**La SSI -des risques en augmentation car les vulnérabilités augmentent**

*Traduction en Français de la*
**déclaration faite par Bruce Schneier**
**fondateur et directeur technique de la société Counterpane Internet Security, Inc.**
**qui commercialise un service de gestion de la sécurité de systèmes (MSSS)**
**L'audition du 25 juin 2003 a pour titre**
**“Sommaire d'un problème de la société de l'information ("cyber problem")**
**— une Nation en dépendance et traitant les risques"**
**devant le comité spécial sur le sécurité intérieure,**
**sous comité sur la recherche et le développement**
**en matière de sécurité de la société de l'information (" cybersecurity ")**

Elle a été cataloguée sous le titre:
"Cybersecurity -Growing risks from growing vulnerabilities"
**La SSI -des risques en augmentation car les vulnérabilités augmentent."**
http://hsc.house.gov/files/Testimony_Schneier.pdf

Testimony and Statement for the Record
Bruce Schneier Founder and Chief Technical Officer
Counterpane Internet Security, Inc.
Hearing on
“Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk”

Merci monsieur le Président et vous tous les membres du comité pour l'occasion qui m'est offerte aujourd'hui de témoigner en ce qui concerne la sécurité des systèmes d'information (SSI –“ cybersecurity ”, ou **s**écurité de la **s**ociété de l'**i**nformation) particulièrement dans sa relation à la défense des infrastructure vitales de notre patrie et de notre nation. Mon nom est Bruce Schneier, et j'ai travaillé dans le domaine de sécurité informatique pendant toute ma carrière. Je suis l'auteur de sept livres sur le sujet, y compris le succès commercial "Secrets et mensonges: la sécurité numérique dans un Monde en réseau" [1]. Mon dernier livre à pour titre "Au delà de la peur: concevoir sagement la sécurité dans un monde incertain" [2], et sera publié en septembre 2003. En 1999, j'ai fondé la société Counterpane Internet Security, Inc., où j'occupe la position de directeur technique. Counterpane Internet Security, Inc. fournit la [télé]surveillance de la sécurité en temps réel pour plusieurs centaines d'organismes, y compris plusieurs organismes du gouvernement fédéral.

**Les risques dans la société de l'information (Cybersecurity).**
Quand j'ai commencé ma longue carrière en sécurité informatique, c'était une discipline marginale. Les seules signes d’intérêt venaient des militaires et de quelque défenseurs dispersés de la protection des données personnelles. L'internet a changé tout cela. La promesse de l'internet est d'être un reflet de la société. Tout ce que nous faisons dans le monde réel —toutes nos interactions sociales et économiques et toutes les transactions— nous voulons le faire sur l'Internet: avoir des entretiens privés, conserver des documents personnels, signer des lettres et des contrats, parler tout en restant anonyme, pouvoir s'appuyer sur l'intégrité d'information, jouer, voter, publier des documents authentiques. Toutes ces actions exigent de la sécurité. La sécurité informatique est un principe qui rend utile les technologies de l'internet; c'est ce qui transforme l'internet d’une curiosité universitaire en un outil économique sérieux [pour faire des affaires]. Les limites de la sécurité [offerte] sont [et seront] les limites de l'internet. Et toutes les entreprises et toutes les personnes ont ces besoins de sécurité.

**La SSI -des risques en augmentation car les vulnérabilités augmentent**

Les risques sont réels. Tout le monde parle des risques directs: le vol de secrets industriels, de fichiers de clients, d'argent. Les gens parlent aussi des pertes de productivité causées par des problèmes de sécurité informatique. Quelle est la perte économique pour une entreprise si son courrier électronique s'arrête pendant deux jours? Ou si dix personnes doivent s'escrimer pour nettoyer après une intrusion particulièrement méchante? J'ai vu des chiffres de l'ordre de plusieurs milliards cités pour les pertes totales liées aux infections Internet comme Nimda et SQL Slammer; la plus grande part en est attribuée à des pertes de productivité.

Les risques indirects sont plus importants: la perte de clients, les dommages à l'image de marque, la perte d'actifs incorporels. Quand une attaque réussie contre une société commerciale est rendue publique, la victime peut ressentir une baisse du niveau de prix de ses actions. Quand "CD Universe" a subi un vol de numéros de cartes de crédit important (et public) au début de l'année 2000, cela leur a coûté très cher dans leur bataille pour les parts de marché contre amazon.com et CDNow. Dans les conséquences d'attaques d'entreprises qui ont été rendues publiques, les entreprises ont plus souvent dépensé de l'argent et des efforts pour les relations publiques que pour la réparation même du problème de sécurité. Les institutions financières maintiennent régulièrement secrètes les attaques réussies, pour éviter d'inquiéter leur clientèle.

Des risques plus indirects encore surviennent dans les traitements des conflits. Les pays européens ont les lois de protections des données [personnelles et de patrimoine] strictes; les entreprises peuvent être tenues pour responsables si elles ne prennent pas de précautions [suffisantes] pour protéger les données personnelles de leurs clients. Les États-Unis ont des lois similaires dans quelques secteurs privés —le secteur bancaire et le secteur de la santé— et il y a des projets de lois au Congrès pour protéger plus généralement les données personnelles [et de patrimoine]. Nous n'avons pas encore vu d'actions en justice d'actionnaires contre des entreprises qui n'ont pas réussi à sécuriser suffisamment leurs réseaux et ont pâti des conséquences, mais cela commence à arriver. Les dirigeants d'entreprise peuvent-ils être tenus personnellement pour responsables s'ils ne pourvoient pas à la sécurité des réseaux? Les tribunaux décideront cette question dans les années qui viennent.

La présente audition a été organisée pour traiter un autre type de risque: les risques encourus par les infrastructures vitales de notre nation qui sont principalement dans les mains de sociétés privées. Un des grands défis de la SSI ("cybersecurity") est dû aux interdépendances entre les réseaux. Les décisions de sécurité que prend une entreprise pour son propre réseau peuvent avoir des effets très lointains à travers nombreux réseaux, et ceci nous conduit à des types différents de risques. J'appelle ces risques externes (" ancillary " de dépendance) parce que leurs effets sont extérieurs mais liés au réseau particulier en question. Les risques externes [externalisés] sont légions dans la société de l'information ("Cyberspace"). Par exemple, les utilisateurs de micro-ordinateurs domestiques risquent des attaques et risquent de voir ainsi leurs machines contrôlées par d'autres, mais un risque externe est ainsi créé quand leurs ordinateurs sont attaqués et contrôlés [par d'autres]: ils peuvent être utilisés [à leur insu] pour d'autres attaques futures contre d'autres réseaux. Les vulnérabilités dans les logiciels créent un risque pour la société qui commercialise ces logiciels, mais elles créent aussi un risque externe pour ceux qui utilisent ces logiciels dans leurs réseaux.

Le risque SSI (" cybersecurity risk ") pour notre nation est principalement externe [aux acteurs]; comme notre infrastructure critique est en grande partie dans les mains de sociétés privées, il y a des risques pour notre nation qui vont [bien] au-delà de ce que ces sociétés

privées prennent en charge. Le réseau de téléphone a de la valeur pour les opérateurs téléphoniques parce qu'ils en tirent leur revenu, et ces opérateurs sécuriseront leurs réseaux à la mesure de cette valeur. Mais, pour le pays, en plus de cela, le réseau a une valeur en tant qu'infrastructure nationale de communications, et il y a donc des risques externalisés. Les entreprises prennent des risques quand elles achètent et utilisent des logiciels fragiles, mais elles causent aussi des risques externes pour tous les autres [acteurs] sur l'Internet parce que ces logiciels sont sur un réseau commun. Ces risques externalisés s'avèrent critiques pour les insécurités actuelles de la société de l'information ("cyberespace"), et c'est seulement en les traitant que nous améliorerons vraiment la situation.

