

La crise économique expose plus fortement les grandes institutions financières mondiales aux risques liés aux systèmes d'information, révèle l'enquête de Deloitte

Neuilly-sur-Seine, le 19 février 2009 – La crise économique mondiale contribue à augmenter les risques pesant sur les systèmes d'information des institutions financières. Selon la dernière enquête sur la sécurité publiée aujourd'hui par le *Global Financial Services Industry* – GFSI^[1] de Deloitte Touche Tohmatsu (DTT), les attaques exploitant l'erreur humaine ainsi que les failles opérationnelles ou techniques créées par des employés soumis à une trop forte pression, insuffisamment sensibilisés ou mécontents, seront la cause première des atteintes à la sécurité des informations dans les mois à venir.

La majorité (86%) des responsables interrogés dans cette sixième édition de l'Enquête Mondiale sur la sécurité confirme que l'erreur humaine est la principale cause des dysfonctionnements des systèmes d'information, constatant ainsi que, bien que le collaborateur soit l'actif le plus précieux d'une entreprise, il est aussi son maillon le plus faible, particulièrement dans un climat économique difficile, caractérisé par une insécurité de l'emploi et un niveau de stress élevé conduisant parfois à des comportements préjudiciables à l'institution.

Bien que le nombre des atteintes à la sécurité ait diminué au cours des 12 derniers mois, les comportements inappropriés d'employés sont une préoccupation croissante des entreprises. Plus d'un tiers (36%) des personnes interrogées ont exprimé leur inquiétude sur les attaques de l'intérieur, alors que seulement 13% s'inquiètent des attaques de l'extérieur. De plus, 6 personnes interrogées sur 10 (59%) se disent « pas très » ou « seulement un peu » confiantes dans leur capacité à protéger leur entreprise contre des cyber-attaques internes.

La popularité grandissante des réseaux sociaux et la prolifération des supports mobiles tels que les clefs USB, les lecteurs MP3 et les PDA sont autant de menaces supplémentaires à la sécurité interne et externe. Il est intéressant de noter que plus de la moitié des institutions financières interrogées restreignent désormais l'usage des réseaux sociaux (53%) et de la messagerie instantanée (58%), alors que plus de 90% d'entre elles autorisent leurs employés à utiliser des supports mobiles. Ceux-ci contribuent sans doute à l'augmentation de la productivité, mais présentent aussi des risques de chargement et de stockage non-autorisés d'informations confidentielles sur des supports éventuellement non-protégés, créant ainsi un environnement favorable à la fuite ou la perte de données. Il est alarmant de constater que seulement 55% des prestataires de services financiers interrogés ont étendu le chiffrement à l'ensemble de leur entreprise et que moins d'un tiers (28%) d'entre eux ont chiffré leurs bases de données ou se sont dotés d'outils de détection d'intrusion interne ou de fuites d'informations (« Data leakage »). Il est par contre rassurant de noter que 32% des personnes interrogées ont l'intention de déployer de tels outils dans les 12 prochains mois.

[1] www.deloitte.com

Le *phishing* et le *pharming*^[2] sont cités par 46% des personnes interrogées comme l'une des menaces les plus préoccupantes et classés par 22% d'entre elles comme étant la première cause d'atteintes à la sécurité.

« Les institutions financières doivent se battre sur deux fronts dans leur lutte pour la protection des données personnelles de leurs clients » déclare François Renault, Associé Deloitte France. *« D'un côté, elles se trouvent face à une sophistication toujours plus grande des attaques et à l'accroissement de l'ampleur et de la fréquence des pertes de données et des vols d'informations relatives aux clients et, de l'autre, à des obligations réglementaires toujours plus contraignantes, dans une conjoncture économique difficile.»*

Les programmes de réduction des coûts imposés par la conjoncture économique accentuent la nécessité d'une vigilance accrue du management pour ne pas détériorer le niveau de sécurité. Bien que 60% des personnes interrogées confirment une augmentation de leur budget, celle-ci n'est pas à la hauteur des enjeux et des besoins actuels en matière de sécurité. Plus de la moitié (56%) des personnes interrogées précisent que les contraintes budgétaires et/ou le manque de ressources sont les deux premières entraves à la sécurité de l'information et, pour 33% d'entre elles, le « manque de ressources » est identifié comme étant la première cause d'échec des projets de sécurité de l'information. De plus, un nombre croissant de personnes interrogées (15% contre 13% en 2007) reconnaît que les investissements dans la sécurité de l'information prennent du retard.

