

LA MENACE RÉELLE D'UN TSUNAMI DE L'INFORMATION

De United Airlines à Wikileaks, d'UBS à la Syrie, la sécurité de l'information est au cœur de l'actualité et prend une ampleur grandissante à la mesure de l'omniprésence des nouvelles technologies. Cependant, pour la plupart des entreprises, cette sécurité reste un concept très flou.

Newsletter n°711

Nos sociétés évoluent aujourd'hui en grande partie grâce aux nouvelles technologies de l'information et de la communication (Internet, Smartphones, etc.). L'information, sous toutes ses formes, est devenue un puissant outil pour le succès des entreprises, quelle que soit leur taille ou leur activité. Ainsi, comme un tsunami paraissait impossible il y a des dizaines d'années, nos sociétés modernes semblent avancer comme si un désastre lié à l'information était au-delà des limites de l'envisageable.

Pourtant, l'actualité est truffée d'événements qui lui sont liés. Très récemment la compagnie américaine United Airlines a connu une panne informatique telle que tous ses avions dans le monde ont dû rester cloués au sol. Tous les départs des vols et les systèmes de réservation ont été interrompus causant ainsi l'immobilisation de milliers de passagers.

Si les conséquences d'un tel événement sont certes moins désastreuses que celles d'un tsunami, elles révèlent pourtant l'importance grandissante de la sécurité de l'information.

Qu'est-ce que la sécurité de l'information ?

Contrairement à une idée répandue, la sécurité de l'information n'est pas essentiellement d'ordre technique. Elle revêt souvent

un aspect humain ou organisationnel. De manière générale, elle s'articule autour de trois types de pertes liées à l'information : perte de confidentialité, perte d'intégrité et perte de disponibilité.

Perte de confidentialité : l'information est divulguée à des personnes non autorisées. Pour ne citer que les derniers exemples en date, cette notion peut être illustrée par le vol et la revente des noms de clients de banques suisses ou encore l'affaire Wikileaks.

Perte d'intégrité : l'information a été endommagée ou modifiée, altérant ainsi son exactitude ou son authenticité. Le cas d'Enron et ses manipulations comptables représente un bel exemple de ce type de situation. Ou, plus récemment, on peut citer

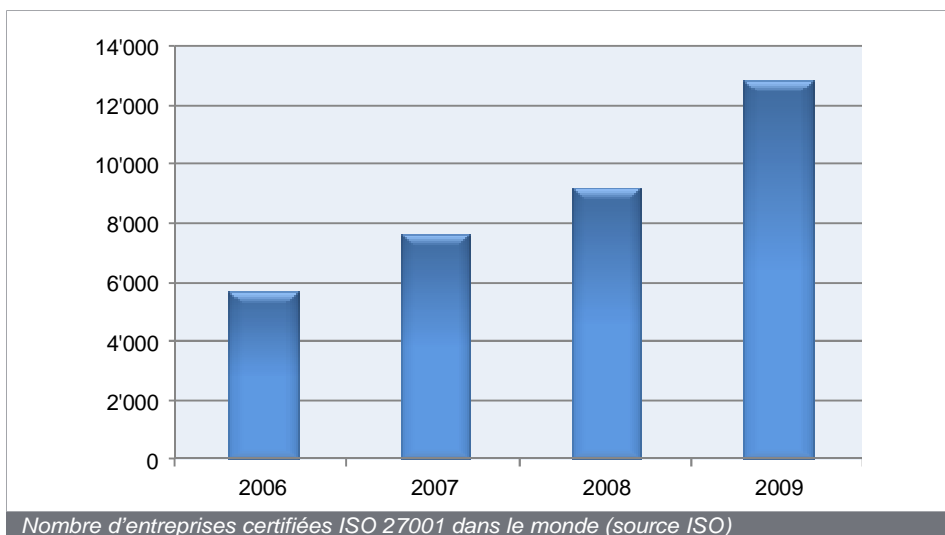
l'erreur médicale qui a conduit à l'irradiation du mauvais poumon d'un patient atteint d'un cancer.

Perte de disponibilité : l'information n'est plus disponible par les personnes qui en avaient légitimement l'accès. Ce cas peut être illustré par les coupures d'accès Internet en Egypte, en Lybie puis en Syrie qui ont nui à l'organisation de mouvements contestataires ou encore l'impossibilité d'accès aux services PayPal qui ont rendu vaine toute transaction sur Internet.

