IBM Institute for Business Value

Faire face aux menaces à l'ère du numérique

Les comités de direction face aux enjeux de sécurité, de risque et de conformité

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 fondées sur des analyses factuelles au sujet de problématiques essentielles rencontrées aussi bien dans le secteur privé que public. Ce rapport stratégique reflète la volonté d'IBM Global Business Services de proposer aux entreprises des analyses et une réflexion qui les aident à produire une forte valeur ajoutée. Pour en savoir plus, vous pouvez contacter les auteurs ou leur adresser un 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 : *ibm.com/iibv*

Auteurs : John Lainhart, Steve Robinson et Marc van Zadelhoff

Les feux des **médias ont récemment** révélé la prolifération d'atteintes à la sécurité affectant des entreprises opérant dans différents secteurs d'activité. Ces défaillances ont non seulement eu pour conséquence des dépenses significatives au sein des entreprises concernées, mais ont en outre considérablement entamé la confiance du consommateur et la réputation des marques. Alors qu'elle n'est plus reléguée dans la sphère d'influence du seul département Informatique, la question de la sécurité est aujourd'hui une priorité incontournable des comités de direction. Dans une économie pilotée par l'information, les entreprises et les organisations doivent s'orienter vers une approche plus méthodique et proactive pour réagir aux menaces contre la sécurité et faire face à leurs obligations en matière de conformité.

Avec l'émergence d'un monde de plus en plus numérique et interconnecté, les brèches possibles pour les menaces et les fuites d'informations se sont multipliées. Aujourd'hui, il existe des milliards de balises RFID (identification par fréquences radio) permettant de localiser des objets, comme, par exemple, des produits, des passeports, des bâtiments et des animaux. Avec plus de 2 milliards d'internautes, et le franchissement de la barre des 5 milliards d'abonnements pour des téléphones mobiles fin 2010, près d'une personne sur trois dans le monde accède au réseau Internet.[1] Plus de 50 milliards d'objets devraient être connectés numériquement d'ici 2020, en particulier les voitures, les équipements et les caméras.[2] Pour accroître encore la complexité de cet éventail de données, le volume d'informations numériques créées et dupliquées dans le monde va progresser pour atteindre un volume inimaginable de 35 milliards de milliards de gigagoctets (Go) d'ici 2020.[3]

Si le volume de ces données a augmenté, la valeur correspondante de ces actifs numériques s'est également accrue. Qu'il s'agisse d'informations sensibles concernant les clients, de propriété intellectuelle ou même de contrôle de machines importantes, les données sont de plus en plus souvent stockées dans des formats électroniques. Les attaques se portant sur ces actifs ont de plus fortes chances d'impacter concrètement l'entreprise tout entière, et pas seulement le département Informatique. Prenons, par exemple, le cas du virus Stuxnet, qui a affecté des contrôleurs de processus chargés du raffinage de l'uranium, en diminuant leurs capacités à traiter et contrôler de manière sécurisée ce matériau extrêmement dangereux.[4] L'incident démontre qu'une action ciblée contre une infrastructure technologique au sein d'une entreprise peut manifestement avoir un impact sur des activités critiques.

Plus importants encore que l'indéniable prolifération des données, des équipements et des connexions, d'autres facteurs font de l'évolution des modalités de gestion de la sécurité et de la conformité au sein des entreprises une question essentielle. Les données importantes existant au sein des entreprises constituent une cible pour les attaquants des systèmes, que ce soit pour des raisons criminelles, en particulier par intérêt économique, pour des motivations personnelles, sous l'effet de la frustration ou avec une intention de vengeance, ou encore pour des raisons politiques, notamment dans le cas du terrorisme. Les atteintes aux informations et aux infrastructures de traitement associées se multiplient, et s'accompagnent d'un degré élevé de « professionnalisme », selon des méthodes toujours mieux organisées.

Il est donc devenu crucial, même si la démarche est difficile, de sécuriser et protéger les informations critiques et les actifs qui y sont associés. En progressant rapidement dans le degré d'attention qu'elle suscite, la sécurité est indéniablement devenue une question émergente au sein des comités de direction. Un directeur marketing évaluera les risques potentiels pour la marque, un directeur financier les conséquences financières d'événements défavorables et un directeur général l'impact des perturbations subies par les systèmes informatiques sur les activités permanentes de l'entreprise. Développer une démarche de *securité intelligente* – c'est-à-dire la capacité à anticiper et à identifier les menaces potentielles, et à y réagir – constitue une priorité inédite dans cette ère numérique.

Les défis en matière de sécurité sont plus redoutables que jamais

L'accroissement du volume des données, du nombre d'équipements et de la prolifération des connexions s'accompagne d'une progression en nombre et en étendue des défis en matière de sécurité, qui appartiennent à trois catégories principales : les menaces extérieures, les menaces internes et les exigences de conformité.

Menaces extérieures

Les médias ont récemment fait état d'une prolifération des attaques extérieures visant des compagnies et des organismes publics importants. Dans le passé, ces attaques provenaient d'individus opérant de manière indépendante. Aujourd'hui mieux coordonnées, elles sont issues de groupes liés aussi bien à des entreprises criminelles qu'à des ensembles organisés de hackers (pirates informatiques) ou « hacktivistes », voire même d'entités financées par des états. Les motivations de ces agresseurs ne se limitent plus à la recherche du profit, et englobent parfois des enjeux de prestige ou d'espionnage. Ces atteintes ont eu pour cible des actifs organisationnels de plus en plus stratégiques, notamment des bases de données de clients, des éléments de propriété intellectuelle, et même des actifs physiques contrôlés par des systèmes informatiques.