Quels que soient les risques d'être sur Internet, les entreprises n'ont aucun autre choix que d'y être présentes. Les leurres et les appâts de nouveaux marchés, de nouveaux clients, de nouvelles sources de revenus, et de nouveaux modèles d'activité sont si forts que les entreprises ont afflué sur l'Internet sans tenir aucun compte des risques. Il n'y a pas d'alternative. Les gouvernements ressentent des pressions du même type: de meilleurs moyens d'interagir avec les citoyens, des moyens plus efficaces de diffuser des informations, une plus grande implication des citoyens dans le gouvernement. L'internet est là pour durer, et nous allons l'utiliser de plus en plus sans aucune considération pour les risques. Ceci, plus que toute autre chose, est la raison de l'importance [du rôle] de la sécurité informatique.

**Quantifier les Risques**

La quantification des risques est difficile, parce que simplement nous ne disposons pas des données. La plus grande partie de ce que nous savons est anecdotique, et les statistiques dont nous disposons sont délicates à généraliser. Sommairement, les agressions ("cyberattacks") sont courantes sur l'Internet. Les entreprises commerciales sont [virtuellement] cambriolées régulièrement, d'habitude par les passionés/pirates/corsaires ("hackers") qui n'ont aucune autre motivation que le simple droit de se vanter. Il y a un vandalisme à la petite semaine considérable sur l'Internet, et parfois ce vandalisme devient géant voire à l'échelle du système. La criminalité augmente sur l'Internet, la fraude individuelle ainsi que les crimes économiques. Nous savons que tout ceci arrive, parce que toutes les enquêtes, toutes les études économiques, et tous les éléments anecdotiques convergent. Simplement, nous en ignorons les chiffres réels.

Chacune des huit années passées, l'Institut de Sécurité Informatique (CSI) a conduit une enquête annuelle sur la criminalité informatique pour les entreprises privées américaines, les agences du gouvernement, et les autres organismes [3]. Les détails sont saisissants, mais la tendance générale est que la plupart des réseaux sont attaqués à maintes reprises et souvent avec succès, ce, d'une foultitude de manières, et que les dégâts économiques sont considérables; de plus les technologies ne peuvent pas faire grand chose pour empêcher cela. En particulier, l'étude 2003 a montré les choses suivantes:

• 56% des réponses signalent "l'accès sans autorisation à des systèmes informatiques" dans l'année dernière. 29% ont affirmé qu'ils n'avaient pas observé de tels accès, et 15% ont dit qu'ils ne savaient pas. Le nombre d'incidents était réparti partout, et le nombre d'incidents d'origine interne équilibrait à peu près le nombre d'incidents d'origine externe. 78% des réponses indiquent leur connexion à Internet comme un point fréquent pour les agressions (ceci a augmenté de façon continue pendant six ans de suite), 18% signalent des agressions par appel téléphonique ("dial-in") (la proportion a bien diminué), et 30% indiquent que les systèmes internes sont des points fréquents d'agression (aussi en diminution).

• les genres d'agressions s'étagent de la fraude aux télécommunications au vol de portable en passant par le sabotage. 36% ont eu l'expérience d'une intrusion dans leur système, 42%

l'expérience d'un déni -refus- de service (arrêt apparent du service offert). 21% indiquent un vol de données, et 15% une fraude financière. 21% signalent un sabotage. 25% ont eu leurs sites Webs (de publication) saccagés -"hacked"- (22% ne savent pas répondre), et 23% ont eu leurs sites Webs saccagés dix fois ou plus (36% des agressions de site Web eu pour résultat des défigurations, 35% des refus de service, et 6% des agressions comprenaient un vol de données de transactions).

• Une chose intéressante soulignée par cette étude est que toutes ces attaques se sont produites malgré le déploiement très répandu de technologies de sécurité: 98% disposent de cloisons pare-feu -firewall-, 73% disposent d'un système de détection d'intrusion, 92% utilisent un type de contrôle d'accès, 49% une pièce d'identité numérique. Il semble que ces produits de sécurité très prisés ne fournissent qu'une sécurité bien partielle face aux agresseurs.

Malheureusement, la base de données de CSI ne s'appuie que sur les réponses volontaires aux enquêtes. Les données ne comprennent que les agressions que les entreprises ont identifiées, et uniquement les agressions qu'elles veulent bien admettre dans une telle enquête.

Il n'y a aucun doute, les agressions réelles sont en nombre beaucoup plus important. Et les personnes qui répondent à l'enquête de CSI sont celles qui sont déjà expertes en sécurité; les entreprises qui sont moins calées en sécurité ne sont pas touchées par cette enquête. Ces sociétés subissent sans aucun doute encore plus d'agressions réussies et des dégâts plus importants.

Le projet "Honeynet" ("réseau de pots de miel") est une autre source de données. C'est un projet universitaire de recherche qui mesure [la pression] des agressions informatiques qui ont lieu sur l'Internet. Selon leurs statistiques les plus récentes [4], publiées en 2001, un ordinateur quelconque sur l'Internet est scruté ("scanned") des douzaines de fois par jour [pour savoir s'il est attaquable]. L'espérance de vie moyenne d'une installation par défaut [à la sortie de la boîte] d'un Linux Red Hat 6.2 serveur —c'est-à-dire le temps avant que quelqu'un ne le saccage avec succès— est inférieure à 72 heures. Une installation classique d'utilisateur à la maison, avec Windows 98 et autorisant les fichiers partagés a été attaquée avec succès cinq fois en quatre jours. Les systèmes sont soumis à des douzaines de balayages hostiles [en recherche] de vulnérabilités chaque jour. Et le délai le plus court avant que le serveur ne soit attaqué avec succès: 15 minutes après avoir branché au réseau. Ces données correspondent à ma propre expérience anecdotique d'avoir mis des micro-ordinateurs sur un accès domestique à haut débit.

A Conterpane Internet Security Inc., nous élaborons nos propres statistiques. En 2002, nous avons contrôlé plus de cent réseaux informatiques dans plus de trente pays. Nous avons traité 160 milliards d'événements sur les réseaux, dans lequel nous avons identifié plus de 105 millions d'alertes de sécurité [1/1500]. Un traitement ultérieur en a tiré 237,000 “tickets” qui ont été examinés par nos spécialistes de la sécurité [1/450], et ont généré 19,000 appels immédiats de clients pour des incidents de sécurité [1/12]. Si nous supposons que nos données sont bien représentatives, [nous en déduisons qu’]une entreprise type aux États-Unis subit chaque année 800 événements critiques de sécurité de réseau —[c'est à dire] des événements exigeant une attention immédiate— [**soit 2,2 par jour !**]. À Counterpane, nous avons suffisamment de compétences et de savoir faire pour que ces incidents ne causent aucune perte financière pour les entreprises que nous protégeons, mais la plupart des entreprises ne disposent pas de gardes aussi vigilants sur leurs réseaux.

