CIO - études -

MAITRISER LE RISQUE A L'HEURE DES MENACES COMPLEXES

MAI 2014

CIO en partenariat avec

CESIN Akamai Check Point SOFTWARE TECHNOLOGIES LTD. FireEye intel Security Level(3) TREND MICRO

Cette étude a été réalisée et publiée à l'occasion de la conférence « Maîtriser le risque à l'heure des menaces complexes » organisée par CIO le 20 mai 2014 au Centre d'Affaires Paris Trocadéro.

La rédaction de CIO tient à remercier tous les répondants à l'enquête qui ont ainsi permis la réalisation de cette étude.

Retrouvez les conférences CIO sur notre site web :
http://www.cio-online.com/conferences/

SOMMAIRE

1.INTRODUCTION

1.1 Pourquoi cette étape ?

Criminalité, catastrophes naturelles, problèmes géopolitiques, retournement du marché, fournisseur défaillant, etc. L'entreprise est par nature plongée en permanence dans les risques. Mais elle doit se doter des méthodes et des outils pour les gérer. Le DSI a un rôle essentiel à tenir, au service de l'entreprise dans sa globalité, en délivrant le système adéquat.

Le DSI est également au coeur du risque car le système d'information est en lui-même facteur de risques. Devenu vital au fonctionnement de l'entreprise, le système d'information ne peut plus connaître de défaillance sans conséquences graves. Ce risque là aussi doit être anticipé et géré.

Un projet qui peut échouer et priver une entreprise d'une réponse à sa concurrence est une source de risque. Un système dont l'exploitation peut être défaillante est une source de risque. L'entreprise peut être elle-même responsable mais elle peut aussi être victime d'un manquement d'un fournisseur. Et les cybercriminels sont toujours en embuscade derrière la moindre faiblesse. Si les outils de sécurité ne doivent pas être la totalité de la réponse, ils en sont une nécessaire partie.

L'externalisation, notamment dans le Cloud, souvent dans des pays problématiques juridiquement (comme les Etats-Unis) ou géopolitiquement (pays classiques d'off-shore), a été adoptée parfois avec légèreté par les DSI. Les risques, là aussi, doivent être connus et maîtrisés.

Enfin, les collaborateurs sont devenus des sources de risques de plus en plus importantes. Utilisateurs d'outils de moins en moins maîtrisés, du smartphone au réseau social, ils peuvent faire peser de réelles menaces sur les intérêts de l'entreprise. Les terminaux mobiles, peu ou pas protégés contre les cybermenaces, sont devenus des sources de risques en même temps que des opportunités importantes de création de valeur.

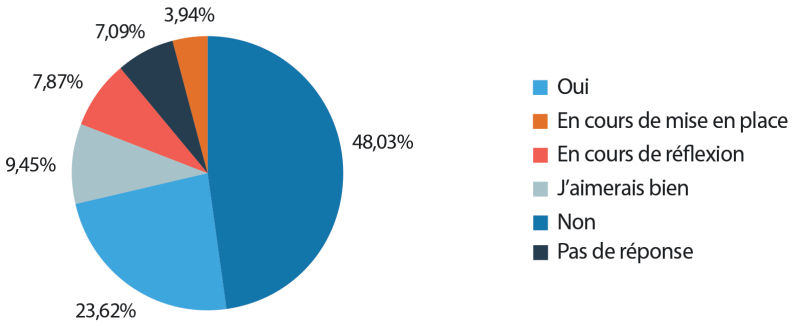
En prélude à la Matinée Stratégique « Maîtriser le risque à l'heure des menaces complexes », CIO a voulu connaître la situation réelle dans les entreprises. C'est là l'objectif de cette étude.

1.2 Qui à répondu à l'enquête de CIO ?

La présente étude est basée sur une enquête réalisée en ligne du 18 mars au 12 mai 2014.
127 entreprises y ont répondu.