Ces attaques issues de l'extérieur s'accompagnent de conséquences financières considérables. Pour prendre un exemple, le détournement de données client de la société Epsilon a porté atteinte aux adresses email de millions de consommateurs, et a directement affecté de très nombreux clients de l'entreprise. Les coûts des réparations initiales et des risques juridiques à plus long terme sont estimés à plusieurs centaines de millions de dollars.[5] Nombre d'autres entreprises, opérant dans les secteurs des services financiers, des médias et du divertissement, mais aussi de la grande distribution et des télécommunications, ont récemment fait état d'atteintes similaires aux informations personnelles et financières de leurs clients, entraînant de ce fait des coûts notables liés aux activités informatiques, juridiques et réglementaires.

Menaces internes

Dans de nombreuses situations, les atteintes à la sécurité de l'information ne sont pas le fait de parties extérieures, mais d'« initiés » opérant dans la place. Ces initiés peuvent être aussi bien des employés, des sous-traitants que des consultants, voire même des partenaires ou des prestataires de services. Les atteintes concernées résultent, par exemple, de négligences ou d'erreurs d'administration (notamment la transmission de mots de passe à des tiers, l'égarement de bandes de sauvegarde ou d'ordinateurs portables, voire la divulgation par inadvertance d'informations sensibles), auxquelles s'ajoutent également les actions délibérées d'employés mécontents.

Ces actions sont tout aussi dangereuses que des attaques extérieures. Pour prendre un cas, l'incident Wikileaks, au cours duquel des enregistrements classifiés ont été diffusés de manière illicite, représente un coût estimé de plusieurs millions de dollars pour le gouvernement américain, outre la dégradation des relations avec les gouvernements d'autres pays du monde.[6]

Exigences de conformité

Les entreprises se doivent de respecter un nombre toujours croissant d'obligations nationales, sectorielles et locales en matière de sécurité, qui répondent à des standards et à des exigences de déclaration spécifiques. Parmi les nombreux exemples possibles, figurent les réglementations U.S. Sarbanes-Oxley (SOX), J-SOX, COSO, COBIT, mais aussi les normes internationales ISO/IEC, la réglementation américaine HIPAA/HITECH, la directive européenne sur la protection des données personnelles, les normes indiennes sur la sécurité et la confidentialité des données, ainsi que les normes PCI DSS et BASEL II. Le respect de ces obligations impose souvent des délais et des efforts considérables pour déterminer les priorités des enjeux, développer des politiques appropriées et contrôler et surveiller la conformité.

Les priorités des comités de direction résultent de la conscience de l'impact

Les menaces et les exigences de conformité ont un impact important sur la capacité de chaque dirigeant à respecter ses priorités stratégiques. Alors que la technologie joue un rôle de plus en plus important, les défis liés à la sécurité des données dépassent largement la sphère d'influence des directeurs des systèmes d'information (DSI). Nos entretiens avec plus de 13 000 dirigeants d'entreprise depuis 2008 indiquent que tous les membres des comités de direction sont influencés par les questions de sécurité (voir Figure 1).

Si certains dirigeants mettent l'accent sur certaines problématiques de sécurité plutôt que d'autres, les entreprises ne peuvent se permettre d'ignorer la nécessité d'agir de front pour répondre aux risques actuels en matière de sécurité. Les responsabilités en la matière, plus clairement définies dans le passé, dépassent aujourd'hui les limites des silos organisationnels, à l'image des dommages potentiels étendus dans le cas où une atteinte est avérée.

À titre d'exemple, un directeur marketing, qui se consacre avec énergie à renforcer l'image de sa marque, peut s'exposer au risque de perdre la confiance de ses clients et d'altérer la réputation de l'entreprise en cas d'atteinte à la sécurité conduisant à la perte d'informations personnelles des clients. Incontestablement, ce risque est primordial et toute atteinte à la réputation d'une entreprise impose une action concertée du comité de direction.

Parmi quelques exemples de risques concernant la sécurité, gérés principalement par certains membres du comité de direction, figurent les situations suivantes :

- Les *Présidents directeurs généraux* doivent porter leur attention sur les éléments de propriété intellectuelle et les données métier sensibles, susceptibles d'être détournés par des personnes opérant de l'intérieur de l'entreprise ou par des parties extérieures. Ces types d'intrusions ont un impact potentiel considérable en termes de pertes éventuelles de parts de marché et de réputation, de risques opérationnels liés à des obligations de cessation d'activité et de poursuites criminelles éventuelles.

