IBM Institute for Business Value

Le nouveau rôle des responsables informatiques et des directeurs des systèmes d'information (DSI)

Enseignements de l'étude IBM Global IT Risk Study 2010

IBM Institute for Business Value

IBM Global Business Services, par le biais de l'IBM Institute for Business Value, publie à l'intention des cadres dirigeants, des études stratégiques sur des problématiques majeures rencontrées au sein des entreprises des secteurs public et privé. Ce rapport s'appuie sur une étude approfondie menée par les consultants de l'institut et reflète la volonté d'IBM Global Business Services de proposer aux entreprises des analyses et une réflexion qui les aident à créer de la valeur pour leur métier. Pour en savoir plus, vous pouvez contacter les auteurs ou écrire par courrier électronique à l'adresse suivante : *iibv@us.ibm.com*. Vous pouvez également accéder à d'autres études de l'IBM Institute for Business Value à l'adresse suivante : *ibm.com/iibv*

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

Les obligations réglementaires croissantes,

le développement de la mondialisation rendent nécessaire un fonctionnement des activités en 24h/7j. Les incertitudes sur le contexte économique viennent renforcer l'importance de la gestion du risque, quelle que soit l'origine de ce risque (qu'il soit lié aux affaires, aux données ou aux événements extérieurs). L'étude IBM Global IT Risk Study 2010 révèle les défis inhérents au risque informatique et les démarches qu'adoptent les directions informatiques pour mieux comprendre, apréhender et résoudre cette problématique. Une majorité des responsables interrogés s'attendent à voir s'étendre leur sphère de responsabilité en matière de gestion du risque. À l'évidence, le périmètre de ce domaine est vaste et impacte directement la compétitivité des entreprises, mais aussi leur crédibilité auprès des clients, partenaires, organismes réglementaires et autres tierce-parties concernées.

Pour les métiers, l'infrastructure informatique joue un rôle stratégique croissant, non seulement en exploitant et protégeant les actifs stratégiques d'une entreprise et en assurant la gouvernance et la conformité réglementaire, mais également en supportant la croissance de l'entreprise. Loin d'être limitée à une fonction strictement technique, la gestion du risque informatique est reconnue comme une activité de management cruciale, porteuse d'avantages directs sur le métier de l'entreprise dans sa globalité.

C'est pour mieux comprendre comment opèrent les entreprises pour gérer et limiter les risques qui menacent leur organisation – et tout particulièrement l'informatique – qu'IBM à réalisé l'étude Global IT Risk Study 2010. Cette étude qui s'intègre dans les actions de recherche permanente d'IBM dans le domaine du risque informatique, est la première d'une série portant sur ce sujet. Menée au mois de mai et juin 2010 en coopération avec l'Economist Intelligence Unit (EIU), elle avait pour objectif de mieux connaître les domaines sur lesquels les responsables informatiques concentrent leurs actions aujourd'hui et qui leur semblent porteurs d'opportunités et de défis à court terme. Des études ultérieures permettront d'explorer ces problématiques de manière plus détaillée, en examinant les options et les décisions auxquelles sont confrontées toutes les équipes responsables de la gestion du risque au sein des entreprises.

« Alors que l'informatique est devenue centrale dans les activités des entreprises, la gestion du risque informatique n'a pas pour autant acquis une importance dans la même proportion. »

Un participant du secteur du Voyage et du Tourisme, Europe

« Si la technologie a atteint, selon certains, sa pleine maturité et son utilisation devenue courante au sein des entreprises, nous constatons que la révolution technologique n'en est qu'à ses débuts. Notre perception des faits suggère que la valeur stratégique apportée par la technologie à l'entreprise continue à augmenter. »

Erik Brynjolfsson et Adam Saunders, « Wired for Innovation: How Information Technology is Reshaping the Economy. » (Anticiper l'innovation : comment l'informatique transforme l'économie), Massachusetts Institute of Technology, 2010.

Les enseignements de cette étude se fondent sur une enquête complète réalisée en ligne auprès de 556 responsables informatiques et autres dirigeants, concernés par la fonction informatique au sein des entreprises (dont 131 DSI). Effectuée dans différentes régions du monde – Amérique du Nord, Europe occidentale, Asie-Pacifique, Moyen-Orient et Afrique, Europe de l'Est et Amérique latine – l'étude concerne de nombreux secteurs – depuis l'informatique, les services financiers, la santé et l'industrie pharmaceutique, jusqu'aux biotechnologies, l'industrie manufacturière et l'administration publique. Les entreprises participantes ont indiqué des chiffres d'affaires compris entre 330 millions de £ et plus de 660 milliards de £.

Les principaux objectifs de l'étude étaient les suivants :

- Evaluer avec précision, auprès d'un échantillon d'entreprises, la situation actuelle en matière de gestion du risque informatique.
- Identifier les facteurs de progression, ou les freins, pour la stratégie de gestion du risque au sein d'une entreprise.
- Évaluer l'étendue de l'application de politiques et de nouveaux programmes de gestion du risque au sein des entreprises.
- Comprendre de quelle manière les évolutions en matière d'informatique, notamment le Cloud computing, sont en adéquation avec les stratégies globales des entreprises en matière de risques.
- Examiner le nouveau rôle des responsables informatiques et notamment des DSI.