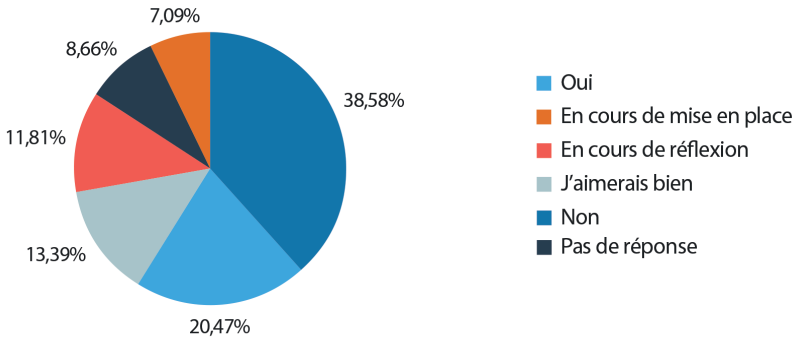
2. QUI POUR GÉRER LES RISQUES DE L'ENTREPRISE ?

2.1 Votre entreprise possède-t-elle une direction du risque autonome ?



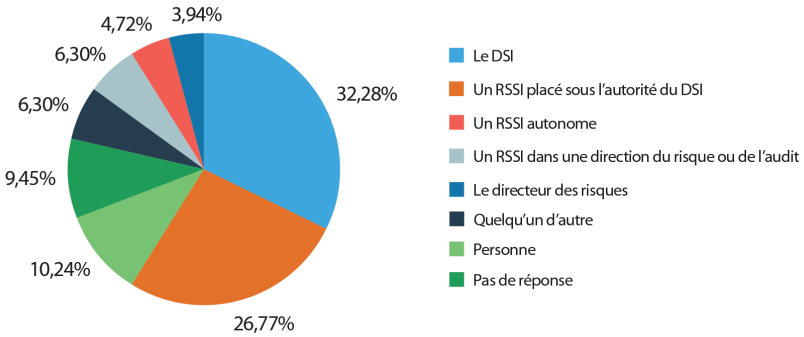
L'existence même d'une direction du risque n'est visiblement pas jugée comme nécessaire par une courte majorité d'organisations. Et moins d'un quart en dispose d'une. Or cette direction du risque, autonome de toutes les autres directions à commencer par une indépendance de la DSI, est seule capable d'être une vraie force de contrôle et de proposition. Indépendante, elle peut agir sans à avoir à se soumettre à un diktat hiérarchique d'une direction ayant d'autres priorités budgétaires.

2.2 Les risques en termes d'Intelligence économique (réputation, espionnage...) sont-ils traités spécifiquement ?



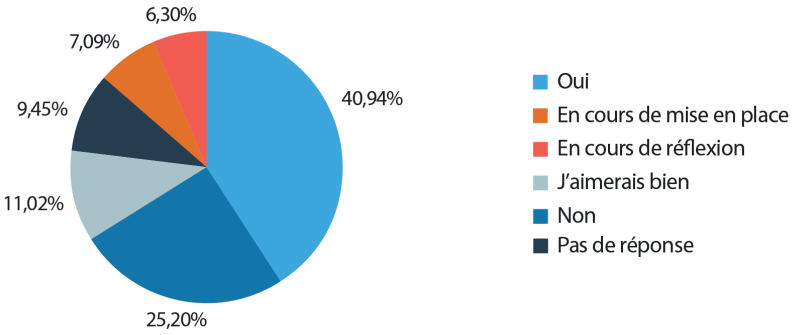
L'Intelligence Economique reste largement négligée : un cinquième seulement des entreprises s'en préoccupe effectivement. Là encore, le coût d'une gestion de tels risques n'est certes pas nul mais les dangers pour l'entreprise qui peuvent être évités sont considérables. L'intelligence économique consiste en effet à compiler et analyser toutes les informations relatives d'une part à l'entreprise d'autre part à ses concurrentes et partenaires. Une telle veille évite les attaques contre, par exemple, la réputation de l'entreprise et permet, à l'inverse, de se saisir d'opportunités en lien avec des faiblesses de ses concurrents.

