Communiqués de presse

# Etude IBM : Les Responsables de la sécurité des systèmes d'information prennent une place stratégique au sein des organisations mondiales

**Trois-quarts des décideurs en matière de sécurité ont déployé des services de sécurité en mode cloud ; les technologies de sécurité déployées le plus récemment sont celles qui concernent la mobilité**

**Paris - 25 oct. 2013:** Une nouvelle étude IBM concernant les responsables de la sécurité des systèmes d'information révèle qu'ils sont de plus en plus sollicités pour répondre aux préoccupations de la direction générale en matière de sécurité. De fait, leur place est devenue stratégique au sein de leurs organisations.

Les résultats de l'étude montrent que face aux technologies émergentes, aux restrictions budgétaires et à un paysage des menaces qui évolue sans cesse, les RSSI doit jouer un rôle plus actif dans la communication avec les métiers et la direction générale, étant donné que l'augmentation des incidents de sécurité impacte la réputation de la marque et la confiance des clients. En outre, l'adoption du cloud et de la mobilité continuent à demeurer des enjeux prioritaires pour la majorité des RSSI.

L'étude « *2013 IBM Chief Information Security Officer Assessment » (Evaluation IBM 2013 du RSSI)*, se penche sur ce que prévoient les responsables de la sécurité des systèmes d'information des entreprises du Fortune 100 et de taille moyenne. En voici quelques résultats :

- ***Les tendances technologiques – aller au-delà des fondamentaux :*** parmi les initiatives déployées le plus récemment, la principale est celle qui vise la sécurisation de la mobilité, un-quart des RSSI interrogés l'ayant déployée dans les 12 derniers mois. Le premier enjeu en matière de mobilité pour les RSSI est de dépasser l'étape initiale qui consiste à déployer les technologies et de penser plus à la mobilité en termes de politique et de stratégie. Moins de 40% des organisations ont mis en œuvre des politiques spécifiques pour les terminaux étant la propriété personnelle des employés ou encore une stratégie d'entreprise pour le « bring-your-own-device » (BYOD).

Près de 76% des RSSI ont déployé un certain nombre de service de sécurité dans le cloud – les plus répandus étant la supervision de données et les audits ainsi que les solutions de gestion et de fédération des identités et des accès (les 2 à 39%). Alors que le cloud et la mobilité continuent à faire l'objet d'une attention particulière au sein des entreprises, les RSSI mettent un accent particulier sur les technologies « fondamentales » telles que la gestion des identités et des accès (51%), la prévention des intrusions réseau et les scans de vulnérabilité (39%) et la sécurité des bases de données (32%).

- ***Les* pratiques métier – comprendre la vision** : Les RSSI interviewés souligne le besoin d'avoir une très bonne vision métier, une bonne compréhension de la stratégie et de la politique d'entreprise et une gestion des risques compréhensible en associant les métiers. Bien appréhender les préoccupations des dirigeants de l'entreprise est également critique pour la réussite du RSSI. Les plus expérimentés parmi ces derniers rencontrent régulièrement la direction générale pour approfondir leur compréhension des enjeux stratégiques et renforcer les liens avec les métiers. Quand ils se réunissent, les sujets qu'ils abordent sont : l'identification et l'évaluation des risques (59%), la résolution des problématiques budgétaires (49%) et le

déploiement de nouvelles technologies (44%).

- ***L'évaluation – fournir le bon feedback*** **:** les RSSI continuent à utiliser les statistiques et des rapports essentiellement pour prendre des décisions budgétaires ou pour décider des domaines d'investissement. Dans certains cas, ils utilisent ces statistiques pour aider à établir les priorités stratégiques pour leurs organisations de sécurité. Par exemple, plus de 90% des personnes interrogées suivent régulièrement le nombre d'incidents de sécurité, les pertes ou vols de documents, données ou terminaux et le statut des audits et de la conformité – dimensions fondamentales, incontournables pour chaque RSSI. Cependant, très peu de RSSI interviewés combinent la notion des impacts métier avec les incidents de sécurité dans le processus de la gestion du risque. Ils reconnaissent néanmoins que l'impact de la sécurité sur le risque global de l'entreprise est le facteur le plus important à prendre en compte dans la définition de la stratégie et de la politique de sécurité.

"*Il est évident dans cette étude que les RSSI doivent trouver une équilibre entre la mise en œuvre d'une sécurité forte avec une vue holistique et la stratégie de gestion de risques, tout en déployant des capacités stratégiques et plus pointues – telle qu'une sécurité mobile solide, incluant une politique pour le BYOD*," a déclaré **David Jarvis, co-auteur du rapport et responsable à « l'IBM Center for Applied Insights ».**

Pour accéder à l'étude complète : http://www.ibm.com/security

**A propos d'IBM Security :**

IBM fournit l'expertise, les compétences, les services et la technologie pour aider à réduire les coûts et la complexité des systèmes d'information de ses clients. Les solutions IBM incluent le planning et le design, la mise en œuvre, les tests, la supervision et la gestion des environnements multi-vendors.

