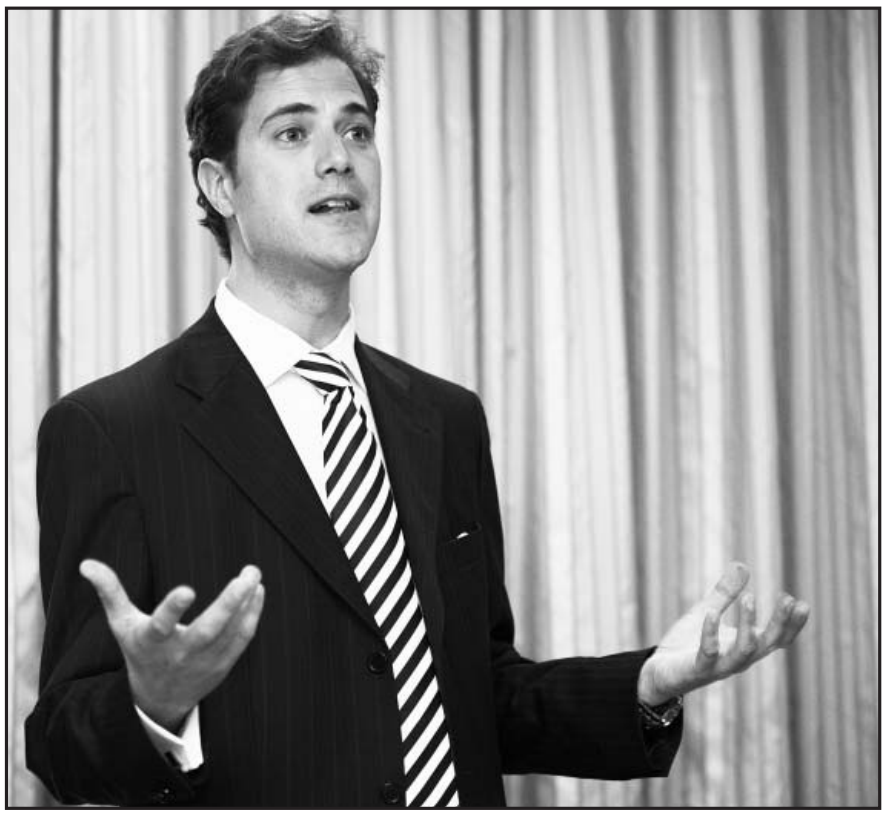
Utilisation inappropriée d'Internet au travail

Nouvelles problématiques en matière de sécurité

Alain Vallières, *Ph.D.*

Ce vendredi après-midi, nous étions plusieurs dizaines de personnes inquiètes à nous demander s'il était possible de nous en sortir indemnes. Ce qui nous était montré semblait être sans issue. Il ne s'agissait pas d'une confrontation avec un nouveau manège de La Ronde, mais bien d'une conférence sur la sécurité informatique. Pour avoir des sueurs froides, il n'y a rien de tel que d'écouter l'exposé d'un expert en sécurité informatique. Avis aux amateurs de sensations fortes...



M. Claude Sarrazin

La conférence était prononcée par **M. Claude Sarrazin**, **président de la Société industrielle et renseignement corporatif (SIRCO)**. Cet ancien policier, enquêteur chevronné, connaît bien les problèmes liés à l'utilisation d'Internet en milieu de travail.

L'utilisation inappropriée de l'autoroute de l'information n'est pas sans conséquences pour les entreprises. Dans le meilleur des cas, l'employeur n'y perdra que du temps payé et de la bande passante achetée. Le mal peut toutefois être plus important si l'employé utilise des informations à son avantage ou à celui d'un tiers. Il peut aussi introduire des virus dans le système informatique de l'entreprise.

Navigation en eaux troubles

La navigation à caractère personnel peut devenir un problème pour une entreprise en raison de l'utilisation abusive que peuvent faire les employés du matériel informatique. Or, il appert que seulement 25 % des entreprises ont une politique pour gérer les situations d'abus.

Un autre problème découle de l'utilisation des postes informatiques pour télécharger du matériel pornographique. Suivant l'expérience de M. Sarrazin, près de 70 % du matériel pornographie est téléchargé entre 9 h et 17 h et 30 % des utilisateurs sont des femmes. On peut généralement trouver du matériel pornographique dans un ordinateur sur trois dans les entreprises. Un des problèmes de cette utilisation réside dans la dépendance qui en découle. Il est arrivé à M. Sarrazin d'étudier le cas d'un cadre qui naviguait sur ces sites jusqu'à six heures quotidiennement, ce qui ne laisse que peu de temps pour le travail.

Gare aux pirates !