D'une manière générale, les enseignements tirés de l'étude se recoupent, et ce quels que soient la zone géographique, la taille de l'entreprise, le secteur et la fonction du participant. Toutes les régions du monde ayant participé à l'enquête s'accordent sur l'importance de la gestion des risques informatiques et mettent en œuvre des actions d'amélioration dans ce domaine. Dans l'ensemble, les participants se sont montrés confiants dans leurs actions en matière de gestion du risque et de conformité (voir Figure 1).

Par ailleurs, si plus de 50 % des répondants mentionnent des budgets stables ou en augmentation, ils sont 36 % à lutter pour obtenir les financements nécessaires afin de relever les défis liés à la gestion des risques. Et malgré la prise de conscience des avantages métier tangibles de la gestion du risque informatique, obtenir le soutien des cadres dirigeants reste une véritable préoccupation. Le point de vue des participants à l'étude semble mettre en évidence un hiatus entre la vision des cadres dirigeants concernant les coûts d'une gestion plus performante des risques informatiques et la valeur qu'elle permet de créer.

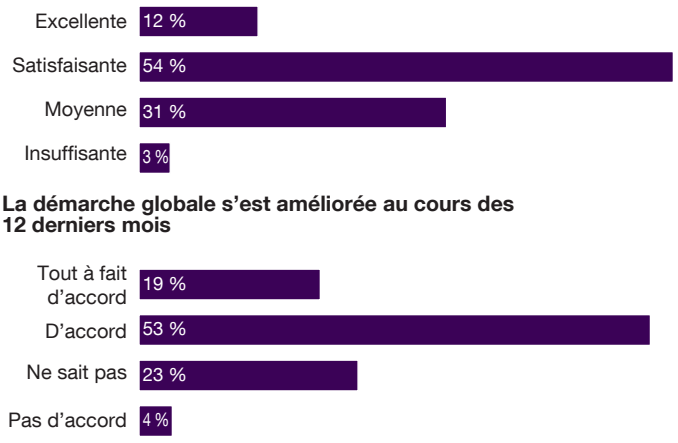

Figure 1 : **Évaluation par les entreprises de leur approche de la limitation du risque informatique.**

Ouvrir la voie à des améliorations

Conscients des bénéfices potentiels pour l'entreprise d'une gestion efficace du risque informatique, nombre de participants interrogés envisagent de développer leurs actions dans ce domaine au cours des trois à cinq ans qui viennent. Néanmoins, nous avons relevé des divergences notables. Les entreprises indiquent pour moitié l'existence d'un service formel de gestion du risque (46 %) ou d'une stratégie parfaitement établie de continuité des activités (54 %). Parallèlement, les risques affectant les directions fonctionnelles et d'autres secteurs opérationnels (finances et stratégie métier, par exemple) ne constituent pas des domaines d'intérêt majeur.

« Les organisations informatiques procèdent généralement à des tests approfondis avant de mettre en œuvre de nouveaux services métier basés sur l'informatique, avec pour objectif principal d'éviter toute défaillance. Cependant les directeurs informatiques actuels doivent mieux connaître le véritable coût de ces tests pour l'entreprise. Au-delà des coûts informatiques, il y a ceux d'un potentiel commercial perdu du fait d'un retard de mise en place d'une prestation. Toute journée passée à effectuer un test est autant de temps perdu pour générer du chiffre d'affaires et du profit. N'est-il pas possible d'évaluer le risque d'une défaillance du service vis-à-vis de l'avantage acquis s'il est opérationnel ? »

Mark Ernest, Ingénieur consultant IBM

Lorsqu'ils décrivent l'approche globale de leur entreprise en matière de limitation du risque informatique, 66 % des personnes interrogées considèrent qu'elle est satisfaisante ou excellente. Si cette proportion concerne la majorité des entreprises, elles sont plus de 30 % à considérer leur organisation comme moyenne ou insuffisante dans ce domaine. Toutefois, 72 % des participants indiquent que l'approche adoptée dans leur entreprise en matière de risque s'est améliorée au cours des 12 derniers mois.

Sans surprise, 47 % des répondants indiquent que la planification du risque informatique est, en grande partie, une fonction disséminée, traitée au sein de silos opérationnels. Ce qui signifie qu'amener différents domaines organisationnels à collaborer représente un défi considérable. Autre enseignement : nombre des responsables interrogés indiquent que, même s'ils consacrent beaucoup de temps à la gestion des risques et de la conformité, ils souhaiteraient y participer davantage. Alors que près de la moitié des répondants indiquent que leur entreprise dispose d'un service de gestion du risque, nombre d'entre eux considèrent comme insuffisantes les actions de leur entreprise en matière de formation et de communication auprès des collaborateurs concernant les politiques et les questions de gestion du risque.