« Plus les effets de la crise financière se feront sentir, plus les entreprises seront tentées de réduire leurs budgets informatiques ainsi que leurs dépenses en infrastructures de sécurité », souligne Rédouane Bellefqih, Associé Deloitte France. *« Mais, aussi tentant que cela puisse être, économiser sur les budgets de sécurité de l'information s'avère déraisonnable. Si l'entreprise baisse sa garde, des individus malintentionnés en profiteront pour exploiter les failles résultant de ces mesures « d'économie ».*

Résultats complémentaires de l'enquête :

- Les trois premières priorités des institutions financières en matière de sécurité sont la conformité réglementaire et, ex aequo en deuxième position, la gestion des accès et des identités et la protection des données afin d'éviter les fuites d'informations.
- En 2008, les institutions financières ont vu diminuer le nombre d'attaques d'origine externe (47% contre 65% en 2007) et interne (27% contre 30% en 2007).
- Les principales motivations des institutions financières à protéger la confidentialité de leurs clients sont les obligations réglementaires en matière de confidentialité (79%) et la protection de leur réputation et de leur marque (70%).

Résultats par zones géographiques

Europe, Moyen-Orient et Afrique (EMEA) : les personnes interrogées dans la zone EMEA représentent le plus fort pourcentage à estimer qu'elles possèdent les compétences nécessaires pour remplir leurs obligations présentes et futures en matière de sécurité (41%). Pourtant, la moitié des institutions financières interrogées dans cette zone (49%) a

subi des attaques répétées de l'extérieur en 2008 et seuls deux tiers (64%) d'entre elles (en avant-dernière position dans le monde) confirment avoir fait suivre à leurs employés au moins une session de formation sur la sécurité des données en 2008. De plus, un peu plus de la moitié (56%) des personnes interrogées dans cette zone estime qu'elle a la motivation et le financement organisationnels nécessaires pour remplir ses obligations réglementaires.

Asie-Pacifique hors Japon : bien qu'en progrès sous certains aspects de la sécurité des informations, les institutions financières de la zone Asie-Pacifique ont subi le plus fort pourcentage d'attaques répétées de l'extérieur (58%) et de l'intérieur (33%) comparé à leurs homologues dans le monde. Seules 58% d'entre elles ont fait suivre à leurs employés une formation sur la sécurité des informations l'année dernière, beaucoup moins que la moyenne mondiale de 72%. Il est donc logique que seule 1 personne interrogée sur 4 (23%) dans la zone Asie-Pacifique estime avoir les compétences nécessaires pour remplir ses obligations présentes et prévisibles en matière de sécurité. Un fait est à signaler dans cette zone : elle a le plus fort pourcentage de personnes interrogées (69%) estimant avoir la motivation et le financement nécessaires pour remplir ses obligations réglementaires.

Japon : les institutions financières japonaises sont presque un monde à part en matière de sécurité des informations. En 2008, elles ont non seulement connu le pourcentage le plus faible d'attaques répétées de l'intérieur et de l'extérieur de toutes les zones du monde (17%), mais elles devancent également leurs homologues dans quatre domaines et notamment dans la formation de leurs employés (assurée par 90% des institutions financières sondées), en ayant nommé l'un de leurs dirigeants responsable de la confidentialité (85%) et en s'étant dotées d'un programme de gestion de la confidentialité et de la conformité (84%). Par contre, il semble que les contraintes budgétaires puissent devenir le principal enjeu de la zone. Seulement 1 institution financière sur 4 (25% contre 60% pour l'ensemble du monde) a augmenté son budget de sécurité des informations et peu nombreuses sont les personnes interrogées (5% contre 43% pour l'ensemble du monde) indiquant que leurs dépenses en sécurité des informations « suivent » ou « sont en avance sur leurs plans ».

Amérique du Nord (Canada et Etats-Unis) : il semblerait que la tempête financière ait détourné l'attention des directions générales des institutions financières de la sécurité des informations. Ce phénomène est illustré par la chute spectaculaire du nombre des personnes interrogées dans cette zone estimant que la sécurité est devenue l'impératif numéro 1 de leur direction générale ou de leur conseil d'administration (de 84% en 2007, le pourcentage tombe à 63% en 2008). La zone a également le plus faible pourcentage (28%) de personnes interrogées en 2008 estimant que la sécurité de l'information est en adéquation avec les besoins des métiers. Pour ce qui est de l'aspect positif : bien que la moitié (51%) des institutions financières nord-américaines interrogées aient connu des attaques externes en 2008, c'est là une amélioration spectaculaire par rapport à 2007, année durant laquelle 78% d'entre elles avaient été victimes de ce type d'attaques. Les attaques internes sont, elles aussi, en baisse (de 44% en 2007, le pourcentage tombe à 27% en 2008), la plus forte diminution de toutes les zones.

