



#### Contact Symantec France

Irène Godeau

Tel : 01.41.38.59.39

[irene\\_godeau@symantec.com](mailto:irene_godeau@symantec.com)

#### Contacts PLEON

Hélène Pereira – Henry de Romans

Tel : 01 53 04 23 46 – 01 53 04 23 71

[helene.pereira@pleon.com](mailto:helene.pereira@pleon.com) [henry.deromans@pleon.com](mailto:henry.deromans@pleon.com)

### **IT PCG Research révèle un important potentiel d'économie pour la sécurité et l'audit informatiques**

*A budget sécurité identique, les entreprises aux plus mauvaises pratiques sont confrontées à des coûts de pertes de données jusqu'à 149 fois supérieurs à ceux des entreprises s'appuyant sur les meilleures pratiques*

**PARIS, France - 05 mars 2009** - IT PCG (IT Policy Compliance Group) a annoncé aujourd'hui la disponibilité de sa dernière étude de marché intitulée "Risk-based Performance Budgeting for Information Security and Audit in IT" (Budgéter la sécurité et l'audit informatique en fonction de la performance face aux risques). S'appuyant sur une enquête réalisée auprès de plus de 2600 sociétés, l'étude indique que **68% des entreprises sous-investissent en sécurité informatique** par rapport aux risques et pertes financières qu'elles subissent. Pourtant, l'augmentation des budgets nécessaires à la mise en place des meilleures pratiques peut se traduire par **un retour sur investissement de 200% à plus de 100 000%** pour l'entreprise moyenne.

Cette nouvelle étude, commanditée par le Computer Security Institute, l'Institute of Internal Auditors, Protiviti, ISACA, l'IT Governance Institute, et Symantec Corp. (Nasdaq : SYMC) revient sur :

- une approche budgétaire basée sur les risques en matière de sécurité informatique et qui fournit des résultats ;
- les pratiques associées à l'utilisation de l'informatique qui impactent la conduite des affaires et les risques financiers ;
- et les réductions substantielles de dépenses d'audit en informatique.

*"Comme pour une prime d'assurance, toutes les entreprises sont prêtes à accepter un certain niveau de perte financière ou de vol de données client ou même à faire face à une certaine perte de chiffre d'affaires du fait de problèmes informatiques," déclare Jim Hurley, Directeur général d'IT PCG et l'un des principaux directeurs de recherche chez Symantec. "Cependant, l'enquête démontre que la tolérance aux pertes d'une organisation est extrêmement faible, et que le retour financier d'améliorations mineures peut être formidablement élevé."*

## Principaux risques pour les entreprises

Les entreprises identifient principalement **trois risques informatiques majeurs** : la confidentialité des données sensibles ; l'intégrité des données, des équipements et des contrôles informatiques ; et la disponibilité des services informatiques.

Le rapport d'IT PCG s'appuie sur les évaluations en cours pour mesurer les performances des entreprises par rapport à ces trois domaines de risque.

Les résultats de l'enquête sont les suivants :

- Résultats les plus mauvais : **19% des entreprises** connaissent **plus de 15 pertes ou vols de données par an**, 80 heures d'arrêt d'activité ou plus à cause de pannes informatiques, et plus de 15 déficiences ayant échappé aux audits
- Résultats moyens : **68% des entreprises** fonctionnent à des niveaux "normaux", avec **entre 3 et 15 pertes ou vols de données par an**, entre 7 et 79 heures d'arrêt d'activité à cause de pannes informatiques, et entre 3 et 15 déficiences ayant échappé aux audits
- Meilleurs résultats : **13% des entreprises** obtiennent les meilleurs résultats, avec **moins de 3 pertes ou vols de données par an**, moins de 7 heures d'arrêt d'activité à cause de pannes informatiques, et moins de 3 déficiences ayant échappé aux audits Les retours financiers dans ces entreprises vont de 22%, à plus de 3000% par an.

Étonnamment, la différence de résultats entre les plus mauvais et les meilleurs ne correspond pas au montant des budgets alloués à la sécurité. En effet, il apparaît que le montant des budgets de sécurité est négligeable, le plus déterminant étant l'utilisation qui est faite de ces mêmes budgets.

## Implications financières

Les implications financières de ces risques s'avèrent correspondre presque parfaitement aux pratiques mises en oeuvre par les directions informatiques pour contrôler l'exposition aux risques. Comme on pouvait s'y attendre, **les sociétés s'appuyant sur les meilleures pratiques ont subi les pertes financières les plus faibles** et les moins fréquentes. **Les sociétés les moins performantes** ont payé au prix fort, littéralement, **avec des pertes et des vols de données pouvant atteindre 9.6% de leur chiffre d'affaires**, et des pertes d'activité du fait de pannes approchant 3% de leur chiffre d'affaires.