Point positif : dans le contexte économique actuel marqué par les difficultés, la gestion du risque informatique et la conformité ont été épargnés des coupes budgétaires et des réductions de coûts. À la question concernant le budget 2010 de leur organisation en matière de gestion du risque, 14 % des personnes interrogées (soit 80 répondants) prévoyaient une augmentation significative des montants, et 39 % une certaine augmentation. 36 % d'entre eux ont indiqué que les budgets de gestion du risque resteraient inchangés.

Les répondants interrogés s'accordent à dire que l'investissement dans la gestion du risque informatique est porteur d'avantages métier considérables, et en particulier en matière de continuité des activités (74 %) et de protection de la réputation de l'entreprise (32 %) (voir Figure 2). Selon eux, la gestion du risque informatique doit aller au-delà d'une tactique défensive, pour apporter de l'agilité à l'entreprise (19 %) et créer des opportunités de croissance (12 %) tout en réduisant les coûts (18 %). Toutefois, la plupart des responsables informatiques (57 %) se concentrent principalement sur les risques liés aux infrastructures.

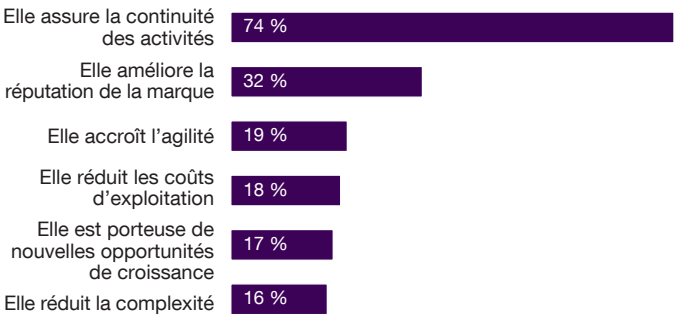

Figure 2 : **Avantages d'une gestion du risque informatique plus performante.**

En tête des priorités : la sécurité informatique

Si le risque informatique concerne les processus, activités et systèmes, la sécurité informatique – qui concerne la vulnérabilité vis-à-vis de pirates et des accès ou des utilisations illicite des systèmes d'entreprise – est la préoccupation prioritaire pour 78 % des professionnels de l'informatique interrogés. Les dysfonctionnements des matériels et des systèmes viennent ensuite – cités par 63 % des personnes interrogées. Les défaillances d'alimentation électrique et la sécurité physique (40 %) viennent immédiatement après, suivies par d'autres préoccupations, par ordre décroissant : vol, qualité des produits, conformité, catastrophes naturelles, enquêtes préliminaires dans les archives électroniques, défaillance des chaînes logistiques, terrorisme.

Les responsables informatiques sont tout à fait conscients de l'importance de la gestion du risque et de domaines particuliers sur lesquels concentrer leur action. Cependant, des disparités importantes apparaissent concernant la confiance qu'ils placent dans les capacités de leur entreprise à répondre et réagir au risque de manière appropriée. Seuls 22 % des répondants, par exemple, considèrent que leurs entreprise est parfaitement préparée en matière de sécurité informatique.

« La notion de continuité des activités va bien au-delà de la planification des catastrophes naturelles ou de la prévention des désastres. Il s'agit en fait d'établir une culture du risque – et donc s'assurer que l'entreprise dispose des outils, des processus et des méthodologies nécessaires et que chaque collaborateur est conscient de ses responsabilités en termes de sécurité et d'intégrité des données. Au final, lors de la mise en œuvre d'outils et de processus, il est essentiel de concilier vitesse de mise sur le marché et niveau d'acceptation du risque. »

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

Vingt-trois pour cent des répondants ont le même sentiment concernant le niveau de préparation de l'entreprise pour répondre à des défaillances du matériel et des systèmes. La protection vis-à-vis des défauts d'alimentation électrique a été davantage citée – 32 % des participants à l'enquête disent considérer leur entreprise parfaitement préparée dans ce domaine. Il apparaît toutefois un hiatus évident entre l'importance qu'accordent les répondants à une réponse aux risques informatiques dans leur ensemble et la confiance qu'ils placent dans leur entreprise pour les gérer et les limiter de manière appropriée.

Étude de cas

Au cours du premier semestre 2010, l'équipe de recherche et développement IBM X-Force a identifié 4 396 nouvelles vulnérabilités – une progression de 36 % par rapport à la même période l'an passé. Selon le rapport, les vulnérabilités des applications web demeurent les menaces les plus fréquentes – elles apparaissent dans plus de la moitié des notifications publiques. Néanmoins, le rapport mentionne que les entreprises agissent davantage qu'auparavant pour identifier et diffuser des informations concernant les vulnérabilités de sécurité. Ce qui provoque des effets positifs sur le secteur en suscitant une collaboration plus large afin d'identifier et d'éliminer les vulnérabilités avant que les cybercriminels puissent les exploiter.[1]

Le défi de la communication

Il ne fait aucun doute que la gestion du risque informatique soit porteuse d'avantages réels pour l'entreprise. Malgré les nombreuses méthodes offertes aux entreprises pour diffuser de l'information concernant les risques, la communication apparaît comme une véritable barrière. Selon 25 % des répondants, obtenir le soutien des cadres dirigeants reste un défi. Et 30 % des responsables interrogés indiquent que la communication auprès des employés en matière de politiques et de procédures liées aux risques constituait un problème.