Si l'atteinte à la confidentialité ou à l'intégrité de l'information présente des conséquences notoires, elles restent pour autant maîtrisables. Une crise liée à la disponibilité de l'information, elle, paralyserait sans doute l'économie dans son ensemble.



Les 3 axes de la sécurité de l'information - © Optimiso Group SA



Les conséquences d'un tsunami de l'information

Il y a seulement 10 ans, une coupure générale des réseaux d'information n'aurait causé que des dommages limités. Cependant, la plupart des entreprises (et des personnes) se sont aujourd'hui réorganisées autour de ces réseaux. Les anciens procédés, les anciens postes de travail et les anciennes machines ont disparus au profit d'un nouvel et vaste accès à l'information grâce à Internet et via les technologies mobiles. De même, l'expansion du commerce en ligne est considérable. Moralité, une telle coupure aurait aujourd'hui des effets colossaux.

Il est par exemple envisageable de subir une crise liée à l'indisponibilité d'Internet et des réseaux téléphoniques. Dans ce cas, les entreprises ne pourraient plus effectuer de paiements en ligne et, pour certaines, ne pourraient plus vendre. Les banques ne passeraient plus d'ordres de paiement, les industries ne pourraient plus passer leurs commandes, créant des ruptures de stocks. Les sociétés de services ne communiqueraient plus avec leurs clients et il serait impossible de retirer de l'argent dans les distributeurs automatiques.

Dans de telles circonstances, tout le monde se dirigerait vers les guichets et réutiliseraient le bon vieux courrier. Ces solutions ne seraient malheureusement d'aucun secours dans la mesure où les entreprises ne sont plus équipées pour y répondre.

Les PME comme les grandes entreprises sont exposées en permanence à ce risque, bien qu'inégales en termes de vulnérabilité. Si certaines pourraient parfaitement fonc-

tionner plus d'une semaine, d'autres seraient bel et bien en danger après quelques heures seulement.

Quelles solutions ?

Pour se préparer à de telles éventualités, les 150 pays membres de l'organisation ISO ont établi en 2005 un guide relatif à la sécurité de l'information : la norme ISO 27001. Cette méthode pragmatique permet aux entreprises privées comme aux établissements publics de se poser les bonnes questions et de mettre en œuvre une approche systématique pour maîtriser les risques liés à l'information.

Cette méthode très complète déclinée en 133 points de contrôles peut être résumée en trois étapes principales :

- 1) Identifier les différents types d'information utilisés par l'entreprise.
- 2) Identifier pour chaque information quel serait l'impact sur la perte de disponibilité, d'intégrité ou de confidentialité.
- 3) Mettre en place les mesures de protection nécessaires et utiles.

En 2009 (derniers résultats publiés par ISO) quelque 13'000 entreprises étaient certifiées ISO 27001 dans le monde, principalement des entreprises de services ou actives dans la technologie de l'information ainsi que des administrations publiques.

Dans le cadre de notre activité de diagnostic et de mise en œuvre de systèmes de sécurité de l'information, nous notons cepen-

dant une prise de conscience croissante de la part des entreprises suisses : "toujours plus d'entreprises sont demandeuses de diagnostic ou d'accompagnement dans la mise en place de la sécurité de l'information ou se dirigent vers une certification ISO 27001. Elles ont pris conscience de leur vulnérabilité et se prémunissent ainsi d'un risque grandissant".

Les entreprises se sont réorganisées autour des nouvelles technologies de l'information et de la communication depuis une dizaine d'années déjà, à une vitesse telle que le phénomène n'est pas prêt de tarir. Corollaire de ce phénomène, elles sont plus que jamais menacées par les risques liés à la sécurité de l'information.

Grâce à la norme ISO 27001 les entreprises disposent d'une approche pragmatique et systématique qui leur permet d'aborder de manière concrète et sereine la sécurité de l'information. Bien que cette norme existe depuis 2005, elle prendra tout son sens dans les années à venir.

Thomas Kortmoller, Optimiso group SA

À propos d'Optimiso Group SA

La mission d'Optimiso Group SA est d'offrir aux entreprises des solutions complètes pour décrire, modéliser et communiquer leur organisation (processus, procédures, risques & contrôles, prestations, instructions, job descriptions, etc.).

Elle offre des solutions utilisées depuis plus de 15 ans sur le plan national et international via deux produits : le logiciel Optimiso® et le service de conseil D-skribe®.

- Qualité
- ISO
- Contrôle Interne
- Processus et procédures
- Optimisation
- Risques
- Sécurité
- Gestion documentaire
- Job description

GENÈVE - BÂLE - LYON