Au-delà de la perte de productivité, la question de la sécurité des systèmes informatiques se pose aussi. Les sites pornographiques possèdent en effet des codes malicieux pouvant être sources de piratage. Plusieurs de ces sites, même gratuits, nécessitent l'utilisation d'une carte de crédit. Or, il arrive que les employés donnent le numéro de leur carte d'entreprise en exposant leurs employeurs. Jusqu'à 2 000 000 de numéros de carte de crédit sont récoltés mensuellement de cette façon.

Les programmes informatiques illégaux présentent aussi des problèmes dans les entreprises. Plusieurs programmes viennent de fichiers partagés. Or, ces fichiers se trouvent souvent dans les ordinateurs des techniciens des entreprises qui prisent l'utilisation des sites de fichiers partagés. Ils installent par la suite ces programmes sur les ordinateurs des autres employés, diffusant des programmes ne respectant pas les droits d'auteur et exposant de la sorte leurs employeurs. Il est arrivé aux employés de SIRCO de trouver jusqu'à 75 programmes piratés dans une entreprise.

L'ennemi n'est pas toujours éloigné

Plusieurs utilisations non appropriées du matériel informatique ont lieu à l'intérieur même de l'entreprise. Il arrive ainsi que des surveillances non autorisées des communications aient lieu, de même que des intrusions non permises dans les boîtes de courriel ou du harcèlement d'employés. Du sabotage industriel peut être opéré de l'intérieur de l'entreprise, de même que de l'espionnage industriel. Suivant les statistiques disponibles, 45 % des compagnies en Amérique du Nord affirment avoir été victimes d'une attaque provenant d'un poste informatique d'un employé. Il existe même des sites Internet fournissant gratuitement les programmes nécessaires pour permettre aux collaborateurs licenciés de se venger.

Comment colmater les brèches ?

Le problème se posant avec Internet est la difficulté de la preuve du méfait. La technologie seule peut permettre d'identifier qu'un poste a servi à poser l'acte, mais, il nous restera à prouver qui l'utilise.

Au-delà de l'identification du responsable se pose la question de la prévention. Ainsi, pourquoi ne pas poser des codes d'accès individuels sur l'ensemble des appareils ? Ce n'est pas suffisant. Cette méthode est d'une efficacité toute relative, principalement en raison de facteurs humains : les codes s'échangent, un poste est resté abandonné allumé et accessible à tous, le code est noté et collé sur l'écran... Les failles sont multiples et difficiles à contrôler. Certains fraudeurs vont jusqu'à le demander le plus simplement du monde à la réceptionniste, sous couvert de procéder à un contrôle technique. Il existe même des programmes disponibles gratuitement pour déchiffrer ces codes.

Plus étonnant mais vrai, le truc – vu dans de nombreux films d'espionnage – de la poudre pour bébé saupoudrée sur une empreinte digitale et collectée sur un papier adhésif pour contourner les systèmes de contrôle.

Des entreprises peuvent avoir des portes ouvertes sur le monde sans même le soupçonner. Certains appareils des plus insoupçonnables peuvent ainsi contenir des fonctions Wifi à l'insu du propriétaire. Que penser de la nouvelle machine de fabrication qui est branchée sur Internet pour assurer un contrôle de qualité par le vendeur ? N'est-ce pas une porte ouverte sur le réseau du propriétaire ?

Que conseiller à votre client victime d'une intrusion

Ne touchez à rien ! Et rien, c'est rien ! Un des plus importants problèmes auxquels doit faire face l'enquêteur est l'appareil manipulé après découverte d'un fait illicite. Il n'est en effet pas rare que le technicien maison ait voulu vérifier les informations. Or, outre le fait qu'il peut détruire de précieuses informations, quelles sont les garanties pour l'employeur que cet employé n'est pas parti au méfait ?

Il est ainsi préférable de ne pas toucher au poste, ne serait-ce que pour le déconnecter. Un ordinateur peut fournir de nombreuses informations. Même un disque dur reformaté de nombreuses fois continue de parler.

Pour éviter les ennuis, il existe quelques conseils simples

1. Ayez une politique claire d'utilisation d'Internet. Si des abus surviennent, il sera possible de se départir de l'employé indélicat.

2. Maintenez à jour vos mécanismes de protection. L'informatique évolue rapidement. Ce que vous avez acheté il y a six mois est maintenant dépassé.

3. Gérez convenablement les ressources humaines. Les banques ont bien compris qu'une seule personne ne peut détenir l'ensemble des informations sensibles. Or, en informatique, des employés subalternes peuvent posséder les clefs les plus importantes d'une compagnie. Plus les informations sont sensibles, plus le nombre de personnes pouvant y accéder devrait être réduit.