Pour plus d'informations : http://www.ibm.com/security/fr

*****

**IBM Study: Security Officers Gaining a Strategic Voice, Transforming Technology and Business in Global Organizations**

*Three-fourths of security leaders have deployed cloud security services; Mobile security most recently deployed technology*

**Armonk, N.Y. - 24 Oct 2013:** A new IBM (NYSE: IBM) study of security leaders reveals that they are increasingly being called upon to address board-level security concerns and as a result are becoming a more strategic voice within their organizations.

The findings reveal that a constantly evolving threat landscape, emerging technologies and budgetary

restraints are requiring security leaders to play a more active role in communicating with C-suite leaders and with their boards, as the rise in security incidents impacts brand reputation and customer trust. Additionally, cloud and mobile adoption continues to grow as a focus area for the majority of security leaders.

The *2013 IBM Chief Information Security Officer Assessment* takes the pulse of security leaders from Fortune 100 and mid-sized businesses**.** Among the findings:

***Technology Trends -- Moving beyond the Foundational:*** Mobile security is the number one "most recently deployed" initiative, with one-quarter of those surveyed deploying it in the past 12 months. According to the findings, while security leaders are looking to advance mobile securitybeyond technology and more about policy and strategy, less than 40% of organizations have deployed specific response policies for personally owned devices or an enterprise strategy for bring-your-own-device (BYOD).

Nearly 76% of security leaders interviewed have deployed some type of cloud security services – the most popular being data monitoring and audit, along with federated identity and access management (both at 39 percent). While cloud and mobile continue to receive a lot of attention within many organizations, foundational technologies that security leaders are focusing on include identity and access management (51%), network intrusion prevention and vulnerability scanning (39%) and database security (32%).

***Business practices -- Catching the Vision:*** The security leaders interviewed stress the need forstrong business vision, strategy and policies, comprehensive risk management, and effective business relations to be impactful in their roles. Understanding the concerns of the C-suite is also critical as more seasoned security leaders meet regularly with their board and C-suite leaders. The top trends that they discuss include identifying and assessing risks (59 percent), resolving budget issues and requests (49 percent) and new technology deployments (44 percent).

When asked what advice they would give to a new security leaders, respondents recommended a strong emphasis on vision, strategy and policies, comprehensive risk management and effective business relations.

"*Building the trust of the C-suite and the board is critical to the success of a security officer*, said **Ken Kilby, Chief Information Security Officer, BB&T Corporation**, one of the largest financial services holding companies in the United States. *Beyond internal relationships, developing relationships with law enforcement, industry partners and legislators is crucial in fostering greater public and private communication and will ultimately help to reduce the total attack surface and protect an organization's data*."

***Measurement -- Providing the Right Feedback:*** Security leaders continue to use metrics mainly to guide budgeting and to make the case for new technology investments. In some cases, they use measurements to help develop strategic priorities for their security organizations. In general, however, technical and business metrics are still focused on operational issues. For example, over 90 percent of respondents track the number of security incidents, lost or stolen records, data or devices, and audit and compliance status – fundamental dimensions security leaders would be expected to track. Far fewer respondents are feeding business and security measures into their enterprise risk process even though security leaders say the impact of security on overall enterprise risk is their most important success factor.

*"It's evident in this study that security leaders need to focus on finding the delicate balance between*

*developing a strong, holistic security and risk management strategy, while implementing more advanced and strategic capabilities such as robust mobile security that includes policies for BYOD*," said **David Jarvis, co-author of the report and manager at the IBM Center for Applied Insights.**

**About the Assessment**

The IBM Center for Applied Insights, in collaboration with IBM Security Systems and IBM Security Services, conducted in-depth interviews with senior leaders who have responsibility for information security in their organizations. The goal of the interviews was to identify specific organizational practices and behaviors that could strengthen the role and influence of other security leaders. To maintain continuity, interviewees were recruited from the pool of 2012 research participants – 80 percent of those recruited were prior participants – with an emphasis on more mature security leaders. Interviewees were from a broad range of industries and four countries. Access the full study, www.ibm.com/security

**About IBM Security**

IBM provides the expertise, skills, services and technology to help you reduce the cost and complexity of securing IT infrastructures for IBM clients. IBM solutions include planning and design through implementation, testing, monitoring and management of multi-vendor environments.

For more information on IBM, visit www.ibm.com/security or to join the conversation and follow @IBMSecurity on Twitter. Visit our Security Intelligence Blog at www.securityintelligence.com

Hear from security leaders on how the role of the CISO is evolving from technical leader to a strategic business leader at

**http://www.youtube.com/watch?v=JnxMsSpZoo8**