**Les tendances en défense de la société de l'information ("Cybersecurity trends")**

**La SSI -des risques en augmentation car les vulnérabilités augmentent**

Plusieurs évolutions en cours de la SSI doivent être soulignées. En premier lieu, dans les dernières dizaines d'années, les agressions sur les ordinateurs individuels, les premiers réseaux et puis l'Internet sont devenues de plus en plus graves. Les outils d'agressions sont devenus plus puissants, ils causent plus de dommages, et ont un meilleur rendement. Les agressions autrefois longues à réaliser sont aujourd'hui automatisées. Les assauts qui étaient parables par un mécanisme unique sont maintenant capables de s'adapter. Les virus, les vers, et les chevaux de Troie sont plus travaillés et doués d'intelligence; les programmes malveillants qui, il y a des années, prenaient des semaines pour se diffuser sur le réseau ("cyberespace"), ont mis quelques heures l'année dernière, et aujourd'hui leur diffusion est une question de minutes.

En deuxième lieu, durant cette même période, le savoir faire nécessaire pour lancer ces agressions a diminué. Beaucoup d'outils d'attaque sont faciles à utiliser. Ils ont des interfaces avec menus et souris ("pointe et clique"). Ils sont automatisés. Ils ne demandent aucune compétences pour être mis en œuvre. Les “rootkit” [boites à outils d'agression permettant aussi d'effacer ses traces] sont à la fois plus faciles à utiliser et plus efficaces.

Ces deux tendances se combinent pour aggraver une autre tendance: l'augmentation de la criminalité dans la société de l'information ("cyberespace" sur les réseaux). La plus grande partie des attaques sur les réseaux ne sont rien plus que du petit vandalisme : l'équivalent sur Internet des tags sur les murs. Les motivations des agresseurs sont réduites à se faire des frayeurs bon marché et à pouvoir s'en vanter. Parfois ce ne sont que des adolescents qui s'ennuient. Parfois ce sont des gosses intelligents sans autres possibilités d'expression. Mais nous commençons à voir des augmentations significatives de la véritable criminalité sur l'Internet. Les criminels, qui manquent souvent du savoir-faire informatique pour faire des effractions dans les réseaux, peuvent utiliser ces outils très faciles d'emploi pour commettre des crimes. Les vols de cartes de crédit et les autres formes de fraude sont en croissance. Le vol d'identité [financière] est en croissance. Les cas d'extorsion augmentent. À Counterpane, souvent le travail le plus difficile que nous ayons est de détecter ces agressions criminelles parmi les centaines d'agressions de petits vandales. Je prévois la poursuite de cette tendance car plus de criminels découvrent le rendement potentiel de leurs fraudes dans la société de l'information ("cyberespace").

Du point de vue défensif -de la protection-, [la société de l'information et ses] réseaux deviennent moins sûrs au fur et à mesure que [les techniques et] les technologies s'améliorent. Il y a beaucoup de raisons à ce phénomène paradoxal en apparence, mais tout peut être ramené à un problème de complexité. Comme j'ai dit par ailleurs [5], la complexité est le pire ennemi de la sécurité. Les raisons en sont compliquées et on peut en faire une analyse très technique, mais je vous peux vous donner une idée de la justification: les systèmes complexes contiennent plus de lignes de code [logiciels] et par conséquent plus d'erreurs de sécurité. Les systèmes complexes ont plus d'interactions et par conséquent plus d'insécurités potentielles. Les systèmes complexes sont plus difficiles à tester et ont par conséquent plus de chance de contenir des parties non testées. Les systèmes complexes sont plus difficiles à définir et architecturer de façon sûre, plus difficiles à réaliser de façon sûre, plus difficiles à configurer de façon sûre, et plus difficiles à utiliser de façon sûre. Les systèmes complexes sont plus difficiles à comprendre pour les utilisateurs. Tout dans la complexité conduit à une sécurité inférieure. Comme nos ordinateurs et nos réseaux deviennent plus complexes, ils deviennent intrinsèquement moins sûrs.

Une autre tendance est l'inefficacité [crasse] des produits de sécurité. Ceci n'est pas dû aux échecs de la technique et de la technologie, mais beaucoup plus aux échecs des modalités de configuration et d'emploi. Aussi stupéfiant qu'il paraisse, la grande majorité des produits de sécurité n'est pas simplement réalisée de façon efficace. Le reproche pourrait être fait aux produits qui sont trop difficiles à utiliser. Le reproche pourrait fait aux administrateurs de systèmes, qui installent souvent les produits de sécurité sans y réfléchir suffisamment. Mais le vrai reproche est à faire à notre culture: la sécurité [des SI] n'est tout simplement pas une priorité pour la plupart des organisations. La sécurité est habituellement négligée, contournée, ou traitée du bout des lèvres. Les produits [de sécurité des SI] sont achetés parce que l'organisme a besoin de réussir un audit ou d'éviter un litige, mais beaucoup moins d'attention est portée à leurs modalités d'utilisation. Cela se compare à un propriétaire qui a acheté une serrure assez chère et l'a installée d'une façon qui ne fournit aucune sécurité.

Des considérations analogues, la qualité de la sécurité des logiciels est catastrophique. Les produits sont couramment livrés avec des centaines ou des milliers de vulnérabilités de sécurité. À nouveau, il y a des raisons techniques à cela. La science de la sécurité informatique en est à ses premiers pas. Nous ne savons pas, par exemple, comment écrire du logiciel qui soit sécurisé. Nous disposons de quelques trucs et astuces, et nous savons éviter quelques problèmes évidents, mais nous n'avons aucune théorie [ou modèle] scientifique de la sécurité. C'est encore de la magie noire et, bien que nous apprenions du nouveau à tout moment, nous avons encore beaucoup de chemin à faire. Mais à nouveau, la vraie raison reste que la sécurité n'est pas une priorité pour les vendeurs de logiciels. C'est bien plus profitable pour une entreprise de livrer un produit fragile en avance d'un an qu'un produit solide et sécurisé un an plus tard.

Le résultat de ces tendances générales est que les technologies de sécurité s'améliorent lentement, mais pas assez vite pour tenir le rythme d'apparition des nouvelles sources d'insécurités amenées par la complexité croissante des systèmes. Chaque année apporte des modes d'agressions nouveaux, des vers à diffusions plus rapides, et des codes malveillants plus nuisibles. Les produits logiciels —les systèmes d'exploitation comme les logiciels d'application— continuent à présenter de plus en plus de vulnérabilités. Aussi longtemps que les tendances à la croissance de la complexité et à la négligence de la sécurité se perpétuent, la société de l'information [et les réseaux] ("cyberespace") continueront à devenir moins sûrs.

La complexité est quelque chose nous ne pouvons pas changer. La seule chose que nous puissions changer sera de faire de la sécurité une plus haute priorité.

**Le "Cyberterrorisme" ou “le Pearl Harbour Numérique”**

Il y a une tendance très discutée que je ne constate pas: l'augmentation du "cyberterrorisme" [6]. Un essai que j'ai écrit sur cette question est joint en annexe #1. Je crois que les peurs de "cyberterrorisme", ou la vraisemblance d'un “Pearl Harbour Numérique” sont principalement le résultat d’entreprises et d'organismes qui veulent alimenter les peurs des personnes et des médias à la recherche des histoires à sensation. Le vrai terrorisme —celui qui attaque le monde physique à travers l'Internet— est beaucoup plus difficile que ce que la plupart des personnes n’imaginent, et les effets d'attaques sur les réseaux sont loin bien moins terrorisants que l'on pourrait croire. Le "cyberterrorisme" est simplement un problème dont nous ne devons pas [encore] nous soucier.

