sécurité bancaire

Le culte de la sécurité et la gestion des risques sont des éléments inhérents aux institutions financières. S'agit-il là de nouveaux métiers ou d'une simple évolution ? Le point avec Solange Ghernaouti.

Risque informationnel : une

Solange Ghernaouti-Hélie
Professeure HEC Lausanne
Expert international à l'UIT

Les **métiers de la sécurité informatique** et de l'information évoluent et se développent pour répondre, entre autres, aux problèmes induits par de la dépendance aux technologies de l'information, la criminalité économique et la cybercriminalité.

Nouveau contexte, nouveaux besoins, nouveau business de la sécurité : force est de constater que le marché de la sécurité est saturé d'acteurs sans toutefois apporter de réponse totalement satisfaisante, comme nous le rappelle constamment l'actualité, qu'il s'agisse d'incidents techniques, de défaillances technologiques ou humaines ou encore de malveillance.

Les ressources informatiques et informationnelles deviennent des cibles et otages privilégiés pour les malveillants et organisations criminelles à la recherche de profits. Il s'agit d'une menace stratégique dans la mesure où l'argent-information se trouve dans les systèmes informatiques. Selon le Département de justice américain, **plus d'un tiers des accès criminels aux systèmes informatiques ont pour cible les institutions financières.** Ainsi, par exemple, l'explosion du phénomène d'usurpation d'identité depuis 2003, que cela soit via des techniques de phishing ou non, démontre que les criminels ont bien compris l'avantage qu'ils pouvaient tirer, non seulement des capacités d'anonymisation offertes par Internet, mais aussi de l'appropriation des fausses identités afin de ne pas être poursuivis ou tenus pour responsables d'actions illicites.

Les technologies de l'Internet facilitent toutes sortes d'infractions (vol, sabotage, détournement, violation du secret professionnel, de l'intimité numérique, dissémination de contenus illégaux, attaques concurrentielles, espionnage industriel, diffusion de fausses informations, dénis de service, fraudes diverses, etc.). Internet permet en toute impunité la réinsertion de l'argent sale dans les circuits économiques par le biais de transferts de flux, d'investissement et de capitalisation. Les placements boursiers en ligne, les casinos en ligne, le e-commerce – vente de produits et services fictifs contre paiement réel, générant des bénéfices justifiés, de telles activités sont incontrôlables et les poursuites en justice impossibles –, l'e-banking, les transactions du foncier et de l'immobilier via le Net, la création de sociétés virtuelles «écran», les porte-monnaie électroniques peuvent être utilisés pour effectuer les opérations nécessaires au blanchiment.

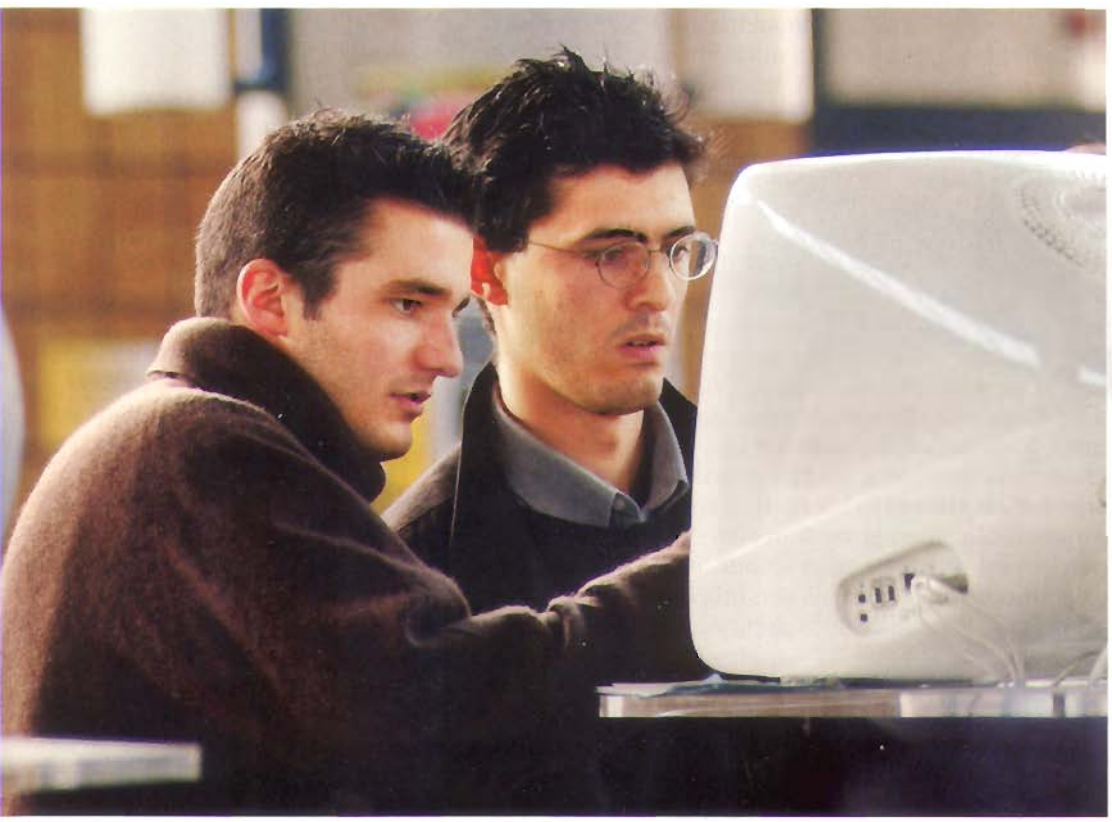
Internet expose les Etats, les organisations, les individus au risque d'origine criminel et permet le positionnement d'acteurs criminels à leur contact. Il peut également être vu comme un outil de déstabilisation et de réalisation de délits et être considéré comme étant une zone criminalisée.