Amérique Latine et Caraïbes : les institutions financières basées en Amérique Latine et aux Caraïbes connaissent les plus fortes améliorations de toutes les zones. En 2008, elles sont en effet leaders dans cinq catégories (devancées seulement par le Japon). Les personnes interrogées indiquent que le point fort de leur entreprise est toujours de s'être dotée d'une stratégie de sécurité définie (68%). Les trois quarts (75% contre 60% pour l'ensemble du monde) d'entre elles ont vu leur budget de sécurité augmenter et 6 sur 10 (59%) confirment que leurs dépenses en la matière « suivent » ou « sont en avance sur leurs plans ». Par contre, l'enquête révèle que les entreprises de la zone Amérique Latine et Caraïbes ont toujours des difficultés à établir des programmes de gestion de la conformité aux exigences de confidentialité et seules 24% d'entre elles ont nommé l'un de leurs dirigeants responsable de la confidentialité.

Méthodologie

Cette enquête a été menée par le *Global Financial Services Industry* – GFSI de Deloitte Touche Tohmatsu (DTT) au moyen d'entretiens et de questionnaires en ligne auprès d'un échantillon de directeurs des technologies de l'information (responsables de la sécurité des systèmes d'information, directeurs des systèmes d'information, etc.) de la plupart des 100 premières institutions financières mondiales dans les secteurs de la banque, de l'assurance, des titres et de la gestion d'actifs.

Les questions posées concernaient la gouvernance de la sécurité, les budgets, le risque informatique, l'utilisation des technologies de la sécurité, la qualité des activités opérationnelles et la protection des données personnelles. Les personnes interrogées représentaient les entreprises cotées et non-cotées de 32 pays, réparties en cinq zones : la zone Europe, Moyen-Orient et Afrique (EMEA), le Japon, la zone Asie-Pacifique, la zone Amérique du Nord et la zone Amérique Latine et Caraïbes. En raison de la diversité des activités des institutions sondées et du format qualitatif de la recherche, certains résultats peuvent ne pas totaliser 100% ou ne pas être représentatifs de chacune des zones identifiées.

A propos de Deloitte en France

Deloitte mobilise des compétences diversifiées pour répondre à l'éventail des services attendus par ses clients, de toutes tailles et de tous secteurs – des grandes entreprises multinationales aux micro-entreprises locales, en passant par les entreprises moyennes.

En France, les 6 300 collaborateurs et associés incarnent le dynamisme et la réussite de la firme par leur engagement auprès de leurs clients et leur souci permanent de garantir l'excellence des prestations qu'ils assurent. Celles-ci couvrent une palette d'offres très large : audit, conseil et risk services, juridique et fiscal, expertise comptable et corporate finance, conformément à la stratégie pluridisciplinaire de Deloitte et suivant une démarche éthique.

Pour en savoir plus, www.deloitte.fr

A propos de Deloitte dans le monde

Deloitte fournit des services professionnels dans les domaines de l'audit, de la fiscalité, du consulting et du corporate finance, à ses clients du secteur public ou privé, de toutes tailles et de toutes activités. Fort d'un réseau de firmes membres dans 140 pays, Deloitte allie des compétences de niveau international à des expertises locales pointues afin d'accompagner ses clients dans leur développement partout où ils opèrent. Nos 165 000 professionnels sont animés par un objectif commun, faire de Deloitte la référence en matière d'excellence de service.

Les collaborateurs et associés de Deloitte sont unis par les mêmes engagements, fondés sur l'éthique professionnelle, les services à forte valeur ajoutée, le respect de l'individu et la richesse issue de leur diversité culturelle. Ils évoluent dans un environnement de travail favorable qui leur fait bénéficier d'une formation continue, de projets professionnels ambitieux et d'opportunités de carrière enrichissantes. Chaque professionnel de Deloitte contribue à renforcer l'engagement citoyen de la firme, à construire la confiance des marchés et à laisser une empreinte positive à toutes les actions entreprises.

Deloitte fait référence à Deloitte Touche Tohmatsu, un Verein suisse (association), et à son réseau de cabinets membres qui sont chacun constitués en entités indépendantes et juridiquement distinctes. Pour en savoir plus sur la structure légale de Deloitte Touche Tohmatsu et de ses cabinets membres, consulter www.deloitte.com/about

Contacts :

Nuno Afonso
Direction de la Communication
+ 33 (0)1 55 61 61 55
nuafonso@deloitte.fr

Eric Chauvelot
Agence Rumeur Publique
+33 6 80 58 38 48
eric@rumeurpublique.fr

Marie Goislard
Rumeur Publique
Tel: +33 1 55 74 52 33
Mobile: +33 6 21 23 37 75
e-mail : marie@rumeurpublique.fr