Ceci ne signifie pas que des menaces à grande échelle dans la société de l'information ("cyberespace") ne sont pas un problème. Une unique vulnérabilité présente dans un produit logiciel très répandu peut affecter des millions de personnes, et une attaque qui exploite cette vulnérabilité peut faire des millions de dollars de dommages du jour au lendemain. Les attaques contre les services courants d'internet, ou contre des services d'informations vitaux ("critical") [ou sensibles] qui utilise[raient] l'Internet pour échanger des données, peut affecter des millions de personnes.

Pendant que des gens surestiment le niveau des risques de "cyberterrorisme", ils sous-estiment le niveau des risques de criminalité sur les réseaux ("cyber-crime"). Aujourd'hui les numéros de cartes de crédit ne sont plus volés un par un dans les porte-monnaie et les portefeuilles; ils sont volés par millions dans des bases de données. La fraude sur internet est une entreprise à grande échelle, et elle continue de croître.

Et un jour, le terrorisme à travers le réseau ("cyberterrorism") deviendra une menace réelle. Les technologies, surtout les technologies liées aux réseaux et systèmes d'information ("cyberespace") évoluent vite et leurs effets sont de grande portée. Tout comme un agresseur inconnu a utilisé le système de courrier physique pour propager le virus du charbon, il est certainement possible qu'un jour, un terroriste puisse imaginer comment tuer un grand nombre de personnes au moyen de l'internet. Mais ce jour n'est pas proche, et le même terroriste aurait probablement gagné beaucoup de temps en tuant le même nombre de personnes par une attaque physique.

**La résistance élastique ("résilience") de l'internet**

En dépit de tous ces risques, l'Internet est raisonnablement sûr face à un risque d'effondrement catastrophique. Aussi faible que soit chacun des composants ou réseaux individuels qui forment l'internet, l'ensemble est étonnamment résistant. Souvent j'ai plaisanté en disant que l'Internet "tombe juste en marche", qu'il est en permanence révisé et amélioré, et que c'est un petit miracle s'il fonctionne tout court.

L'internet a expérimenté des exemples de ce que beaucoup de gens ont à l'esprit quand ils pensent à des attaques ou du terrorisme à grande échelle, mais ce n'était que le résultat d'accidents au lieu de la malveillance. Des ensembles de commutateurs téléphoniques furent arrêtés par des pannes de logiciels, laissant des millions de personnes sans service téléphonique. Des satellites de communications fonctionnèrent mal un moment, coupant temporairement un réseau national de messagers personnels ("pagers"). Le 11 septembre [2001], le World Trade Center s'est effondré sur une bonne partie du réseau de communications du sud de Manhattan. Ce que nous avons appris de ces épisodes est que les effets ne sont pas dévastateurs et qu'ils ne sont que temporaires; les communications peuvent être restaurées rapidement, et les gens s'adaptent jusqu'à leur remise en fonction.

En plus, des événements fortuits sont encore plus dévastateurs que les évènements malveillants. Dans l'exemple le plus proche d'une agression terroriste sur un réseau ("cyberterrorist attack") qui ait existé, Vitek Boden a attaqué un réseau informatique et a fait déverser un million litres de polluant dans un estuaire en Australie. Les dommages ont été nettoyés en une semaine. Quelques mois plus tard, un oiseau a atterri sur un transformateur dans la vallée de la rivière Ohio, en le faisant exploser; cela a déclenché une réaction en chaîne qui a fait déverser à peu près dix fois plus de polluants dans la rivière. Le nettoyage fut beaucoup plus cher et prit sensiblement plus de temps. Même aujourd'hui, des oiseaux

peuvent causer fortuitement de dommages plus significatifs que ceux qui résulteraient d'un effort conscient de quelqu'un qui veut nuire.

**La sécurité et la gestion des risques.**
Les entreprises gèrent des risques. Elles gèrent toutes sortes de risques; les risques en SSI ("cyber risks") n'en sont qu'un de plus. Et il y a beaucoup de manières différentes de gérer des risques. Une entreprise pourrait choisir de réduire les risques au moyen de technologies ou de procédures. Une entreprise pourrait choisir de s'assurer elle-même contre les risques, ou simplement d'accepter le risque lui-même. Les méthodes qu'une société choisit dans une situation donnée dépendent des particularités de cette situation. Et des échecs se produisent régulièrement; beaucoup d'entreprises gèrent incorrectement leurs risques, payent pour leurs erreurs, et persévèrent malgré tout. Les entreprises sont aussi remarquablement résistantes.

Pour prendre un exemple concret, considérons un magasin physique et le risque de vol à l'étalage [ou de démarque d'origine inconnue]. La plupart des épiceries acceptent ce risque comme un coût d'exploitation. Les magasins de vêtements peuvent mettre des étiquettes sur leurs vêtements et des détecteurs aux sorties; ils diminuent le risque au moyen de technologies. Une bijouterie peut diminuer le risque au moyen de procédures: toute la marchandise est enfermée à clef, les clients ne peuvent pas manipuler quoi que ce soit sans être contrôlés, etc. Et cette bijouterie pourra ajouter une assurance anti-vol, un autre outil de gestion des risques.

Une valorisation de la gestion des risques est fondamentale pour la compréhension de comment les entreprises traitent la sécurité informatique. Demandez à n'importe quel administrateur de réseau pourquoi il a besoin de SSI ("cybersecurity"), il pourra vous décrire les **menaces**: les défigurations de sites Web, la corruption et la perte de données en raison suites à des intrusions de réseau, les attaques en déni (refus) de service, les virus, et les chevaux de Troie. La liste de menaces semble sans fin, et elles sont toutes réelles. Interrogez la haute direction sur la SSI ("cybersecurity"), et vous obtiendrez une réponse très différente. Elle va parler de retour sur investissement. Elle parlera des **risques**. Et alors que les menaces en SSI ("cyber threat") sont grandes, les risques le sont beaucoup moins. Ce dont l'entreprise [l'activité économique, "business"] a besoin c'est une sécurité acceptable à un coût raisonnable.

Étant donné la situation actuelle, les entreprises dépensent probablement les bons montants pour la sécurité. Les menaces sont réelles et les attaques sont fréquentes, mais la plupart du temps, il n'en résulte que des désagréments mineurs. Les attaques graves sont rares. Les épidémies sur internet sont rares. Et d'un autre point de vue, les produits de sécurité informatique sont souvent bien moins efficaces que ne l'annoncent leurs publicités. Les technologies changent rapidement, et il est difficile de réduire les risques dans un environnement qui évolue aussi rapidement. Il est souvent plus efficace au même coût de subir les effets maléfiques d'une mauvaise sécurité que de dépenser suffisamment d'argent pour essayer d'améliorer le niveau de sécurité.

**Les effets externes et nos infrastructures sensibles/vitales ("critical" critiques)**
Si les entreprises sont si bonnes en gestion des risques**, pourquoi [alors] ne pas les laisser simplement gérer leurs propres risques?** Les entreprises peuvent décider d'avoir ou non un

garde dans les bureaux du siège, d'installer ou non un système d'alarme dans leurs entrepôts, voir de prendre une assurance anti-kidnapping pour leurs dirigeants clés. Ne devrions-nous pas laisser simplement aux entreprises le choix de leurs options de sécurité fondées sur [la gestion] de leurs risques propres de sécurité? Si elles ne se soucient pas de l'achat et de l'utilisation de logiciels non sûrs, si elles ne se préoccupent pas d'installer correctement les produits de sécurité, si elles n'appliquent pas les bonnes politiques de SSI ("cybersecurity"), pourquoi serait-ce le problème de quelqu'un d'autre? Si elles décident qu'il est moins cher de subir toutes les attaques internet que de s'obliger à améliorer leur propre sécurité, n'est ce pas leur propre affaire?