Parmi les entreprises réalisant plus de 5 milliards de dollars de chiffre d'affaires, le coût global des pertes et vols de données, et des pertes d'activité varie entre 329 millions de dollars, pour les sociétés ayant les plus mauvaises pratiques, à 2.25 millions de dollars pour celles ayant mis en oeuvre les meilleures pratiques, soit 149 fois moins.

L'enquête montre que les sociétés obtenant les meilleurs résultats dépensent en fait entre 35% et 52% de moins en frais et dépenses d'audit. Pour ces sociétés, l'argent dépensé en pratiques réduisant les risques, les pertes et les dépenses d'audit, a produit un retour financier 1000% à 500.000% supérieur aux pertes que ces entreprises étaient prêtes à supporter.

## **Réduction des risques et des coûts**

*"Les entreprises peuvent, soit attendre qu'une urgence les pousse à fixer de nouvelles priorités, soit décider qu'il est plus intéressant de mettre en oeuvre les pratiques éprouvées par le marché,"* déclare M. Hurley.

Le nouveau rapport détaille les cinq pratiques suivantes, sur lesquelles s'appuient ceux ayant les meilleurs résultats et les moindres pertes financières :

1. S'appuyer sur une équipe de direction senior pour gérer le risque
2. Classer les risques par priorité, améliorer les contrôles, et automatiser les procédures
3. Evaluer en continu les contrôles et les risques
4. S'appuyer sur des contrôles techniques, des politiques, et une gestion du changement informatique
5. Mettre en oeuvre un reporting complet

## **Quelques citations de membres d'ITPCG ...**

*"Ce rapport montre clairement les avantages que les entreprises peuvent tirer d'une bonne gestion de la sécurité, de la disponibilité et d'autres risques liés à l'informatique,"* a déclaré Brian Barnier, membre de la Risk IT Task Force, de l'IT Governance Institute. *"Les bonnes pratiques telles que celles présentées dans le schéma COBIT, téléchargeable gratuitement, peuvent aider les organismes à prendre des mesures spécifiques pour atténuer les risques et maximiser la valeur. »*

## **A propos de l'enquête**

Les sujets étudiés par les benchmarks de l'IT Policy Compliance Group font partie d'un calendrier de recherche, établi à partir d'éléments fournis par les membres actifs, par des membres consultatifs, et par des résultats de recherches récentes. Les benchmarks les plus récents inclus dans ce rapport ont été réalisés entre septembre et décembre 2008, auprès de 734 entreprises concernées. Les 734 entreprises ayant participé aux benchmarks les plus récents sont toutes installées en Amérique du Nord, avec une majorité (95%) aux Etats-Unis. La majorité (90%) des plus de 2600 adhérentes sont aux Etats-Unis. Les 10% restant viennent d'Europe, d'Amérique latine, du Moyen-Orient, d'Asie ou de pays de la côte Pacifique.

## **A propos de l'IT Policy Compliance Group**

L'IT Policy Compliance Group a vocation à promouvoir le développement de la recherche et de l'information susceptibles d'aider les entreprises à se conformer à leurs objectifs et à la législation en vigueur. Le groupe s'efforce d'aider ses entreprises membres à améliorer leur activité, leur gouvernance, leur gestion du risque et leur niveau de conformité sur la base de benchmarks factuels. L'IT Policy Compliance Group est soutenu par plusieurs grandes organisations parmi lesquelles : le Computer Security Institute (Institut de sécurité informatique), l'Institute of Internal Auditors (institut des experts comptables), Protiviti, ISACA, l'IT Governance Institute (Institut de gouvernance informatique), et Symantec Corporation (NASDAQ : SYMC). Plus d'information est disponible sur [www.ITPolicyCompliance.com](http://www.ITPolicyCompliance.com).

## **A propos de Symantec**

Symantec est leader mondial des solutions de sécurité, de stockage et de gestion des systèmes pour aider les particuliers et les entreprises à sécuriser et gérer leur environnement informatique. Les logiciels et les services de Symantec protègent plus largement et plus efficacement contre davantage de risques, en davantage de points. Ils renforcent le niveau de confiance des utilisateurs partout où leurs données sont utilisées ou stockées.

Pour plus d'informations, rendez-vous sur [www.symantec.com](http://www.symantec.com)