Au lieu d'une démarche proactive, la plupart des entreprises privilégient une approche passive de la gestion et de la limitation du risque. Dans de nombreux cas, l'information est placée sur l'intranet de l'entreprise, ce qui implique un certain délai pour que les collaborateurs y accèdent. Certaines entreprises incorporent les politiques de gestion du risque dans les supports de formation des nouveaux embauchés – sans prendre en compte la nécessité de les rendre disponibles à tous. (Seuls 22 % des responsables informatiques indiquent que les politiques de gestion du risque sont intégrées à la formation officielle dispensée à chaque employé). Plus surprenant encore, moins de 15 % des répondants ont incorporé un plan intégré de gestion du risque à l'infrastructure physique et technique de leur entreprise.

« Nous déployons des efforts considérables pour que le management et le personnel acceptent de faire évoluer leur comportement pour améliorer les pratiques de sécurité. »

Un participant du secteur de l'industrie manufacturière, Europe occidentale

« Il est de plus en plus difficile de préserver des budgets pour répondre aux problèmes de risque informatique, même si les dirigeants d'entreprise identifient parfaitement les coûts lié à la NON RÉSOLUTION de ces problèmes. Il y a souvent une absence de volonté générale d'investir. »

Un participant du secteur Aérospatiale et Défense, Amérique du Nord

Si l'on considère l'éventail des canaux de communication et de formation possibles pour sensibiliser chacun au risque, les entreprises seraient bien inspirées d'adopter une approche plus organisée et précise pour rester en phase avec les problématiques de risque, en communiquant sur ces sujets avec les collaborateurs et en incorporant la gestion du risque informatique dans tous les secteurs de l'entreprise. Répondant à la question « Comment votre entreprise s'informe-t-elle principalement en matière de risques ? », la majorité des répondants ont indiqué que les menaces pour la sécurité étaient prises en charge par des ressources à la fois internes et externes (38 %), une équipe inter-fonctionnelle de dirigeants (26 %) ou un service chargé de la gestion du risque (19 %).

« Généralement, les utilisateurs, le management et les partenaires considèrent le risque selon des perspectives différentes. Mon besoin est de faire converger ces points de vue de manière raisonnable. »

Un participant du secteur de l'industrie manufacturière, Europe occidentale

Évaluer les technologies émergentes

Les participants à l'enquête ont été interrogés sur le positionnement de leur organisation concernant l'acquisition et le déploiement de cinq technologies nouvelles (voir Figure 3) :

- Les outils de réseaux sociaux (par exemple, forums intranet et Internet, messagerie instantanée, bibliothèques, blogs et wikis)
- Plateformes mobiles (Windows® Mobile, BlackBerry OS et Google Android OS, pour n'en citer que trois)
- Cloud computing
- Virtualisation
- SOA.

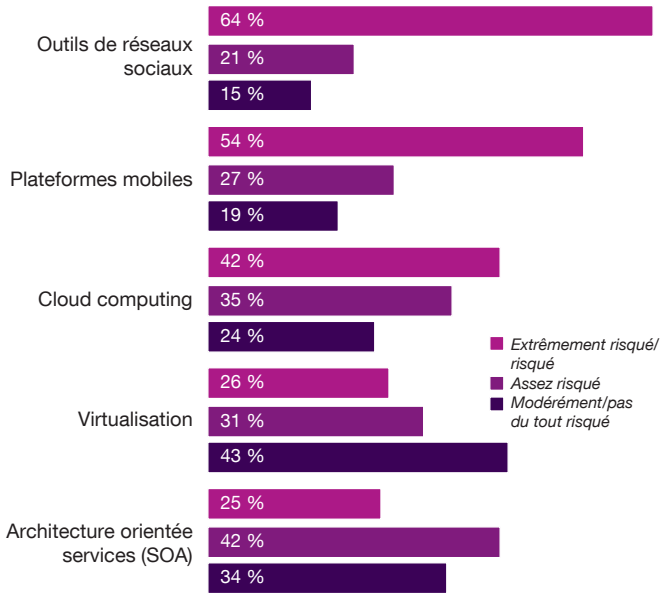

Figure 3 : **Ce sont les réseaux sociaux, les plateformes mobiles et le Cloud computing qui préoccupent le plus les responsables informatiques en matière de risques.**

Des cinq technologies, ce sont les réseaux sociaux, les plateformes mobiles et le Cloud computing qui préoccupent le plus en matière de risques. Pour 64 % des répondants, les outils de réseaux sociaux constituent la principale préoccupation en matière de risques, immédiatement suivis par les plateformes mobiles et le Cloud computing (respectivement 54 % et 43 %). Les risques les plus cités concernent l'accessibilité, l'utilisation et le contrôle des données, notamment concernant les réseaux sociaux, et le danger que représente un accès illicite à des informations confidentielles et sensibles. À noter que la plupart des entreprises n'ont actuellement mis en place ni processus, ni méthodes, pour intégrer les outils de réseaux sociaux dans leurs infrastructures et leurs flux de traitement.