L'erreur de ce raisonnement est la cause de la convocation de cette audition: les menaces externalisées ("ancillary") pour les infrastructures sensibles et vitales de notre nation. Les risques pour ces infrastructures sont bien plus grands que la somme des risques pour chacune des entreprises prise isolément. Nous avons besoin de nous protéger contre l'attaque d'un militaire ennemi. Nous avons besoin de nous protéger contre un futur où des "cyberterroristes" pourront cibler notre infrastructure électronique. Nous avons besoin de protéger la confiance économique fondamentale dans l'Internet qui est un mécanisme pour le commerce. Nous avons besoin de protéger l'Internet au-delà des risques subis par ses composants individuels. Les entreprises sont bonnes en gestion des risques, mais elles ne vont considérer que leurs propres risques; les risques externes pour nos infrastructure vitales ne seront pas pris en compte.

Un exemple simple est celui des numéros de cartes de crédit. Les bases de données des sociétés sont régulièrement cambriolées [par voie électronique] et des numéros de cartes de crédit sont volés, parfois des centaines de milliers d'un coup. Les entreprises travaillent pour sécuriser ces bases de données, mais pas très dur, parce que la plus grande part du risque n'est pas supporté par ces entreprises. Quand un individu découvre que son numéro de carte de crédit a été volé et a été utilisé frauduleusement ou, même pire, que son identité complète a été volée et a été utilisée frauduleusement, le nettoyage du désordre peut coûter beaucoup de temps et d'argent. L'entreprise sécurise la base de données en s'appuyant sur [la valorisation] de ses risques propres en interne; la base de données n'est pas sécurisée au niveau nécessaire compte-tenu de l[a valorisation] du risque agrégé subi par tous les individus dont les données y sont emmagasinées.

La sécurité des logiciels est un autre exemple. Les vendeurs de logiciels font quelques essais de sécurité sur leurs produits, mais ils sont minimes parce que la plus grande part du risque n'est pas leur problème. Quand une vulnérabilité est découverte dans un produit logiciel, le vendeur répare le problème et distribue une correction, une rustine ("patch"). Cela coûte de l'argent, et quelque mauvaise publicité. Le risque réel est supporté par les entreprises et les personnes et les individus qui ont acheté et utilisé ces produits, et ce risque n'affecte pas autant le fournisseur. Lors la diffusion du ver Slammer SQL sur l'Internet en janvier 2003, les pertes au niveau mondial ont été estimées à des dizaines de milliards de dollars. Mais les pertes pour Microsoft, dont le logiciel contenait la vulnérabilité que le ver Slammer a utilisée en premier lieu, étaient bien inférieures. Comme la plupart des risques pour Microsoft sont externalisés, la sécurité n'est pas une priorité aussi haute pour cette entreprise qu'elle ne devrait l'être.

Ceci nous conduit au problème fondamental de la SSI [**S**écurité de la **S**ociété de l'**i**nformation] ("cybersecurity"): elle a besoin d'être améliorée, mais ceux-là mêmes qui pourraient l'améliorer —les entreprises qui construisent le matériel informatique et produisent

les logiciels informatiques, ainsi que les personnes et les entrepises qui possèdent et administrent les réseaux élémentaires qui forment l'Internet— ne sont pas motivées pour le faire.

***De façon plus détaillée:*** nos ordinateurs et nos réseaux sont non sécurisés, et il y a tout lieu de craindre qu'ils deviendront [encore] moins sécurisés à l'avenir. Les menaces et les risques sont significatifs, et il y a toute raison de croire qu'ils deviendront plus importants à l'avenir. Mais en même temps, puisqu'une bonne partie de ces risques sont externalisés, les fabricants de logiciels et de matériels ne dépenseront pas beaucoup d'argent pour améliorer la sécurité de leurs produits et les propriétaires de réseaux privés ne dépenseront pas beaucoup d'argent pour acheter et installer des produits de sécurité sur leurs réseaux.

Dans la science économique, **une déséconomie externe ("externality")** est un effet d'une décision qui ne fait pas partie du champ du processus de cette décision. La plupart des pollutions, par exemple, sont des déséconomies externes. Une usine prend une décision économique pour la quantité de polluant qu'elle déverse dans une rivière en fonction de ses propres motivations économiques; la santé des personnes qui habitent en aval est une déséconomie externe. Une mère qui bénéficie de l'aide sociale prend la décision d'épouser ou non celui qui cohabite avec elle en partie en fonction de la logique économique [induite par le] système de l'aide sociale; la dégradation sociale de l'institution du mariage est une déséconomie externe. Les risques SSI externes ("ancillary cyberrisks") sont un exemple de déséconomie externe.

***Il y a plusieurs façons de traiter les déséconomies externes.*** Elles peuvent être gérées par un système juridique: les lois et les règlements qui interdisent certaines actions et qui en rendent d'autres obligatoires sont un moyen de gérer les déséconomies externes. Elles peuvent être réincorporées par la fixation de taxes ou de responsabilités, qui, toutes deux, fournissent des incitations économiques pour prendre en compte les déséconomies externes. Parfois, les normes sociales modifient les déséconomies externes. Et ainsi de suite. Le mécanisme spécifique choisi dépendra des choix politiques, mais le but général est de contraindre les diverses déséconomies à devenir internes au champ du processus de décision.

Je crois que ces déséconomies externes sont le problème fondamental de la SSI ([sécurité de la société de l'information] ("cybersecurity"). La sécurité d'un composant particulier de l'Internet peut être assez bonne pour l'organisation qui le gère, mais les effets externes de cette "assez bonne" sécurité peuvent ne pas être suffisants globalement pour la nation. Les infrastructures sensibles et vitales de notre nation deviennent de plus en plus dépendantes d'un internet fonctionnel et sûr, mais il n'y a aucun organisme chargé de maintenir l'internet en fonctionnel et sûr. **Nos logiciels offrent une sécurité très médiocre, et il n'y a pas d'incitation pour améliorer cela.** Nous sommes de plus en plus vulnérables aux attaques qui touchent tout le monde un petit peu, mais personne n'est assez motivé pour le réparer.

**Des recommandations**

Ce problème fondamental de la SSI ("cybersecurity") est beaucoup plus du domaine économique que du domaine technique. Nos infrastructures informatiques [et réseaux] nationales pourraient être beaucoup plus sécurisées, si les incitations économiques étaient mises en place pour ce faire —si les déséconomies externes sont réincorporées, réinternalisées, pour ainsi dire-. Demander aux entreprises d'améliorer leur propre sécurité ne

fonctionne pas. (Nous avons essayé cela à maintes reprises; c'est voué à l'échec.) Essayer de construire un réseau gouvernemental séparé ne marche pas. (L'important dans la société de l'information ("cyberespace") est qu'il y a un seul grand réseau connecté.) Espérer que la technologie améliorera les choses ne marche pas. (Peu importe la qualité de la technologie est si les personnes ne veulent pas l'utiliser.)