2.3 Qui est responsable des risques IT ?



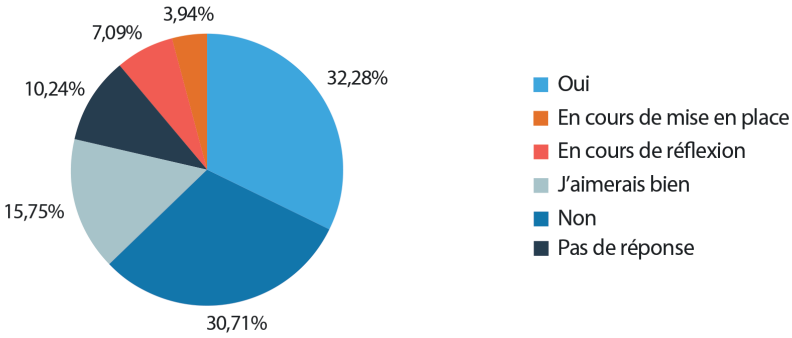
La responsabilité des risques IT incombe encore directement à la DSI, soit au DSI lui-même soit à un RSSI qui lui est soumis hiérarchiquement. Le RSSI autonome ou rattaché à un directeur des risques reste une configuration marginale. Or, comme avec la Direction du Risque, l'existence d'un lien hiérarchique interdit un véritable contrôle. Si un arbitrage doit être rendu entre les budgets et la sécurité, gageons que la sécurité ne sera pas gagnante.

2.4 Y a-t-il des audits réguliers par un extérieur à la DSI de la sécurité du SI ?



Heureusement, il existe tout de même une forme de contrôle extérieur de la sécurité du SI via des audits. Ces audits peuvent, dans une certaine mesure, apporter cette indispensable vision externe. Encore faut-il qu'ils soient bien analysés par des décideurs d'un niveau au moins équivalent au DSI et au DAF pour que les arbitrages, notamment budgétaires, soient rendus en tenant compte d'une vision à long terme.

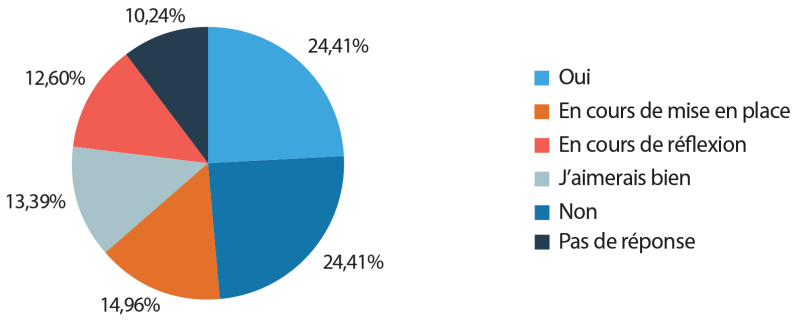
2.5 Y a-t-il des audits réguliers par un extérieur à la DSI des risques IT ?



Mais le contrôle de l'ensemble des risques -au delà du seul problème de la sécurité au sens strict- est, lui, nettement moins fréquent. Or les risques IT sont bien au delà des seules tentatives d'intrusion par un cybercriminel. L'informatique est devenue trop importante dans l'ensemble des processus de l'entreprise pour que toutes les causes d'un éventuel arrêt d'exploitation ne soient pas clairement analysées. Ces risques concernent les fournisseurs, les partenaires, la législation des pays où l'entreprise est implantée, les catastrophes naturelles, etc.

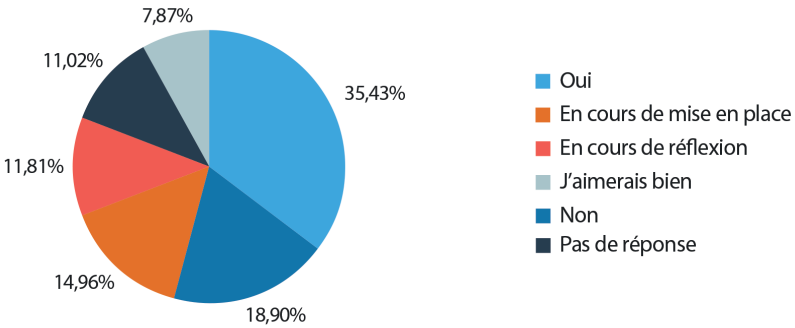
3. L'APPRÉHENSION DES NATURES DE RISQUES

3.1 Les actions des utilisateurs à pouvoir (administrateurs, développeurs, consultants...) sont-elles surveillées ou tracées spécifiquement ?