Lorsqu'il leur est demandé de citer les deux risques principaux associés au Cloud computing, la majorité des personnes interrrogées indiquent la protection et la confidentialité des données (voir Figure 4). Si la continuité des activités est à l'évidence une priorité pour plus de la moitié des participants, 44 % des répondants considèrent que les nuages privés apportent davantage de risques que les services IT traditionnels, et 77 % des responsables interrogés expriment leurs préoccupations concernant la confidentialité.

« Le Cloud computing n'apporte un potentiel de résolution d'un problème que si vous pouvez en exploiter les meilleurs atouts. C'est un élément à prendre en compte. »

Un participant du secteur de l'Informatique, Amérique du Nord

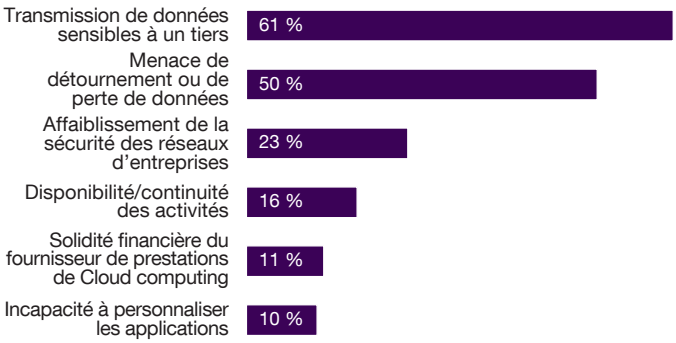

Figure 4 : **Risques associés au Cloud computing.**

La transmission de données à un tiers est également considérée comme un risque par 61 % des répondants, alors que 23 % se préoccupent des failles d'accès aux réseaux.

Vingt-six pour cent seulement des répondants ont indiqué que la virtualisation entraînait des risques significatifs pour leur entreprise. Parallèlement, les risques liés à l'architecture SOA ne préoccupent que 25 % des répondants.

S'appuyer sur le Cloud

Les responsables informatiques sont exposés à l'obligation de réduire leurs dépenses d'infrastructure, de gagner en efficacité et d'améliorer les niveaux de service à l'échelle de l'entreprise. Et nombre d'entre eux se tournent vers le Cloud computing pour contribuer à ces objectifs. Cette technologie constitue une évolution cruciale en matière de modèles informatiques – à l'instar des modèles client-serveur et mainframe qui les ont précédés. Les traitements sont mis en œuvre au moyen d'un réseau de ressources informatiques réparties et accessibles mondialement, exploitables à la demande, sous la forme d'un service. Le Cloud computing constitue une alternative dynamique et hautement automatisée destinée à acquérir et mettre en œuvre des services informatiques – grâce auxquels les utilisateurs accèdent à des Cloud publics, privés ou hybrides, constitués de ressources informatiques et de services, et ce, sans avoir à se préoccuper directement de la technologie associée. Aujourd'hui, les entreprises s'appuient sur les capacités massives d'évolutivité et de collaboration qu'offre le Cloud computing pour résoudre des problèmes qu'il aurait été impossible de traiter auparavant. De plus, le déploiement de nouveaux services s'effectue plus rapidement – et sans investissement supplémentaire. Néanmoins, la prudence et la qualité des informations sont déterminantes lorsqu'il s'agit de choisir un fournisseur, notamment concernant les risques associés.

Conséquences pour les responsables informatiques

Une majorité des responsables informatiques interrogés s'attendent à ce que leurs responsabilités – exécution des politiques et procédures, définition des stratégies de limitation des risques, contribution à la définition et/ou à la surveillance des stratégies en matière de risques informatiques pour l'entreprise – augmentent au cours des trois prochaines années (voir Figure 5). Plus de 65 % d'entre eux s'accordent pour indiquer que la limitation des risques fait partie intégrante de leur fonction et 83 % des répondants considèrent que les responsables informatiques devraient participer davantage à la limitation des risques.

À considérer l'interdépendance croissante de l'opérationnel et de l'informatique, ces réponses ne sont guère surprenantes. Les responsables informatiques et les DSI interrogés considèrent que leur fonction devra englober leur contribution à la stratégie globale de l'entreprise, voire à la marque (pour le marketing et le service client par exemple). Dans le sillage des nombreuses entreprises qui stabilisent ou renforcent leurs stratégies, processus et procédures de gestion du risque, il est possible de confier la responsabilité de l'infrastructure à un fournisseur ou un partenaire – offrant ainsi aux responsables informatiques la possibilité de se recentrer sur la sécurité, la résilience et la continuité des activités métier.

Il est également intéressant de noter qu'après croisement, les réponses données par les 131 DSI participants ne différaient pas significativement de celles des responsables informatiques interrogés.

Si l'intérêt de la gestion du risque informatique et de la conformité est volontiers reconnu par les entreprises, tous secteurs confondus, et qu'elles s'efforcent d'améliorer ces aspects au sein de leurs organisations, peu d'entre elles sont totalement préparées à faire face à l'ensemble des situations associées aux questions de risques et de conformité.

