

## **Lutte contre le crime cybernétique – au-delà du vol d'identité et du pourriel**

Dans l'opinion publique le crime cybernétique concerne principalement le vol d'identité et le pourriel. Mais le problème est plus vaste que cela et les résolutions ci-incluses visent à traiter de questions allant au-delà de ces deux problèmes graves.

Lors d'une rencontre avec Janet Napolitano, secrétaire du département de la Sécurité intérieure, le ministre de la Sécurité publique du Canada, Peter Van Loan, a qualifié la sécurité cybernétique de « nouvelle course aux armements » alors que le gouvernement lutte pour protéger ses systèmes d'information contre des menaces en provenance du monde entier.

En 2008, un sondage national effectué par Deloitte à la demande de l'Association canadienne des commissions de police (ACCP) a révélé que le crime cybernétique est le principal enjeu auquel sont confrontés les organismes d'application de la loi au Canada.

L'Internet est devenu un élément essentiel de la vie quotidienne et un mécanisme indispensable pour le commerce international. Il a engendré une multitude d'opportunités qui ont apporté d'énormes succès financiers aux entrepreneurs légitimes et criminels du globe. Malheureusement, le jeu et les lois qui régissent les organismes d'application de la loi à l'échelle mondiale favorisent les criminels. En effet, grâce à leurs énormes ressources financières (aptés à rivaliser avec celles de nombreux pays), ces criminels peuvent embaucher les gens les plus talentueux, acheter les plus récentes technologies et tirer parti de systèmes légaux archaïques qui ne sont pas à jour des activités criminelles, n'instituent pas des recours judiciaires conformes aux nouvelles méthodes des criminels et paralysent les organismes d'application de la loi parce qu'ils sont inadéquats, désuets et inadaptés au monde moderne.

Le vol d'identité et la fraude subséquente remplacent rapidement le trafic de stupéfiants comme principale source d'argent provenant d'activités criminelles, tandis que le pourriel menace de sursaturer le système, accaparant temps et ressources tout en étant le vecteur de fraude et d'attaques contre les systèmes cybernétiques du globe.

Voici certaines constatations du sondage effectué par Deloitte pour l'ACCP :

- 49 % des répondants ont été victimes de crimes cybernétiques (y compris virus informatiques, perte ou vol de renseignements bancaires ou personnels sur Internet, intimidation ou abus sexuel d'enfants par le truchement de contacts en ligne, piratage et imposition de rançons aux entreprises, vol d'identité et interférence de l'infrastructure essentielle comme les réseaux électriques, systèmes de distribution d'eau ou services téléphoniques).
- 70 % des victimes d'un crime cybernétique n'ont pas signalé le crime, faute de savoir à qui le signaler ou de croire que justice serait faite.
- 86 % des répondants indiquent que le crime cybernétique est devenu préoccupant.
- 95 % des répondants croient qu'ils sont la cible de crimes cybernétiques (la majorité des répondants croit que les menaces les plus graves sont le vol d'identité, la fraude financière et les virus informatiques).
- 89 % des répondants pensent que la prévention du crime cybernétique devrait être une priorité pour le gouvernement et les organismes d'application de la loi.

Quelques considérations additionnelles :

- Un récent sondage mené par IBM auprès des secteurs des services de santé, de la finance, de la vente au détail et de la fabrication révèle que près de 60 % des entreprises croient que le crime cybernétique leur coûte plus cher que le crime physique.
- Une étude effectuée en 2007 par la U.S. Cyber Consequences Unit révèle que la destruction due à une seule vague d'attaques cybernétiques contre les infrastructures essentielles pourrait excéder

700 milliards de dollars – l'équivalent de 50 ouragans majeurs frappant les États-Unis simultanément.

- Selon une étude menée en 2007 par Symantec, le Canada se classe neuvième parmi les pays les plus souvent ciblés par les actes cybernétiques malveillants, tandis que les États-Unis sont au premier rang. Cette étude a également découvert plus de 700 000 menaces découlant de nouveaux codes malveillants pour 2007, en hausse par rapport à 125 000 en 2006.

La Chambre de commerce du Canada a discuté du vol d'identité et du pourriel dans des résolutions antérieures (2007); or, il y a des crimes cybernétiques autres que ces aspects, notamment l'espionnage et le terrorisme, qui menacent le commerce et l'intégrité du pays et doivent être traités par notre gouvernement.

## **Recommandations**

Que le gouvernement fédéral

Outre les recommandations sur l'usurpation d'identité (2007) et l'endiguement du pourriel (2007):

1. Modifie le *Code criminel* pour moderniser les dispositions relatives à la perquisition, à la saisie et à l'interception (particulièrement la partie 6) en fonction des progrès technologiques et, pour ce faire :
  - Oblige les fournisseurs de services téléphoniques et Internet à ajouter une capacité d'interception aux nouvelles technologies dès que des normes nord-américaines auront été formulées;
  - Oblige les fournisseurs de services de télécommunications à communiquer le nom et l'adresse de leurs clients au personnel des organismes d'application de la loi qui en fait la demande;
  - Oblige les fournisseurs de services à s'assurer que les renseignements désignés concernant un abonné particulier soient conservés et fournis en réponse à une ordonnance d'un tribunal;
  - Engage des discussions avec les fournisseurs afin de fixer des coûts raisonnables pour la satisfaction des exigences précédentes et d'élaborer un processus d'indemnisation de ces coûts.
2. Établisse un mécanisme centralisé relatif au signalement obligatoire d'attaques désignées contre la sécurité cybernétique pour faciliter la quantification des torts éventuels à l'économie canadienne.

Établisse un programme national d'éducation pour sensibiliser les enfants au crime cybernétique et mette en œuvre des programmes de prévention qui seraient intégrés aux programmes d'études.

Formule et mette en œuvre une campagne nationale visant à sensibiliser la population et le milieu des affaires aux risques associés au manque de connaissance des activités des criminels cybernétiques et à l'absence de protection contre ces activités.

Établir un site Web qui jouerait le rôle de centre de renseignements à jour sur le crime cybernétique au Canada, à des fins d'information et d'éducation publique, comportant des liens surveillés vers des centres d'information semblables à l'échelle du globe.