Le système économique de base, capitaliste et démocratique est capable d'améliorer la SSI (sécurité de la société de l'information, "cybersecurity"), mais uniquement si les incitations adéquates sont mises en place. Ma recommandation générale est que vous construisiez des règlements et des lois faites pour traiter les déséconomies externes dans les décisions SSI ("cybersecurity") afin que les organismes soient motivés à fournir un niveau plus élevé de sécurité —qui soit proportionné avec la menace contre les infrastructures sensibles et vitales de notre nation— et ensuite que vous vous retiriez pour laisser jouer les mécanismes de l'innovation économique jouer pour résoudre les problèmes et améliorer la sécurité. En particulier:

**1. Terminer les vaines recherches d'un accord consensuel.**
Au long des années, nous avons vu plusieurs projets gouvernementaux de sécurité SSI ("cyberespace") et des stratégies provenir de la Maison Blanche, le dernier est celui cette année [7]. Ces documents souffrent tous d'une incapacité à prendre le risque de blesser n'importe quelle industrie. Dans le tout dernier plan stratégique, par exemple, les premières versions contenaient des mots forts sur la mauvaise sécurité des liaisons sans fil qui ont été enlevées à la demande de l'industrie [du WIFI], qui ne désirait pas apparaître incapable en n'ayant rien fait. Une recommandation que les fournisseurs d'accès à internet fournissent des cloisons pare-feu personnelles ("personal firewalls") à tous leurs clients fut retirée de la même façon, parce que les grands fournisseurs n'ont pas voulu apparaître incapables en ne fournissantt pas déjà une telle fonction de sécurité. Contrairement à beaucoup d'autres processus gouvernementaux, la recherche d'un consensus nuit ici à la sécurité. La SSI ("Cybersecurity") demande des choix difficiles. Ces choix causeront nécessairement des coûts additionnels pour quelques industries et quelques intérêts spécifiques. Aussi longtemps que le gouvernement ne voudra pas contrarier les intérêts d'une partie de ses soutiens industriels, des insécurités gigantesques persisteront.

**2. Tenir pour responsables les fournisseurs : matériel informatique, logiciels, et réseaux .**
J'ai beaucoup écrit sur l'effet des engagements juridiques de responsabilités dans l'industrie informatique [8]; l'un de mes articles est joint en annexe #2. La raison majeure pour laquelle les entreprises raisonnables ne se soucient pas des déséconomies externes résultant de leurs décisions de sécurité —les effets sur les autres de leurs produits et leurs réseaux sans sécurité— est qu'il ne sont pas réellement responsables juridiquement de leurs actions. La responsabilité [des dégâts induits] changera immédiatement [la structure] du rapport entre coûts et bénéfices pour les entreprises, parce qu'elles devront [alors] porter la responsabilité financière pour les risques induits causés à des tiers suite à leurs actions. Avec une mise en place ferme [et claire] des responsabilités, l'intérêt bien compris des fournisseurs de logiciels, et les intérêts de leurs actionnaires, se trouveront dans l'affacetation du temps et des budgets nécessaires pour faire des produits sûrs et sécurisés avant leur livraison. Les intérêts bien compris des entreprises privées, et les intérêts bien compris de leurs actionnaires, seront satisfaits en affectant le temps et les budgets nécessaires pour sécuriser leurs propres réseaux. L'industrie de l'assurance prendra alors le relai et contraindra les entreprises à améliorer leur propre sécurité si elles veulent savoir exercer leurs responsabilités en sécurité à un coût raisonnable. La responsabilité [juridique et financière] est un mécanisme économique

("capitalist") ordinaire pour gérer les déséconomies externes ("externalities"), et ce mécanisme fera plus pour sécuriser les infrastructures sensibles et vitales de notre nation que toute autre action.

**3. Sécuriser vos propres réseaux.** Financez la sécurité des réseaux du gouvernement, à la fois les réseaux internes et les réseaux accessibles au public. N'achetez que des matériels et des produits logiciels sécurisés. Avant de vous préoccuper de la sécurité de tous les autres, faites le ménage chez vous. Ceci ne signifie pas qu'il soit nécessaire de reproduire ce qui est déjà fait dans l'industrie. Le gouvernement est un consommateur de produits informatiques, tout comme une grande entreprise. Le gouvernement n'a pas besoin de développer ses propres produits de sécurité; la sécurité de tous sera mieux servie si le gouvernement achète des produits commerciaux [de sécurité]. Le gouvernement n'a pas besoin de créer sa propre organisation pour identifier et analyser les menaces SSI ("cyber threats"); il est mieux de faire appel à une organisation privée analogue à celles auxquelles les entreprises font appel. Les menaces contre le gouvernement sont les mêmes que les menaces contre tous les autres, et les solutions sont analogues. Le gouvernement américain, en particulier le Departement of Homeland Security, doit utiliser et doit améliorer les ressources qui sont accessibles à tous, puisque tout le monde en bénéficie.

**4. Utiliser votre puissance d'achat pour piloter une augmentation de la sécurité.** Les achats du gouvernement américain peuvent devenir un outil puissant pour piloter la recherche et le développement. Si vous exigez plus de produits sécurisés, les entreprises les fourniront. Normalisez [en vous appuyant] sur quelques-uns des bons produits de sécurité, et forcez les à s'améliorer de façon continue. Il y aura un effet de vague montante qui se produira; une fois que les entreprises livreront des produits conformes aux spécifications de plus en plus exigeantes du gouvernement, les mêmes produits seront mis aussi à la disposition des organismes privés. Le gouvernement américain est un énorme consommateur de matériel informatique, de logiciels, de systèmes, et de services. Et puisque vous utilisez les mêmes produits commerciaux que ceux que tout le monde utilise, ces produits seront améliorés pour le profit de tous. L'argent que vous dépensez pour votre propre sécurité bénéficiera à la sécurité de tous.

**5. Investir dans la recherche en sécurité [des SI]; investir dans la formation à la sécurité.** Comme le marché commence à demander une sécurité réelle, les entreprises ont besoin de trouver comment la fournir. La recherche et la formation sont sur le chemin critique pour l'amélioration de la sécurité des ordinateurs et des réseaux. Ici encore, utilisez votre puissance financière pour améliorer la sécurité pour tous. Les recherches dans ce domaine et la formation dans ce domaine important ont besoin d'être augmentées. Les profits seront supérieurs à tout ce que nous pouvons nous imaginer aujourd'hui.

**6. Poursuivre rationnellement les criminels sur les réseaux (“ cybercrime ”)**
Dans notre société, nous parvenons rarement à résoudre les problèmes de sécurité par les seuls moyens techniques. Nous ne portons pas de gilets pare-balles d'habitude et nous ne vivons pas [encore] dans des forteresses. À la place, nous faisons confiance au système du droit pour poursuivre rationnellement les criminels et servir de moyen de dissuasion pour les crimes futurs. Nous avons besoin de renforcer [les moyens d']application de la loi pour traiter des crimes informatiques véritables. Ceci ne veut pas dire d'incriminer des gosses de seize ans comme des adultes pour des faits qui ne sont à la base que des farces du 21e siècle; cela signifie poursuivre ceux-là mêmes qui commettent de vrais crimes sur l'Internet.

**La conclusion**
Rien de tout cela n'est facile. Chaque entreprise informatique que vous faites venir dans cette salle vous dira que de les rendre responsables [juridiquement et financièrement] est nuisible pour leur industrie. Bien sûr, c'est ce qu'ils vont vous dire; c'est leur intérêt de ne pas être responsables de leurs propres actes.