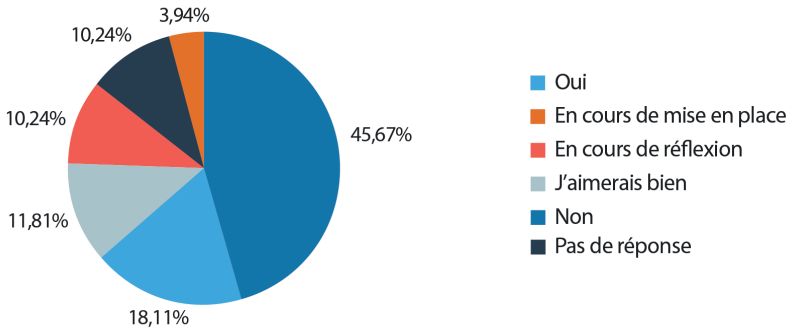
Les utilisateurs à pouvoir restent peu surveillés. Autrement dit, un « admin » demeure potentiellement une source importante de danger, y compris s'il est extérieur à l'entreprise (un ingénieur de SSII par exemple). Ce danger peut être lié à un acte délibéré ou bien à une erreur. Or une erreur peut être très coûteuse et entraîner la responsabilité civile du prestataire, pourvu qu'on puisse prouver son implication. Tracer est donc préventif, notamment pour dissuader les actes volontaires, mais aussi réactif pour obtenir réparation d'un préjudice accidentel.

3.2 Analysez-vous les logs des connexions réseau ou des connexions aux applications pour repérer les anomalies ?



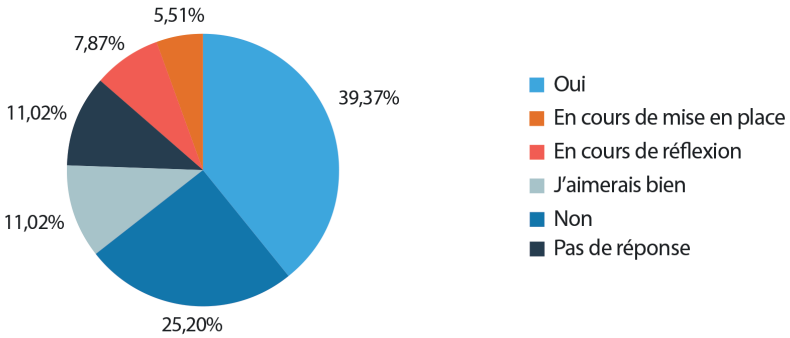
Un peu plus d'un tiers des organisations seulement analyse pour l'heure les logs de connexion pour vérifier l'existence d'une anomalie. Or seule une telle analyse peut démontrer l'existence d'une attaque comme de dysfonctionnements. A l'heure d'attaques de plus en plus sophistiquées, une telle analyse est souvent la seule manière de détecter qu'une faille a bien été exploitée.