	PDG	DAF/DG	DSI	DRH	DM
Priorité DG et CoDir	• Maintenir la différenciation vis-à-vis de la concurrence	• Respecter les obligations légales de conformité	• Développer l'utilisation des équipements mobiles	• Favoriser la flexibilité du personnel au niveau mondial	• Renforcer la marque
Risques relatifs à la sécurité	• Détournement d'éléments de propriété intellectuelle • Détournement de données métier sensibles	• Impossibilité de respecter les obligations légales	• Prolifération des données • Terminaux non sécurisés et accès inappropriés	• Fuite de données sensibles • Comportement irréfléchi d'un collaborateur interne	• Vol d'informations personnelles concernant les clients ou les employés
Impact potentiel	• Pertes de parts de marché et dégradation de la réputation • Mises en examen	• Échec des audits • Amendes, compensations et mises en examen	• Atteintes à la confidentialité, à l'intégrité et/ou à la disponibilité des données	• Violation de la vie privée des employés	• Perte de confiance des clients • Dégradation de la réputation de la marque

Source : Plus de 13 000 entretiens en face à face avec des dirigeants, menés dans le cadre des études de l'IBM Institute for Business Value.

Figure 1 : **Répondre aux enjeux de sécurité et de conformité est une priorité pour les comités de direction.**

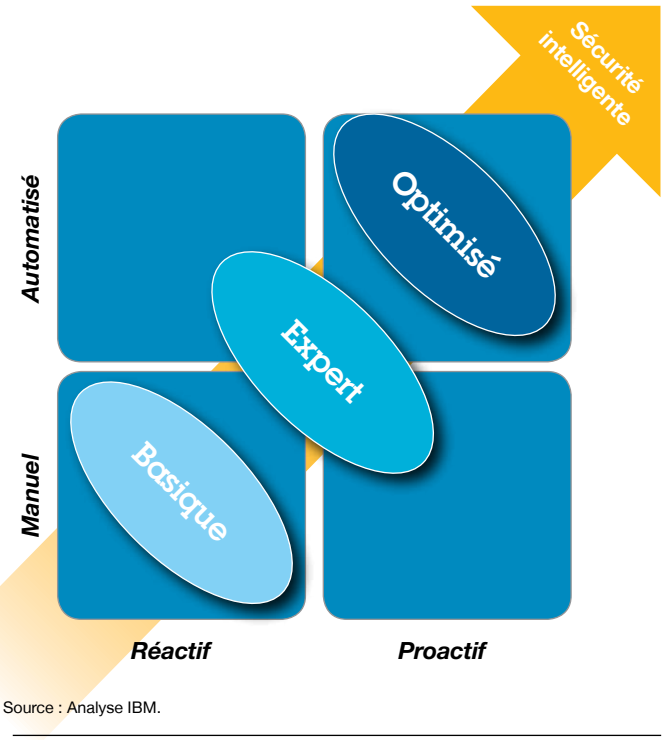
- Les *directeurs financiers* sont particulièrement concernés par les questions de réglementation. L'incapacité à respecter les dispositions de sécurité prévues par la réglementation peut conduire à un échec des processus d'audit et à des amendes pour l'entreprise, voire même des poursuites criminelles aussi bien à titre personnel que pour l'entreprise.
- Les *directeurs des systèmes d'information* qui cherchent à développer la flexibilité et la mobilité au sein de l'entreprise doivent résoudre les défis relatifs à la prolifération des données, à l'augmentation du type et du nombre de terminaux non protégés et à des accès inappropriés à des données. Ces différents problèmes peuvent potentiellement conduire à des atteintes à la confidentialité, à l'intégrité ou à la disponibilité des données.
- Les *directeurs des ressources humaines*, dont la mission est de développer la flexibilité du personnel de l'entreprise, doivent être sensibilisés à l'éventualité de fuites de données sensibles, voire même aux attitudes potentiellement négligentes de personnes appartenant à l'entreprise, susceptibles d'entraîner des atteintes à la confidentialité des informations concernant les employés.

Pour résumer, les questions de sécurité ne relèvent ni de la seule responsabilité du directeur des systèmes d'information, ni d'une simple délégation au directeur de la sécurité. Le sujet réclame l'attention et l'action de l'ensemble du comité de direction.

Construire une « sécurité intelligente » par étapes successives

Pour répondre à la fois à la prolifération et à l'intensité des risques, les entreprises se doivent d'envisager une approche plus automatisée et proactive de la sécurité. Ce qui veut dire intégrer la *sécurité intelligente* et la considérer comme un élément essentiel de l'entreprise. Pour cela, l'entreprise doit s'appuyer sur une démarche complète englobant différentes problématiques, notamment la sécurité physique, la classification des données, la sensibilisation des employés et les capacités de contrôle.

Dans la plupart des entreprises, la sécurité intelligente évolue à trois niveaux. D'où le remplacement des approches manuelles par des processus de plus en plus automatisés permettant d'identifier, de suivre et de résoudre les menaces. La tendance s'oriente sur une anticipation accrue des problèmes de sécurité plutôt que de s'appuyer sur des démarches réactives (voir Figure 2).



Source : Analyse IBM.

Figure 2 : **Une approche structurée en trois niveaux pour bâtir une sécurité intelligente**

- *Basique* – La sécurité est recentrée sur une protection périmétrique, pour réguler à la fois les accès physiques et virtuels. La protection périmétrique permet l'entrée d'informations pour la diffusion de rapports établis manuellement concernant les incidents et les piratages. Les entreprises opérant à un niveau de sécurité Basique déploient des pare-feu, des antivirus, des systèmes de contrôle d'accès et la génération manuelle de rapports, qui constituent des étapes initiales pertinentes. Cependant, elles agissent dans un mode réactif et manuel et bénéficient d'une vision limitée de leur situation réelle en matière de sécurité.