Le Ministère de la Sécurité Intérieure (Departement of Homeland Security") vous dira qu'ils ont besoin d'argent pour ceci et pour cela dans un programme géant de sécurité de l'État. Bien sûr c'est ce qu'ils vont vous dire; c'est dans leur intérêt d'obtenir le plus gros budget possible. Le FBI va vous dire que des sanctions extrêmement lourdes sont nécessaires pour les adolescents " cyberterroristes " qui ont été pris aujourd'hui; ils font paraître le problème plus terrible qu'il n'est vraiment pour améliorer leur propre image. Si vous voulez aider à améliorer la sécurité de notre nation, vous aller devoir regarder au-delà des intérêts individuels de chacun en direction des meilleurs intérêts de tous.

Les risques en SSI ("cybersecurity") pour notre nation sont plus importants que ceux qu'affronte une entreprise commerciale isolée ou un organisme, et le seul moyen pour gérer ces risques est de les traiter directement. Je recommande avec force que vous mettiez les intérêts de la sécurité SSI ("cybersecurity") de notre nation [bien] au-dessus des intérêts de chaque entreprise privée ou de chacun des organismes du gouvernement. Les déséconomies externes des décisions en SSI ("cybersecurity") prises par des entreprises raisonnables nous causent des dommages à tous. C'est la mission du gouvernement que de prendre en compte le paysage complet et les besoins de toute la société, et de motiver alors convenablement des acteurs pour satisfaire ces besoins.

Merci pour l'opportunité offerte d'exposer devant votre comité aujourd'hui. Ce sera pour moi un plaisir que de répondre aux questions que vous voudrez me poser.

**Références :**
[1] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.
[1a] Bruce Scheier: Secrets et mensonges: la sécurité numérique dans un monde en réseau. Vuibert Informatique ISBN
[2] Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World, Copernicus Books, 2003. ISBN 0-387-02620-7
[3] Computer Security Institute, "2003 CSI/FBI Computer Crime and Security Survey," 2003. http://www.gocsi.com/press/20030528.html
[4] Honeynet Project, :Know Your Enemy: Statistics," 22 July, 2001. http://www.honeynet.org/papers/stats/
[5] Bruce Schneier, "Software Complexity and Security," Crypto-Gram, March 15, 2000. http://www.counterpane.com./crypto-gram-0003.html
[6] Bruce Schneier, "The Risks of Cyberterrorism," Crypto-Gram, June 15, 2003. http://www.counterpane.com./crypto-gram-0306.html
[7] White House, National Strategy to Secure Cyberspace, Feb 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
[8] Bruce Schneier, "Liability and Security," Crypto-Gram, April 15, 2002. http://www.counterpane.com./crypto-gram-0204.html

## Annexe 1
## Les risques du "cyberterrorisme" Bruce Schneier

Réimpression de: Cryptogram, 15 juin 2003.
http://www.counterpane.com/crypto-gram-0306.html

Les menaces de "cyberterrorisme" causent beaucoup d'alertes ces jours-ci. Il nous a été dit de nous attendre à des attaques après le 11 septembre [2001]; que des "cyberterroristes" essaieraient de paralyser notre système de distribution électrique, de mettre hors de service le contrôle de la navigation aérienne et les services d'urgence, d'ouvrir des barrages hydroélectriques ou [encore] d'interrompre des transactions bancaires et des communications. Mais jusqu'à maintenant, rien ne s'est produit. Même pendant la guerre en Irak, qui, par hypothèse, augmentait spectaculairement le [niveau des] risques, rien ne s'est produit. L'imminence de la guerre des réseaux ("cyberwar") fut un gros plouf. Pourtant, il ne faut pas en féliciter notre vigilance sécuritaire; l'alarme a été causée par une mauvaise compréhension des agresseurs et des attaques.

Ces attaques sont très difficiles à réaliser. Les systèmes logiciels qui contrôlent l'infrastructure de notre nation sont pourris de vulnérabilités, mais ce ne sont généralement pas des vulnérabilités du type de celles qui causent des interruptions catastrophiques. Les systèmes sont conçus pour limiter les dommages qui résultent d'erreurs et d'accidents. Ils peuvent repasser en contrôle manuel. Ces systèmes ont été vérifiés dans leurs fonctions; ils ont expérimenté des interruptions causées par des accidents et des catastrophes naturelles. Nous avons connu des coupures globales d'électricité, des coupures de téléphone, et des arrêts d'ordinateurs de contrôle de circulation aérienne. En 1999, une panne de logiciel a mis hors d'usage un système de messagerie personnelle nationale toute une journée. Les résultats auraient pu être gênants, et les ingénieurs ont du passer des jours ou des semaines à travailler dur, mais l'effet général sur la population a été minime.

Le souci est qu'un terroriste puisse causer un problème plus sérieux qu'une catastrophe naturelle, mais ce genre de chose est étonnamment difficile à réaliser. Les vers et les virus ont causé toutes sortes d'interruptions de réseau, mais c'est arrivé par accident. En janvier 2003, le ver de Slammer de SQL a interrompu 13,000 guichets automatiques du réseau de la Bank of d'America. Mais avant que cela ne se produise, vous ne pouviez trouver un spécialiste de sécurité capable de comprendre que ces systèmes dépendaient de cette vulnérabilité. Simplement nous ne comprenons pas suffisamment les interactions pour prédire correctement quels types d'attaques pourraient causer des résultats catastrophiques, et les organisations terroristes n'en savent pas plus même si elles ont essayé de se payer le service d'experts.

L'exemple le plus proche que nous ayons de ce genre d'évènement vient d'Australie, en l'an 2000. Vitek Boden s'était introduit dans le réseau informatique d'une usine de retraitement des effluents le long de la Côte du Soleil en Australie. Durant deux mois, il a fait fuir des centaines de milliers de litres de boue putride dans les rivières et les parcs proches. Entre autres effets, des eaux noires, l'extinction de la vie aquatique, et une puanteur insupportable dont les habitants se sont plaints. C'est le seul cas connu d'une intrusion dans un système de contrôle numérique avec une intention de causer des dégâts à l'environnement.

En dépit de notre prédilection pour qualifier n'importe quoi de “terrorisme”, ces agressions n'en sont pas. Nous savons ce qu'est le terrorisme. C'est quelqu'un qui se fait exploser dans un restaurant surpeuplé, ou qui fait rentrer un avion dans un gratte-ciel, ce n'est pas infecter des [micro-]ordinateurs avec des virus, contraindre des contrôleurs aériens à gérer en procédure manuelle les avions, ou mettre en panne un réseau de messagers personnels pendant une journée. Cela ne crée que des contrariétés et des irritations, mais aucune terreur.

Ceci est un message délicat pour certains, parce que aujourd'hui toute personne qui cause des dommages importants est étiquetée “terroriste.” Mais imaginons une minute, la direction d'Al-Qaeda, assise quelque part dans sa caverne, préparant la prochaine action de leur “ djihad “ contre les États-Unis. Un des dirigeants sursaute et s'écrie: “j'ai une idée! Nous allons leur couper le courrier électronique ...” Le terrorisme classique —lancer un camion bourré d'explosifs dans une usine d'électricité nucléaire, par exemple— est encore [pour le moment] plus facile et beaucoup plus efficace.