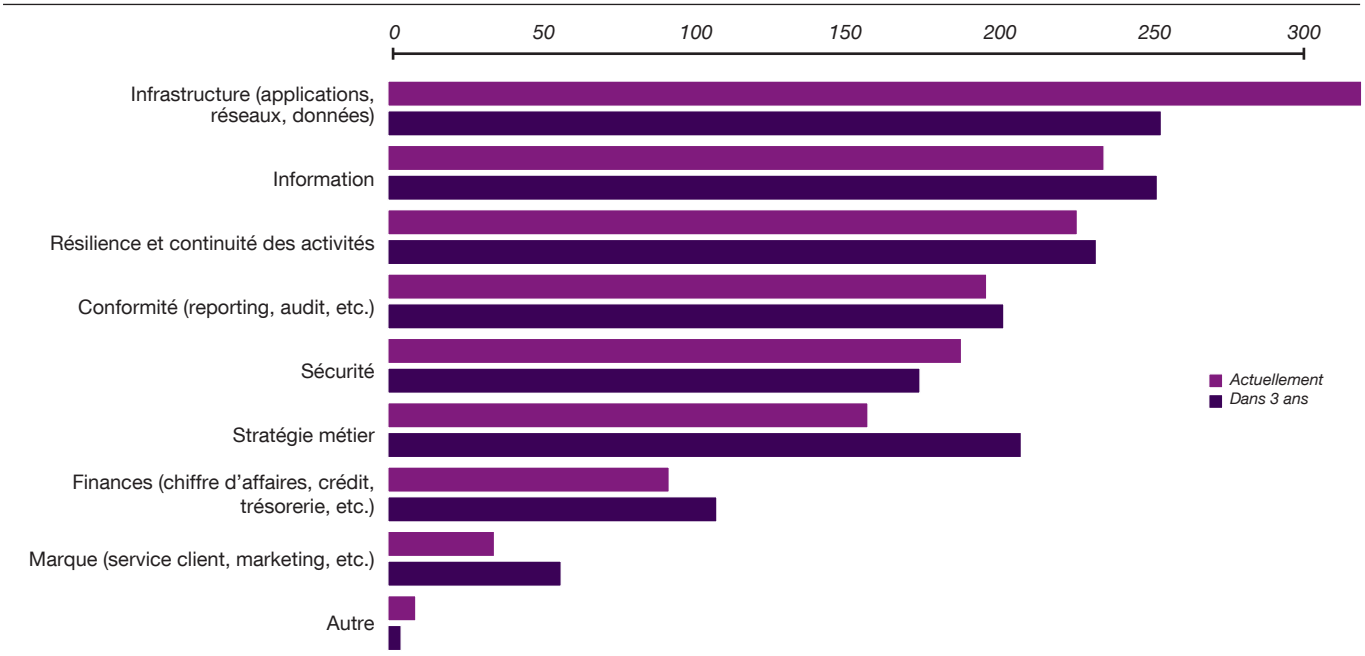

Figure 5 : **Les responsables informatiques envisagent une transformation de leurs domaines de responsabilité au cours des trois prochaines années.**

Les enseignements de l'étude IBM Global IT Risk Study 2010 révèlent des domaines d'intérêt susceptibles de contribuer à l'action des responsables informatiques pour évaluer leur maturité en matière de gestion du risque, à mettre en lumière des disparités, à fixer des priorités et à développer des stratégies dans différents domaines de l'entreprise :

- Au sein d'une entreprise, la sensibilisation aux risques est de la responsabilité de chacun. Hormis les cas pour lesquels les politiques et les procédures en matière de risque font partie intégrante de la culture d'entreprise, nombre d'initiatives de gestion et de limitation des risques n'atteignent pas leurs objectifs, quand elles n'échouent pas totalement. Les enseignements de l'étude confirment que les entreprises doivent renforcer leurs efforts en matière de formation, de communication et de contribution aux actions de gestion du risque et de conformité à l'échelle de l'organisation tout entière.
- Les données constituent une préoccupation commune dans tous les aspects de la gestion du risque informatique – qu'il s'agisse de sécurité, de résilience et de continuité des activités, ou encore de disponibilité, de reprise après incident, de piratage informatique, de conformité, d'infrastructure et de gestion des données. Ceci étant posé, les entreprises se doivent d'adopter une approche unifiée et holistique – c'est-à-dire globale – en prenant en compte tous les éléments permettant d'atteindre leurs objectifs globaux, à savoir obtenir de meilleurs retours sur investissement et gagner en efficacité.

- Lorsqu'il s'agit d'adopter des technologies, des architectures et des stratégies émergentes, de développer des applications nouvelles ou d'intégrer des systèmes existants, la limitation du risque constitue un élément essentiel de discussion. La prise en compte des risques positifs – risques qu'une compagnie est prête à accepter car ils s'accompagnent d'une opportunité commerciale – et des risques négatifs – du fait d'incidents potentiels capables de porter atteinte aux activités – permet de créer davantage de valeur métier et éventuellement, d'accroître le chiffre d'affaires, mais uniquement s'il est prévu un financement approprié pour la gestion du risque informatique.