- *Expert* – La sécurité est intégrée dans les différentes couches du réseau d'applications informatiques et d'opérations métier. Cette démarche se caractérise par l'intégration de la sécurité dans des applications, des bases de données et des processus métier essentiels. Au niveau Expert, la sécurité devient plus complète, avec l'inconvénient, cependant, de la complexité supplémentaire qui accompagne les efforts de sécurité de l'entreprise. D'où un niveau insuffisant de sécurité intelligente, sous l'effet de mesures plus diffuses et moins bien coordonnées.
- *Optimisé* – À ce niveau, les entreprises utilisent des outils analytiques de sécurité prédictifs et automatisés pour évoluer vers une sécurité intelligente. La sécurité est optimisée, car cette démarche englobe le profilage des intrusions précédentes, des activités des employés et d'autres sources de données, permettant ainsi d'anticiper la localisation des atteintes potentielles aux données et de les éviter.

Chacun de ces trois niveaux vient ajouter une couche supplémentaire de préparation aussi bien concernant les incidents involontaires que délibérés. Pour identifier et combler les failles de sécurité à l'échelle de l'écosystème global d'une entreprise, il est nécessaire d'explorer et d'exploiter les capacités analytiques pour répondre aux besoins les plus urgents. Une évaluation détaillée des quatre domaines de sécurité permet d'accompagner les entreprises vers une sécurité plus intelligente en améliorant méthodiquement la gouvernance, la gestion des risques et la conformité (voir Figure 3).

- *Personnes* – Dépasser le contrôle des accès, application par application, au moyen de mots de passe, pour s'orienter vers une approche fondée sur les rôles, en maîtrisant les accès des utilisateurs au travers de tableaux de bord et de dispositifs de contrôle des droits des utilisateurs.
- *Données* – Aller au-delà des méthodes élémentaires de protection des données (contrôle d'accès, chiffrement), en améliorant la gouvernance des données et la gestion de l'utilisation et de la circulation de ces données.
- *Applications* – Dépasser la nécessité d'analyser les vulnérabilités dans les applications existantes pour s'orienter vers la détection des actes frauduleux et l'intégration de la sécurité dans les nouvelles applications.
- *Infrastructure* – Remplacer les méthodes réactives – comme par exemple le blocage des accès non autorisés et des virus – par des méthodes proactives, permettant de sécuriser les systèmes en assurant des opérations évoluées de surveillance et d'expertise judiciaire en informatique.

Domaines de sécurité	Aujourd'hui	Fossé des processus de sécurité	Demain : Sécurité intelligente	
Personnes	Gérer les identités application par application		Utiliser des tableaux de bord intégrant les rôles et une gestion des utilisateurs privilégiés	Appliquer des outils de corrélation évoluée et d'analyse détaillée
Données	Déployer des processus de contrôle des accès et de chiffrement		Surveiller l'utilisation et contrôler les fuites	
Applications	Analyser les vulnérabilités		Intégrer la sécurité dès la phase initiale	
Infrastructure	Bloquer les accès réseau indésirables et les virus		Mettre en œuvre une détection en temps réel des menaces avancées dans une logique de recherche de preuves (Forensic)	

Réactif → ***Proactif***

Source : analyse IBM.

Figure 3 : **Une approche équilibrée est nécessaire pour gérer les actifs physiques, technologiques et humains.**

Une approche sur trois axes pour les comités de direction

Les membres du comité de direction se doivent d'agir sur trois axes pour l'élaboration d'une sécurité intelligente :

- **Information.** Adopter une approche structurée pour évaluer les risques métier et informatiques.
- **Cohérence.** Mettre en œuvre et appliquer l'excellence en matière de sécurité à l'échelle de l'entreprise tout entière.
- **Intelligence.** Utiliser les outils analytiques pour mettre en évidence de manière proactive les risques, et identifier, surveiller et résoudre les menaces.

1. Information

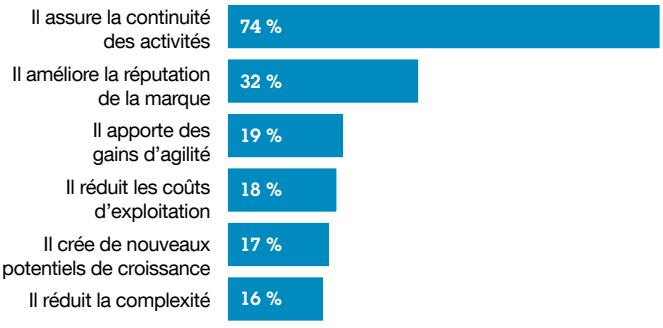
Obtenir des informations suppose de résoudre les risques de sécurité informatique au sein d'un cadre étendu de gestion des risques d'entreprise (voir Figure 4).

Source : IBM Institute for Business Value. Étude « IBM Global IT Risk Study 2010 ». Septembre 2010.

Figure 4 : **Étapes essentielles pour mettre en œuvre une gestion du risque opérationnel.**

Cette approche structurée de l'évaluation des risques métier et informatiques consiste à identifier les menaces essentielles et les obligations légales de conformité ; analyser les risques et les défis en matière de sécurité ; mettre en œuvre et appliquer les processus de gestion des risques et les cadres communs de contrôle ; et exécuter les processus de gestion des incidents en cas de crise. Autre action importante, la nomination d'un responsable chargé des risques, au sein du comité de direction. Ce responsable assure une liaison permanente avec le conseil d'administration et les autres membres de la direction concernant les enjeux de sécurité, et conduit un dialogue au sujet du risque informatique au sein de l'entreprise.

