmes autogérés. Ric peut être joint à l'adresse *rtelford@us.ibm.com*.

Mark Ernest est ingénieur chez IBM et membre de l'académie des technologies d'IBM. Il assiste les clients au moment de la création et de la mise en œuvre de systèmes de gestion informatiques afin de maximiser la valeur de leur investissement et d'améliorer l'efficacité de leur utilisation de la technologie de l'information. Mark peut être joint à l'adresse *lernest@us.ibm.com*.

Le partenaire idéal dans un monde en constante évolution

Chez IBM, nous collaborons avec nos clients et apportons notre connaissance du secteur, une recherche et des technologies de pointe pour offrir un avantage significatif dans l'environnement en évolution rapide d'aujourd'hui. Grâce à notre approche intégrée de la conception et de l'exécution, nous vous aidons à transformer les stratégies en action. Notre expertise dans 17 industries et des capacités mondiales dans 170 pays nous permettent d'aider nos clients à anticiper les changements et à tirer profit des avantages de nouvelles occasions.

Référence

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010.

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
PO6 3AU
Royaume-Uni

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland Limited est immatriculée en Irlande sous le numéro 16226.
La page d'accueil d'IBM se trouve à l'adresse ibm.com

Veuillez recycler

GBE03365-CAFR-00