  Toutes les technologies émergentes ne se valent pas, mais certaines, notamment la virtualisation et le Cloud computing, offrent nombre d'avantages en termes de moyens et de possibilités de limitation des risques. Si le Cloud computing requiert une attention particulière en matière de sécurité des données, un déploiement approprié de cette technologie contribue à réduire les coûts et à limiter les risques associés à la résilience opérationnelle. Cependant, il est essentiel de mettre en place des processus capables de traiter les risques liés à une nouvelle technologie, quelle qu'elle soit.

« Nous avons parfois tendance à aborder le plan d'un projet de manière trop simpliste en pensant avoir identifié les risques, et nous traitons de l'affectation des ressources sur cette base. »

Un participant du secteur Informatique et Technologie, Moyen-Orient et Afrique

Quelle approche adopter ?

Une gestion efficace du risque informatique repose sur une action relevant de plusieurs domaines. Dans leur action, les responsables informatiques peuvent adopter l'approche suivante :

Examiner et évaluer les capacités de l'entreprise en matière de gestion du risque informatique

- Mettre en place une planification à l'échelle de l'entreprise pour toutes les catégories de risques (données, sécurité, résilience, reprise après incident, nouvelles technologies)
- Évaluer l'étendue des problématiques de risque et confirmer qu'un plan est en place pour y répondre (gérer les priorités et limiter les risques « négatifs » comme par exemple les défaillances de systèmes et les failles de sécurité), et vérifier comment tirer parti des risques « positifs » (réduction des délais de mise sur le marché et nouveaux points de contact client, par exemple).

Rechercher le soutien des cadres dirigeants

- Devenir un conseiller avisé et une ressource de valeur pour le DSI ; argumenter les avantages apportés par ces cadres dirigeants en répondant à la problématique du risque informatique
- « Promouvoir » les avantages de la limitation des risques, notamment la croissance de l'entreprise, les gains d'agilité et une meilleure visibilité de la marque.

Déterminer comment sensibiliser davantage à la notion de risque, à tous les niveaux, et l'instiller dans la culture de l'entreprise

- Intégrer la sensibilisation aux risques dans les processus métier et informatiques les plus courants. S'assurer de l'existence de différentes approches pour former l'ensemble du personnel de l'entreprise
- Créer une stratégie de communication périodique concernant l'étendue de la gestion du risque, ainsi que les questions et les problématiques de conformité, en insistant sur le fait qu'il ne s'agit pas d'une activité « au coup par coup ».

Identifier des approches innovantes de mise en œuvre des procédures de limitation du risque

- Élaborer des procédures de gestion du risque intégrées à l'infrastructure informatique, au lieu de les ajouter aux applications élément par élément
- Examiner les processus métier sous l'angle des problématiques potentielles de risque et établir un plan spécifique de gouvernance du risque informatique applicable à l'échelle de l'entreprise tout entière.

S'assurer de l'existence de protections pour éviter tout accès illicite aux données et systèmes de l'entreprise

- Réviser les plans de continuité de l'activité. Celle-ci va bien au-delà de l'anticipation d'une catastrophe naturelle. Elle englobe un éventail large de scénarios d'interruption des activités, des défaillances de serveurs jusqu'aux pandémies
- Sensibiliser chacun à la responsabilité qui lui incombe d'assurer la sécurité et la protection des données, ainsi que les modalités d'exécution de cette responsabilité
- Identifier des outils, des processus et des méthodologies permettant de sécuriser et protéger les données. Garder à l'esprit que de nombreuses solutions existent déjà (accès aux identités et contrôle ; gestion des données de référence ; gestion du cycle de vie de l'information ; processus de gestion de la propriété des données).

La question n'est plus de savoir *si* de nouvelles technologies vont être mises en œuvre dans une entreprise, mais *quand*. Comme mentionné précédemment, si toutes les technologies émergentes ne se valent pas, certaines apportent des avantages considérables en matière de gestion du risque informatique. Les technologies les plus récentes, telles que la virtualisation et le Cloud computing, possèdent des potentiels considérables pour limiter les risques et réduire les coûts.

Qu'en est-il de votre entreprise ?

- **Comment votre entreprise évalue-t-elle sa maturité en matière de risques et de gestion du risque, aussi bien en termes métier que d'infrastructure et de ressources informatiques ?**
- **Quelle stratégie votre entreprise a-t-elle mise en place pour adopter les bonnes pratiques sectorielles et informatiques de limitation du risque – en premier lieu concernant la sécurité, mais aussi en matière de résilience et de continuité des activités ?**
- **De quelle manière les initiatives en matière de risque au sein de votre entreprise contribuent-elles à améliorer la visibilité et le contrôle, et à assurer la conformité avec les contrats, les normes sectorielles, les réglementations et les contrôles internes ?**
- **De quelle manière votre infrastructure informatique contribue-t-elle aux objectifs de performances permanents de l'entreprise en termes de flexibilité, de sécurité, de disponibilité, de gouvernance, d'évolutivité et de résilience ?**
- **Quel type de plan votre organisation a-t-elle adopté pour s'assurer que les ressources humaines, les processus et les systèmes ont la capacité à reprendre leurs activités et réagir à un événement perturbateur ?**

Une gouvernance conjoncturelle du risque informatique, prenant en compte les points de vue technologique et métier, évalue en permanence la vulnérabilité de l'entreprise aux risques informatiques, classe ces risques par ordre de priorité et agit pour les contrer. Il est donc essentiel d'intégrer des protocoles de gestion du risque dans les nouvelles technologies, dès leur mise en œuvre.