Les participants à l'étude mondiale « IBM Global IT Risk Study » disent considérer les investissements dans la gestion du risque informatique comme porteurs d'avantages importants pour l'entreprise, notamment concernant la continuité des activités (74 pour cent) et la protection de la réputation de l'entreprise (32 pour cent, voir Figure 5). Selon les dirigeants interrogés, la gestion du risque informatique doit aller bien au-delà d'une tactique de défense. Ces dirigeants citent également les gains d'agilité, la réduction des coûts, les opportunités nouvelles de croissance et la simplification comme des avantages résultant d'une gestion plus efficace du risque informatique.[7]



Source : IBM Institute for Business Value Étude « IBM Global IT Risk Study 2010 ». Septembre 2010.

Figure 5 : **Les avantages de l'amélioration de la gestion du risque informatique.**

Exemple :

Les difficultés liées aux audits relatifs aux risques pesant sur le contrôle de la sécurité informatique entraînent une modernisation des processus de gouvernance informatique

Une grande institution financière se trouvait confrontée à des problématiques importantes de contrôle des activités métier et de gouvernance informatique, aussi bien en interne qu'à l'extérieur de l'entreprise. Un chargé d'audit extérieur a mis en évidence un certain nombre d'insuffisances significatives, notamment des lacunes concernant l'application de la réglementation Sarbanes-Oxley (SOX). Par ailleurs, des processus d'audit interne ont conduit à la production de nombreux rapports défavorables concernant la sécurité informatique.

L'entreprise s'est préparée à mettre en œuvre un programme de gouvernance robuste et complet, fondé sur les meilleures pratiques du secteur, et accompagné d'un système permettant de s'assurer de la mise à jour et de l'amélioration périodiques des nouveaux contrôles. Le processus a débuté par une évaluation complète de la sécurité de l'entreprise et de l'ensemble de ses systèmes de contrôle (contrôles informatiques généraux, contrôles des applications, gouvernance informatique). La gouvernance en matière de sécurité des informations a ensuite été évaluée, notamment pour analyser les processus de sécurité et rédiger ou mettre à jour des politiques, des normes et des procédures.

Les failles identifiées ont été résolues en nommant des comités chargés de la gouvernance informatique, s'appuyant sur des politiques, des normes et des procédures précises. En outre, l'entreprise a mis en œuvre un cadre de gouvernance informatique et des outils opérationnels pour résoudre efficacement les problèmes et les points faibles relatifs au reporting financier concernant la sécurité, l'intégrité des données, la conduite du changement et l'opérationnel.

Suite à ces actions, cette institution financière a pu réaliser un audit parfait de sa situation financière et obtenir de son chargé d'audit extérieur une opinion favorable concernant la réglementation SOX – un résultat que l'entreprise n'avait pas obtenu au cours des trois années précédentes. L'institution a pu ainsi déposer une nouvelle offre d'actions auprès de la SEC (autorité américaine des marchés financiers), en bénéficiant d'une confiance accrue des investisseurs et d'une augmentation de la valeur de ses actions. Elle a en outre pu institutionnaliser son programme complet de gouvernance informatique, en assurant une amélioration continue de cette gouvernance et des processus et pratiques de sécurité.

2. Cohérence

La sécurité est appelée à dépasser les frontières de l'entreprise. Les plus efficaces d'entre elles se doivent de mettre en œuvre et d'appliquer l'excellence en matière de sécurité à l'échelle de l'organisation tout entière. Ce qui suppose de susciter la participation des principales parties prenantes, et notamment :

- *Les clients* – Développer des politiques concernant les informations personnelles, et communiquer à leur sujet. Assurer la transparence et répondre rapidement aux atteintes à la confidentialité.
- *Les collaborateurs de l'entreprise* – Définir des objectifs précis en matière de sécurité et de confidentialité. Mettre en œuvre des formations pour identifier et résoudre des risques relatifs à la sécurité. Gérer les accès aux systèmes et aux données, et leur utilisation.
- *Les partenaires* – Collaborer avec des entreprises intégrées à la chaîne logistique pour développer et mettre en œuvre des normes de sécurité. Informer les partenaires des risques, et les gérer (par exemple, les incidents relatifs à la sécurité), et ce, comme un processus normal dans le cadre des activités opérationnelles.
- *Les chargés d'audit* – Corréler les risques pesant sur l'entreprise et sur l'informatique. Contribuer aux cadres de référence des contrôles. Procéder à des évaluations périodiques des politiques liées à la réglementation et aux processus internes à l'entreprise.
- *Organismes de régulation* – Gérer les risques liés à la réglementation et démontrer la conformité à cette réglementation. Évaluer et modifier les contrôles existants en fonction des besoins de changement.