Tout potentiel dysfonctionnement informatique, quelle que soit son origine «accident – erreur – malveillance», constitue un risque opérationnel dans la mesure où il en résultera un «risque de pertes dû à l'inadéquation ou à l'échec de processus internes, du personnel et de systèmes ou provenant d'événements externes» (Bâle II).

La culture de la sécurité et la gestion des risques sont des éléments inhérents aux institutions financières. A l'heure d'Internet, de la dématérialisation des données, des services, de l'argent et depuis notamment les accords de Bâle II, sécurité et risque informationnels prennent une dimension prépondérante dans la stratégie des organisations. Pour être pérennes, les institutions ont dû faire évoluer leur fonction sécurité. Evolution des fonctions, des tâches, des structures organisationnelles, des budgets, des mesures, des procédures, des contrôles, des outils et formations consacrés à la sécurité informatique, tout cela reflète un certain niveau de maturité du management et

« Plus d'un tiers des accès criminels aux systèmes informatiques ont pour cible les institutions financières »

simple évolution?



de l'ingénierie de la sécurité informatique dans le monde bancaire.

La plupart des institutions répondent au besoin de maîtrise des risques par l'intégration dans leur management, de la notion de «gouvernance» de la sécurité. **La mise en place d'une structure organisationnelle dédiée à la sécurité**, dotée de moyens d'action, concrétise la volonté directoriale de maîtriser le risque informatique par le développement d'une véritable doctrine de sécurité afin d'assurer la protection des valeurs, l'intelligence économique et la conformité juridique et ainsi contribuer au bon fonctionnement des institutions.

Bien que les métiers et les cahiers des charges possèdent des périmètres variables plus ou moins bien définis, les titres suivants sont couramment acceptés: *Chief Information Officer (CIO)*, associé au top management d'une institution. Il/elle est responsable de la stratégie et du management liés aux technologies de l'information ou du système d'information de l'organisation. *Chief Technology Officer (CTO)*, le plus souvent responsable de la recherche, du développement ou de l'innovation, liés aux technologies de l'information.

Pour ce qui concerne plus spécifiquement les métiers de la sécurité, retenons le responsable de la sécurité de l'organisation *Chief Security Officer (CSO)* et le responsable de la sécurité des informations *Chief Information Security Officer (CISO)*.

Selon la taille, les besoins ou la culture de l'organisation, diverses fonctions, missions spécifiques existent comme par exemple: responsable de la sécurité des systèmes d'information, de la sécurité des réseaux, des systèmes, de la veille technologique en matière de sécurité, auditeur ou encore architecte de la sécurité. La prise en compte des contraintes légales et des besoins de conformité à des règlementations ou à des politiques internes ont par ailleurs conduit à la définition de la fonction de *Chief Compliance Officer* ou de *Corporate Compliance Officer (CCO)*.

Auteure d'une quinzaine d'ouvrages, Solange Ghernaouti-Hélie est dorénavant mondialement connue par son ouvrage «Cybersecurity guide for developing countries», publié par l'Union Internationale des Télécommunications. Cet ouvrage de référence, présentant une approche interdisciplinaire de la maîtrise du risque informationnel, a été présenté à la World Telecommunication Development Conference, en mars dernier au Qatar comme ouvrage de référence au service du développement des nations.

«Dans la plupart des cas, les accords de Bâle II constituent une alerte pour les institutions financières qui souhaitent faire face aux risques opérationnels. Les institutions financières qui prennent le contrôle de ces risques par le biais des contrôles de sécurité des informations sûrs ont une bonne chance de réduire de manière significative leurs réserves de capitaux et de prospérer au cours des prochaines années». Bruce Moulton, vice-président en stratégie d'entreprise pour la sécurité des informations de Symantec Corporation.
«Bâle II: risques opérationnels et sécurité des informations.»[1]

[1] http://information-integrity.symantec.fr/article.cfm?articleid=270