3.3 Auditez-vous ou faites-vous auditer vos fournisseurs d'hébergement ou de solutions cloud (SaaS/PaaS/IaaS) ?



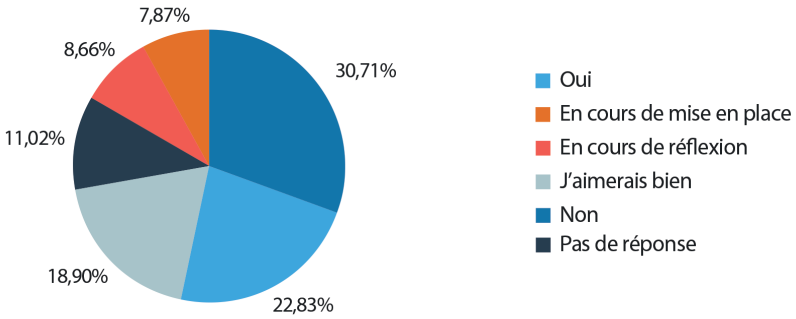
Plus grave peut-être, les prestataires de cloud sont audités de manière marginale. Les organisations acceptent donc majoritairement de confier à des tiers une partie de leur système d'information sans aucune forme de contrôle.
En rapprochant cette question des précédentes, on s'aperçoit que plus quelqu'un a du pouvoir sur le système d'information moins il est contrôlé. Ce paradoxe est une véritable menace contre l'entreprise.

3.4 Surveillez-vous votre réputation sur Internet, notamment les réseaux sociaux ?



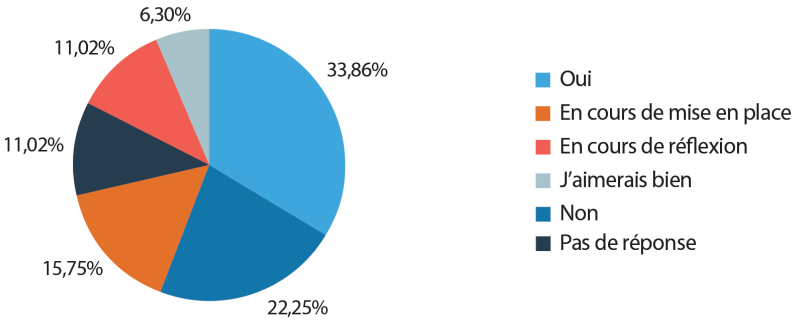
Si les « admins » ou les hébergeurs sont peu contrôlés, les réseaux sociaux sont, eux, davantage surveillés. L'impact marketing (et donc sur le chiffre d'affaires) d'un incident est ici clairement compris. Les entreprises, on le voit ici nettement, se préoccupent donc et investissent volontairement sur la réaction à des risques aux conséquences visibles immédiatement par le marketing ou les ventes.

3.5 Disposez-vous de garanties réelles (au delà des clauses contractuelles) face à une défaillance ou une faute de l'un de vos fournisseurs ?



Obtenir des garanties semble visiblement peu dans les mœurs des DSI. Le contrat reste l'arme classique. Si le coupable disparaît, l'entreprise n'a plus pourtant aucun recours. Lui réclamer des dommages et intérêts ne sert dès lors plus à rien. Apparemment, disposer de garanties réelles comme des clauses contractuelles de back-up obligatoire chez un tiers, est dès lors une nécessité.

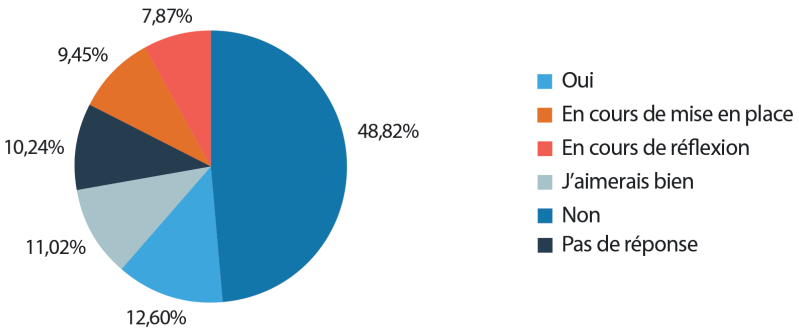
3.6 Avez-vous testé votre PCA (Plan de continuité d'activité) ou votre PRA (Plan de reprise d'activité) ?



Encore une fois, la confiance aveugle des DSI dans leurs procédures et leurs fournisseurs semble les pousser à ne pas vérifier que tout fonctionne correctement. Certes, tester un PCA/PRA est une manœuvre complexe et avec un coût non-nul. Mais la vérification de la pertinence des procédures est pourtant nécessaire. Comment, sinon, être absolument certain qu'aucune perte de fonctionnalité ou de donnée ne sera à déplorer en cas d'incident ?