Exemple :

Une gouvernance efficace contribue au respect des obligations sectorielles de conformité et à la réactivité des processus d'audit

Face à une multitude d'opérations d'audit menées chaque année, une mutuelle de santé souhaitait gérer ses risques en mettant en œuvre et en actualisant des processus de contrôle de prudence plutôt que d'avoir à réagir à chaque rapport d'audit. Cette mutuelle souhaitait en outre réduire l'impact de ces audits sur son activité. Parallèlement, elle se devait d'assurer sa conformité à de nouvelles exigences réglementaires liées au secteur de l'assurance, notamment avec la réglementation HIPAA (Health Insurance Portability and Accountability Act) et le modèle d'audit NAIC (National Association of Insurance Commissioners).

La solution adoptée a consisté à restructurer la gouvernance des processus informatiques. Dans le cadre de cette démarche, la mutuelle a institué des contrôles standardisés de sa gouvernance informatique pour l'ensemble de ses activités et de ses divisions opérationnelles, notamment pour la gouvernance de 15 processus informatiques critiques. Pour chacun d'eux, un processus cyclique a été mis en place, afin d'identifier les risques et de définir le cadre de contrôle, par une approche consistant à concevoir et mettre en œuvre des procédures de gouvernance, puis à les tester, et enfin, à évaluer les résultats et à diffuser des rapports.

Au-delà de sa capacité à évaluer, grâce à ces nouveaux contrôles, son niveau de conformité à la réglementation et aux normes sectorielles, la mutuelle a réussi à mieux corréler les objectifs de l'entreprise et de l'informatique, à gérer plus efficacement le risque et à gagner en sécurité. Elle dispose aujourd'hui d'une capacité de réaction plus efficace et cohérente aux audits, en réduisant de près de moitié les opérations nécessaires pour faire face à ces audits.

3. Intelligence

Utiliser les outils d'analyse pour mettre en évidence de manière proactive les risques, et identifier, surveiller et résoudre les menaces. Alors que les entreprises se doivent de renforcer leurs défenses en matière de sécurité, l'utilisation des outils d'analyse prévisionnelle joue un rôle de plus en plus important (voir Figure 6). Ces outils permettent des corrélations sophistiquées permettant de détecter des menaces évoluées et durables, intègrent la notion de gouvernance et utilisent des processus automatisés de gestion du risque – autant d'éléments de construction nécessaires à une sécurité intelligente.

Ces outils disposent des capacités nécessaires pour :

- Identifier des modèles concernant des atteintes précédentes et des menaces extérieures pour prédire des domaines potentiels d'attaque ;
- Analyser de manière détaillée les comportements des systèmes des employés pour identifier des modèles de détournements possibles ;
- Surveiller l'environnement extérieur pour y détecter des menaces potentielles relatives à la sécurité.

Sécurité intelligente

	Personnes	Données	Applications	Infrastructure
Optimisé	• Gouvernance, risque et conformité • Outils de corrélation évoluée et d'analyse détaillée			
	• Analyse fondée sur les rôles • Contrôle des utilisateurs privilégiés	• Analyse des flux de données • Gouvernance des données	• Développement d'applications sécurisées • Détection d'actions frauduleuses	• Surveillance évoluée des réseaux/expertise judiciaire informatique • Systèmes sécurisés
Expert	• Gestion des identités • Authentification forte	• Surveillance des activités • Prévention des pertes de données	• Pare-feu d'application • Analyse du code source	• Gestion des actifs • Gestion de la sécurité des points terminaux/ des réseaux
Basique	• Mots de passe et identifiants utilisateur	• Chiffrement • Contrôle des accès	• Analyse des vulnérabilités	• Sécurité périmétrique • Anti-virus

Source : Analyse IBM.

Figure 6 : **Utiliser les outils d'analyse pour mettre en évidence de manière proactive les risques, et identifier, surveiller et résoudre les menaces.**

Exemple :

Les outils d'analyse facilitent la mise à niveau des capacités de gestion des risques relatifs à la sécurité

Tout en cherchant une approche « plus intelligente » pour résoudre les menaces auxquelles elle était exposée, une entreprise de dimension mondiale opérant dans le secteur du médicament souhaitait réduire les coûts et la complexité de son environnement de solutions de sécurité, issues de différents fournisseurs. L'absence de corrélation entre les menaces signalées et les données de vulnérabilité de son infrastructure de sécurité obsolète rendait difficile l'identification d'incidents réellement critiques. En outre, il était nécessaire de faire appel à des personnels compétents pour surveiller proactivement et en temps réel les alertes émises par différents équipements de sécurité et de mettre en œuvre les actions nécessaires avant que les atteintes au système ne se produisent.

Grâce à des solutions logicielles de sécurité, à l'expertise de consultants et à des prestations externalisées, l'entreprise a pu à la fois développer ses capacités de protection et réduire les coûts et la complexité.

Aujourd'hui, des millions d'événements de sécurité issus de solutions hétérogènes sont analysés dans l'ensemble de l'environnement informatique de l'entreprise, et des outils d'analyse sophistiqués traitent en temps réel les données relatives à ces événements. Pour corriger rapidement les problèmes et réduire les domaines de vulnérabilité, l'entreprise bénéficie de conseils d'experts. De plus, les rapports générés permettent le suivi et l'analyse de tendance des données relatives aux vulnérabilités et aux menaces, au profit d'une vision élargie de la situation en matière de sécurité.