La mise en œuvre d'outils et de processus doit s'accompagner, in fine, d'une prise en considération des besoins de l'entreprise. C'est-à-dire concilier vitesse de mise sur le marché et risque acceptable. En adoptant une approche proactive de la gestion du risque informatique, les entreprises disposent des moyens d'anticiper les vulnérabilités et de préserver leur sécurité et leur résilience face aux incidents, planifiés ou non.

En savoir plus

Pour plus d'informations sur cette étude réalisée par l'IBM Institute for Business Value, contactez l'institut à l'adresse suivante : *iibv@us.ibm.com*. Pour obtenir un catalogue complet de nos études, consultez le site à l'adresse suivante :

ibm.com/iibv

Pour accéder à d'autres informations concernant la gestion du risque informatique, consultez le site à l'adresse suivante :

ibm.com/security/fr

Auteurs

Linda Ban est directrice du programme « CxO Study » et responsable des services Application Innovation Services pour l'IBM Institute for Business Value. Elle a la responsabilité de l'équipe mondiale chargée du développement, du déploiement et du suivi des activités IBM à destination des CIO. Parmi d'autres fonctions exercées jusqu'ici, Linda Ban possède une expérience approfondie dans les technologies émergentes et collaboratives, les stratégies métier et opérationnelles, le développement de systèmes et la gestion des opérations. Outre ses interventions auprès de clients, elle a publié de nombreuses contributions concernant un large éventail de problématiques et de solutions métier. Vous pouvez contacter Linda Ban à l'adresse suivante : *lban@us.ibm.com*.

Richard Cocchiara est ingénieur consultant IBM et directeur de l'entité Business Continuity and Resiliency Services chez IBM Global Services. Fort d'une expérience de 28 ans dans les systèmes d'information, il est intervenu en tant que consultant dans les plus grandes entreprises du monde, et en particulier dans le secteur de la finance et de la gestion des titres. Richard Cocchiara est actuellement responsable des activités de recherche et de développement pour les solutions et services de continuité des activités au sein d'IBM Global Technology Services. Vous pouvez contacter Richard Cocchiara à l'adresse suivante : *rmcocch@us.ibm.com*.

Kristin Lovejoy est vice-présidente, chargée de la stratégie de sécurité IBM. Elle a été distinguée par InfoWorld en 2005, parmi les 25 directeurs technologiques les plus performants et par Security Magazine en 2006 comme l'un des 25 dirigeants chargés de la sécurité les plus influents. Elle est l'auteur de brevets américains et européens portant sur un modèle et une méthodologie de gestion du risque orientée objet. Vous pouvez contacter Kristin Lovejoy à l'adresse suivante : *klovejoy@us.ibm.com*.

Ric Telford est vice-président des activités IBM Cloud Services et responsable de la définition de nouvelles solutions et services venant compléter la large gamme d'offres de Cloud computing proposée par IBM. Dans ses fonctions chez IBM, Ric Telford a contribué de manière déterminante à différentes initiatives, notamment en matière de gestion documentaire, d'organisations de réseaux, de gestion de systèmes et de services d'infrastructure IT. Ric Telford était précédemment vice-président, chargé de l'informatique autonome, et responsable du développement de systèmes auto-administrables. Vous pouvez contacter Ric Telford à l'adresse suivante : *rtelford@us.ibm.com*.

Mark Ernest est ingénieur consultant IBM et membre de l'IBM Academy of Technology. Il collabore avec les clients pour la conception et la mise en œuvre de systèmes de gestion informatique permettant de maximiser la valeur de leurs investissements IT et de gagner en efficience et en efficacité dans l'utilisation de l'informatique. Vous pouvez contacter Mark Ernest à l'adresse suivante : *lernest@us.ibm.com*.

Votre partenaire dans un monde en plein changement

Chez IBM, notre mission est de collaborer avec nos clients, en conjuguant notre vision de l'entreprise, nos activités de recherche de haut niveau et nos technologies, pour leur apporter un avantage personnalisé dans un monde en évolution permanente. Grâce à une approche intégrée de la conception et de l'exécution des processus métier, nous contribuons à transformer les stratégies en action. Et avec notre expertise dans 17 secteurs d'activités et une capacité d'intervention couvrant 170 pays, nous sommes aux côtés de nos clients pour les aider à anticiper le changement et bénéficier de nouvelles opportunités d'activité.

Références

1 The IBM X-Force 2010 Mid-Year Trend and Risk Report. IBM Corporation, 2010. http://www-935.ibm.com/services/fr/gts/html/xforce/trendreports/

IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex
France

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

Pensez à recycler

GBE03365-FRFR-00