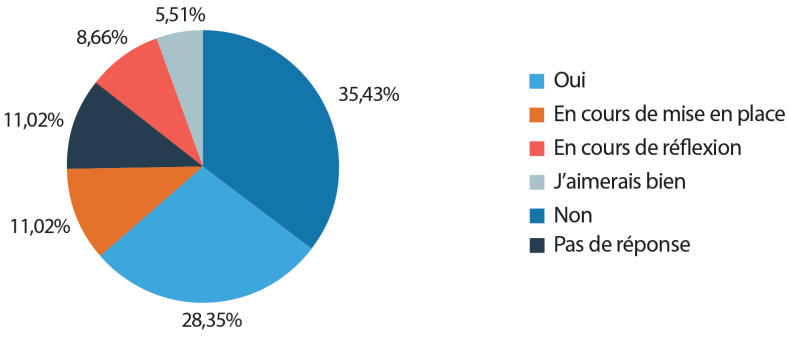
4. OUTILS ET MÉTHODES POUR GÉRER LES RISQUES

4.1 Disposez-vous d'un système de gestion des risques (SIGR) ?



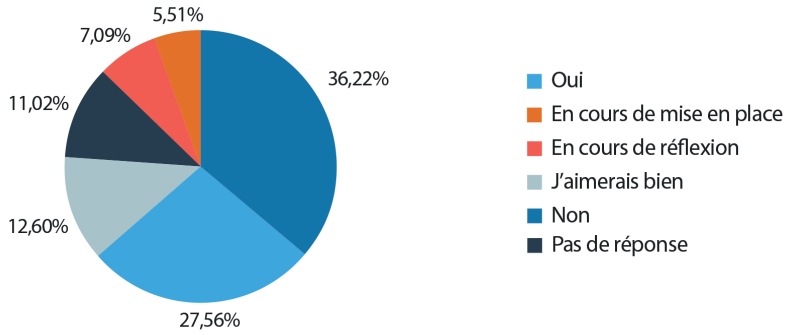
Dans leur immense majorité, les entreprises ne sont pas équipées et n'envisagent pas de s'équiper d'un progiciel de gestion des risques. Cette gestion des risques est donc condamnée à rester très artisanale. Or un suivi précis des risques, des assurances et des modalités concrètes de réponses est nécessaire à leur saine gestion. En fonction des risques précis encourus dans l'entreprise, il convient de se doter d'un outil approprié. L'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) publie annuellement un panorama des outils avec leur couverture fonctionnelle.

4.2 Avez-vous adopté un référentiel normalisé de bonnes pratiques ou une norme pour gérer vos risques (eBios, ISO 27000...) ?



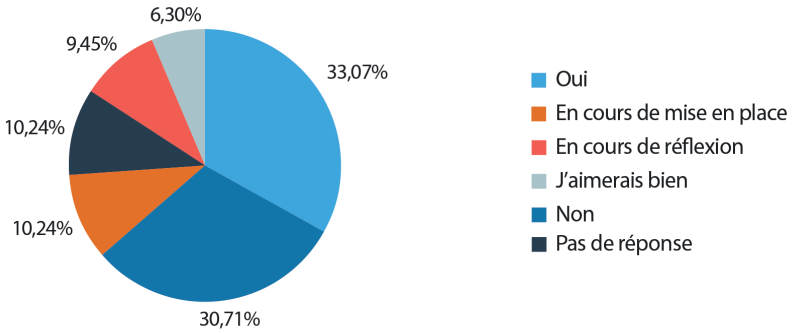
Le côté artisanal de la gestion des risques est confirmé par les réponses à cette question ! Les référentiels et les normes associés à la gestion des risques demeurent marginaux. Si la certification demeure un processus long et coûteux, elle n'est pas forcément nécessaire. Malgré tout, adopter, éventuellement partiellement, un référentiel de bonnes pratiques ou une norme permet de guider les actions à entreprendre.