Dans le cadre de cette transformation des processus de sécurité, l'entreprise a réussi à consolider les environnements utilisés, issus aujourd'hui d'un seul fournisseur, contre cinq auparavant. Plus important encore, cette approche proactive a permis à l'entreprise de réduire de 57 pour cent les coûts de gestion de la sécurité, avec une baisse du nombre d'événements de sécurité critiques ramené à 15, contre 10 000 auparavant.

Êtes-vous en train de construire une démarche de sécurité intelligente ?

Selon les menaces potentielles et les possibilités de limiter les risques grâce à une approche plus évoluée de la sécurité, une entreprise peut évaluer ses réponses aux questions suivantes :

Tous domaines

- Disposez-vous d'un programme d'évaluation de vos risques relatifs à la sécurité ?
- Quelles sont vos capacités à détecter des menaces et à contrôler la conformité, quel que soit le domaine concerné ?
- Disposez-vous de fonctionnalités de stockage de journaux et d'audits ?
- Quels processus utilisez-vous pour traiter les réponses à des incidents et les reprises après sinistre ?
- Comment suscitez-vous la participation d'intervenants internes et extérieurs à l'entreprise concernant les questions de sécurité ?

Personnes

- Quelle est la portée du déploiement du programme de gestion des identités mis en œuvre ?
- De quelle manière êtes-vous informé de ce que font les utilisateurs autorisés ?
- Disposez-vous d'un programme d'automatisation de la gestion des identités et des rôles ?

Données

- Quelles méthodes utilisez-vous pour classifier et chiffrer vos données sensibles ?
- Comment savez-vous si des données sensibles sont en train de quitter votre réseau ?
- Comment surveillez-vous les accès à des données, y compris les accès privilégiés ?

Applications

- Comment les dispositions de sécurité ont-elles été intégrées dans votre processus de développement d'applications dès la phase initiale ?
- Comment procédez-vous pour tester périodiquement les vulnérabilités de votre site web ?
- Quelle est votre approche pour tester les applications patrimoniales et détecter des expositions potentielles à des risques ?

Infrastructure

- Comment procédez-vous pour installer rapidement des correctifs logiciels sur des équipements connectés ?
- Comment surveillez-vous les échanges réseau en entrée et en sortie ?
- Comment intégrez-vous une démarche de sécurité dans vos nouvelles initiatives (par exemple l'environnement Cloud, les solutions de mobilité, entre autres) ?

Conclusion : la réalité des risques exige une action intégrée du comité de direction

Dans un monde actuel de plus en plus complexe et interconnecté, les risques sont réels et progressent de manière exponentielle. Une entreprise qui aurait choisi de déléguer les questions de sécurité au seul directeur des systèmes d'information cumulerait les facteurs de risque. Plus que jamais, chaque membre de la direction d'une entreprise est dépositaire d'un enjeu significatif – et peut jouer un rôle important – pour protéger les données et le capital intellectuel circulant dans l'entreprise (voir Figure 7). S'il existe un dénominateur commun, c'est de constater qu'aujourd'hui, la sécurité va bien au-delà d'une simple question technique. Il s'agit davantage d'engager un dialogue franc concernant les risques et les investissements, et d'adopter une approche préventive pour répondre aux questions de sécurité.

Il est bien sûr impossible de répondre de manière abordable à tous les risques et imprévus possibles. Plutôt que d'essayer d'assurer une protection contre toutes les menaces possibles, les entreprises doivent définir les priorités des risques potentiels, liées à leur impact métier. Cependant, ces priorités dépendent des informations données par les différents dirigeants de l'entreprise qui disposent de point de vue spécifiques sur leurs domaines d'intervention particuliers.

Pour en savoir plus sur cette étude publiée par l'IBM Institute for Business Value, contactez-nous à l'adresse suivante : *iibv@us.ibm.com*. Si vous souhaitez obtenir un catalogue complet de nos études, visitez le site :

ibm.com/iibv

Recevez en priorité les informations les plus récentes proposées par l'IBM Institute for Business Value. Inscrivez-vous pour recevoir IdeaWatch, notre lettre d'information électronique mensuelle proposant des études de haut niveau, et constituant une source de connaissances et de recommandations stratégiques issues de nos études :

ibm.com/gbs/ideawatch/subscribe

PDG	DAF	DG	DSI	DRH	DM
Éviter tout impact des risques relatifs à la sécurité sur l'actionnariat et la confiance	Connaître les conséquences financières d'événements indésirables en matière de sécurité	Évaluer l'impact des perturbations des systèmes informatiques sur l'opérationnel	Connaître les effets à l'échelle de l'entreprise des erreurs relatives à la sécurité des informations	Déterminer les risques associés à une fuite injustifiée de données relatives aux employés	Répondre aux problématiques de marque consécutives à des atteintes à la sécurité

Source : Analyse IBM.

Figure 7 : **La sécurité est l'une des responsabilités des comités de direction.**

Le partenaire de choix, sur une planète en pleine évolution

Chez IBM, la collaboration avec les clients est une priorité. Notre objectif est de conjuguer notre vision de l'entreprise, des études approfondies et des technologies pour apporter à nos clients un avantage personnalisé dans un environnement marqué par les évolutions rapides. Grâce à notre approche intégrée des processus métier et de l'exécution, nous contribuons à transformer les stratégies en actions. Et avec nos compétences d'experts dans 17 secteurs d'activité et nos capacités d'intervention mondiales dans 170 pays, nous sommes aux côtés de nos clients pour anticiper le changement et leur permettre de bénéficier de nouvelles opportunités.