4.3 Suivez-vous les ateliers d'un club dédié à la sécurité ou aux risques (CLUSIF, CESIN, AMRAE...) ?



Au delà des seuls référentiels, les partages avec les pairs au sein d'un club ne séduit guère les répondants. Or de tels échanges permettent d'enrichir sa propre réflexion, d'éviter de refaire les erreurs déjà commises par d'autres et de réinventer l'eau chaude.

4.4 Disposez-vous d'une gestion des identités et des droits d'accès reliée automatiquement aux entrées/sorties de personnels ?



Un petit tiers des entreprises gère de manière convenable les droits d'accès au système d'information avec une mise à jour automatique en fonction des évolutions du personnel. La part de la gestion manuelle demeure donc très importante, malgré les coûts et les lenteurs associés. Or un retard de prise en compte à l'entrée implique une perte de productivité pour le salarié concerné ; un retard à la sortie implique une faille de sécurité en faveur d'une personne qui pourrait avoir du ressentiment envers l'entreprise.

5. CONCLUSION

Malgré tous les incidents connus et des affaires ayant défrayé la chronique comme le cas Snowden, la sécurité reste un parent pauvre dans l'entreprise, en particulier la sécurité informatique conçue au sens large. Il ne s'agit pas seulement d'empêcher des piratages mais aussi de tenir compte de tous les types d'incidents possibles.

Or l'enquête démontre que les organisations sont très immatures envers ces sujets.

La surveillance des réseaux sociaux est ainsi mieux faite que celle du réseau interne de l'entreprise. Et le recours massif au Cloud Computing s'effectue là encore sans contrôle.

La sécurité coûte cher, il est vrai. Le calcul d'un retour sur investissement est complexe. Il en résulte qu'un problème sur les réseaux sociaux, qui a un impact direct sur le chiffre d'affaires, sera mieux détecté et analysé que du piratage du réseau interne de l'entreprise alors que le préjudice potentiel, dans ce dernier cas, est bien plus grand.

Mais qui pourrait alerter le DSI ou la DG ? Les responsables de la sécurité sont rarement indépendants. Ils ne peuvent donc pas alerter quelqu'un d'autre que celui qui est la cause des manquements aux bonnes pratiques. Ces manquements peuvent être, il est vrai, dus à des arbitrages budgétaires à courte vue que seule une DG pourrait remettre en cause, alertée par un cadre dirigeant indépendant des autres directions, notamment de la DSI.

6. A PROPOS DE CIO-ONLINE

CIO France est une plate-forme multi-format de contenus et de services dédiée aux Directeurs de Systèmes d'Information (DSI ou CIO, Chief Information Officer) de grandes entreprises.
Le site web CIO-Online.com est associé à la revue sur abonnement CIO.PDF et aux événements tels que les Matinées Stratégiques.

CIO France est édité par IT News Info et est partenaire de CIO.com, un service du groupe IDG.

Site web :
www.cio-online.com

7. A PROPOS DE IT NEWS INFO

IT News Info, c'est 4 marques médias : LeMondeInformatique.fr, Cio-Online.com, Reseaux-Telecoms.net, Distributique.com ainsi qu'un pôle conférences avec près de 30 événements par an organisés pour les décideurs et managers IT.

IT News Info est une filiale des groupes IDG (International Data Group) et Adthink Média.
C'est le 1er groupe d'information et de services dédiés aux professionnels de l'informatique en France. En 2013, IT News Info est la plus forte audience auprès des informaticiens professionnels en France.

Site web :
www.cio-online.com
www.lemondeinformatique.fr
www.distributique.com
www.reseaux-telecoms.net

8. CONTACTEZ-NOUS

Pour toute information complémentaire :

Georges Pinheiro - Directeur commercial
+33(0) 1 41 97 62 16
gpinheiro@it-news-info.com

Bertrand Lemaire - Rédacteur en chef
+33(0) 1 41 97 62 10
blemaire@it-news-info.com