À propos des auteurs

John Lainhart est responsable des activités Global Security & Privacy Service et U.S. Public Sector Cybersecurity & Privacy Service au sein d'IBM Global Business Services. Il représente IBM au sein de l'équipe Data Integrity du comité exécutif des prestations d'assurance de l'AICPA (Certified Public Accountant). Il a occupé différents postes au sein de l'ISACA (Information Systems Audit and Control Association) et de l'IT Governance Institute, notamment dans ses fonctions de président international, et est actuellement membre du Framework Committee, co-président de l'équipe CobiT 5 Task Force, et conseiller principal des initiatives IT Governance, CobiT, ValIT et d'autres initiatives relatives au référentiel RiskIT. Vous pouvez le contacter par email à l'adresse : *john.w.lainhart@us.ibm.com*.

Steve Robinson est directeur général d'IBM Security Solutions, et responsable mondial des initiatives IBM Security concernant les produits de sécurité et les divisions de services. Dans son rôle de responsable stratégique, il accompagne les équipes de développement de logiciels, de matériels et de prestations, ainsi que les équipes marketing et commerciales des offres de sécurité. Précédemment, Steve Robinson a été directeur commercial mondial IBM Rational Software depuis 2005, avec la responsabilité de la stratégie commerciale et de la mise en œuvre pour la marque Rational. Il a dirigé une équipe internationale de plus de 1 000 personnes englobant des commerciaux et des équipes de distribution, ainsi qu'une communauté étendue fondée sur des relations stratégiques (partenaires commerciaux, intégrateurs de systèmes, ISV - éditeurs indépendants de logiciels). Entré chez IBM en 1984, Steve Robinson a occupé différentes fonctions de direction et d'encadrement relatives aux activités commerciales, aux prestations techniques et à la gestion de produits. Vous pouvez le contacter par email à l'adresse : *steve_robinson@us.ibm.com*.

Marc van Zadelhoff est directeur de la stratégie mondiale d'IBM Security Solutions. Sa responsabilité englobe la gestion des offres, les budgets et le positionnement mondial de la gamme de logiciels et de prestations d'IBM. Dans ses fonctions, il est chargé d'accompagner le conseil consultatif des clients d'IBM et rencontre des clients du monde entier pour développer les orientations d'IBM. Au sein d'IBM, Marc van Zadelhoff a dirigé des opérations de fusion-acquisition pour Tivoli, l'équipe marketing de la division Internet Security Systems (ISS) rachetée par IBM, et, plus récemment, les activités Strategy, Portfolio & Business Development d'IBM Security Services au sein de la division Global Technology Services. Marc van Zadelhoff a commencé sa carrière comme consultant en stratégie. Vous pouvez le contacter par email à l'adresse : *marc.vanzadelhoff@us.ibm.com*.

Ont collaboré à ce rapport stratégique

Linda Ban, directrice des études Global CIO Study, études AIS, IBM Institute for Business Value, IBM Global Business Services.

Hans A.T. Dekkers, Associate Partner, IBM Global Business Services.

Peter Korsten, partenaire et responsable mondial, IBM Institute for Business Value, IBM Global Business Services

Eric Lesser, directeur d'étude et responsable pour l'Amérique du Nord, IBM Institute for Business Value, IBM Global Business Services.

Kristin Lovejoy, directrice, IT Risk, équipe IBM BT/CIO.

Wolfram Stein, partenaire et directeur, chargé des activités Global Strategy & Transformation Service, Consulting Services, IBM Global Business Services.

Nichola Tiesenga, partenaire, Public Sector, Cybersecurity and Privacy, IBM Global Business Services.

Marisa Viveros, directrice, IBM Security Services, IBM Global Technology Services.

Références

1 International Telecommunications Union. « Global Number of Internet Users, total and per 100 Inhabitants, 2000-2010 » United Nations. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/Internet_users_00-10_2.xls

2 Ericsson. « More than 50 billion connected devices – taking connected devices to mass market and profitability ». 14 février 2011. http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c

3 IDC « Digital Universe Study », sous l'égide d'EMC. Mai 2010.

4 McMillan, Robert. « Siemens: Stuxnet worm hit industrial systems ». *ComputerWorld*. 14 septembre 2010. http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

5 Greene, Tim. « Worst-case projected cost of Epsilon breach: $4B ». *NetworkWorld*. 1er mai 2011. http://www.networkworld.com/news/2011/050111-epsilon-breach-costs.html

6 Fildes, Jonathan. « What is Wikileaks? ». BBC. 7 décembre 2010. http://www.bbc.co.uk/news/technology-10757263

7 Ban, Linda B., Richard Cocchiara, Kristin Lovejoy, Ric Telford et Mark Ernest. « Le nouveau rôle des responsables informatiques et des directeurs des systèmes d'information » - IBM Institute for Business Value, septembre 2010. http://www-935.ibm.com/services/fr/gts/pdf/ibm_it_risk_study2010_overview_gbe03367frfr.pdf

IBM France
17 Avenue de l'Europe
92275 Bois Colombes Cedex
France

Produit aux États-Unis
Août 2011

Veuillez recycler

GBE03423-FRFR-00