Il y a beaucoup de passionnés/pirates/corsaires ("hackers") informatiques dans le monde —les gamins, surtout— qui aiment jouer à la politique et déguisent leurs propre cirque dans les pièges du terrorisme. Ils s'introduisent dans les ordinateurs de quelque autre pays (généralement en évitant les ordinateurs du gouvernement) et affichent un message politique. Nous avons souvent vu ce genre de chose quand deux pays se querellent: la Chine contre Taïwan, l'Inde contre le Pakistan, l'Angleterre contre l'Irlande, les États-Unis contre la Chine (en 2001 dans la crise de l'avion d'espion américain qui s'était écrasé dans le territoire chinois), les États-Unis et Israël face aux divers pays Arabes. C'est l'équivalent des supporters vandales ("hooligans") exprimant des frustrations nationalistes contre les supporters d'un autre pays pendant un match de football. C'est bas et méprisable, et cela cause de vrais dommages, mais le vandalisme sur les réseaux ("cyberhooliganism") n'est pas du terrorisme sur les réseaux ("cyberterrorism").

Il existe plusieurs organismes qui pistent les attaques sur l'Internet. Dans les derniers six mois, moins de 1% de toutes les attaques provenaient des pays figurant sur la liste du gouvernement américain "Cyber Terrorist Watch List"), alors que 35% d'entre elles provenaient de l'intérieur des États-Unis. La sécurité informatique est encore importante. Les gens surestiment les risques de "cyberterrorisme", mais ils sous-estiment les risques de criminalité sur les réseaux ("cybercrime"). La fraude et l'espionnage sont, eux, des problèmes graves. Heureusement, les contre-mesures qui visaient le "cyberterrorisme" sont identiques et bloqueront aussi des pirates informatiques et des criminels. Si les organismes sécurisent leurs réseaux d'ordinateurs pour de mauvaises raisons, ils auront quand même bien fait.

## Annexe 2
## Responsabilités juridiques et financières et la sécurité
## Bruce Schneier

Réimpression: Cryptogram, 15 avril, 2002.
http://www.counterpane.com./crypto-gram-0204.html

Aujourd'hui, la sécurité informatique est à la croisée des chemins. Elle échoue, régulièrement, et ce, avec des conséqences de plus en plus graves. Je crois qu'elle finira par s'améliorer. Dans le futur proche, les conséquences de l'insécurité s’aggraveront avant que la situation ne s'améliore. Et quand elle s'améliorera, l'amélioration sera lente et se heurtera à une résistance considérable. **Le moteur de cette amélioration sera [la clarification] de la responsabilité**

**[juridique et financière] —tenir les fabricants de logiciels responsables pour la sécurité et, plus généralement, pour la qualité de leurs produits— et le calendrier de cette l'amélioration dépend uniquement de la vitesse à laquelle la responsabilité de la sécurité pénètre dans la société de l'information ("cyberespace")**.

La sécurité des réseaux n'est pas un problème que les technologies peuvent résoudre. La sécurité a une composante technologique, mais les entreprises approchent la sécurité [des SI] comme elles traitent les autres risques de l'entreprise: en termes de gestion des risques. Les organismes optimisent leurs activités pour diminuer le produit "coût x risque"[1], et la compréhension de ces motivations est essentielle pour la compréhension de la sécurité informatique aujourd'hui.

Par exemple, la plupart des organismes dépensent beaucoup d'argent pour la sécurité des réseaux. Pourquoi? Parce que les coûts sont significatifs: le temps, la dépense, le fonctionnalités dégradées, les utilisateurs finaux frustrés. D'autre part, les coûts induits par le fait de négliger de la sécurité [informatique] et d'être victime d'une intrusion sont faibles: l'éventualité d'une mauvaise image et de clients mécontents, peut-être quelques coupures de réseau, aucun dommage n'est permanent. Et s'il y a quelques pressions réglementaires, liées à des audits ou des procès en cours, cela ajoute des coûts supplémentaires. Le résultat: un organisme intelligent ne fait que ce que tout le monde fait et rien de plus. `

Le même raisonnement économique explique pourquoi les vendeurs de logiciels ne dépensent pas beaucoup d'effort pour sécuriser leurs produits. Les coûts [nécessaires] pour ajouter de la bonne sécurité sont significatifs —de grandes dépenses, une réduction des fonctions, des livraisons de produit retardées, les utilisateurs gênés— alors que les coûts induits si on néglige la sécurité sont mineurs: quelques atteintes à l'image, et peut-être quelques utilisateurs passant aux produits de la concurrence. **Tout vendeur intelligent de logiciels parlera beaucoup de la sécurité, mais il en fera le moins possible**.

Pensez aux raisons du succès des cloisons pare-feu ("firewalls") sur le marché. Ce n'est pas dû à leur efficacité; la plupart des cloisons pare-feu ("firewall") sont si mal installées qu'elles ne sont pas efficaces, et il y a beaucoup de produits de sécurité plus efficaces qui n'ont jamais connu un grand succès. Les cloisons pare-feu sont partout parce que les inspecteurs/auditeurs ont commencé à exiger des cloisons pare-feu. Cela a changé l'équation de coût pour les entreprises. Le coût additionnel d'une cloison pare-feu était la charge de l'achat et de l'utilisation, mais le coût de ne pas avoir une cloison pare-feu était de faire échouer un audit. Et même pire, une société sans une cloison pare-feu pourrait être accusée de ne pas suivre les meilleures pratiques de l'industrie au cours d'un procès. Le résultat: tout le monde a une cloison pare-feu, que ce soit bon ou pas.

La sécurité des réseaux est un problème d'entreprise, et la seule façon de le gérer, est de se focaliser sur les objectifs et motivations opérationnelles. Nous avons besoin de changer la structure des coûts; les besoins de sécurité doivent affecter le résultat d'une organisation d'une façon simple et évidente. Pour que la sécurité informatique s'améliore, le PDG doit s'en occuper. Pour que le PDG s'en occupe, il faut que cela touche le prix de l'action et [donc] les actionnaires.

[1] NdT trop sommaire : [coût de la protection + (coût de l'impact) x (potentialité du risque)] est plus exact

J'ai un programme en trois étapes vers l'amélioration de la sécurité des ordinateurs et des réseaux. Aucune des étapes n'a à voir avec les technologies; elles ont toutes à voir avec l'activité de l'entreprise ou de l'organisme, la science économique, et les personnes.

**Étape un: Rendre [les acteurs] plus responsables**.
C'est essentiel. Aujourd'hui, il n'y a pas de vraies conséquences si on a une mauvaise sécurité, ou des logiciels de mauvaise qualité quels qu'ils soient. En fait, le marché récompense la mauvaise qualité. De façon plus précise, il récompense des livraisons hâtives [même] au prix de pratiquement toute qualité. Si nous voulons que les PDG affectent des ressources significatives à la sécurité —et surtout la sécurité de leurs clients— ils doivent être tenus pour responsables des mauvais traitements des données de leurs clients. Si nous voulons que les fournisseurs de logiciels diminuent les fonctions, allongent les cycles de développement, et investissent dans les procédés de développement de logiciel sûrs, ils doivent être tenus pour responsables des [faiblesses et] vulnérabilités de sécurité de leurs produits.

Le législateur pourrait imposer des responsabilités à l'industrie informatique [et réseaux], en contraignant les fabricants de logiciels à vivre avec des lois de répartitions des responsabilité pour les produits analogues à celles qui touchent d'autres industries. Si les fabricants de logiciels fournissaient un produit défectueux, ils seraient tenus responsables pour les dommages. Même sans ce type de lois et de règlements, les tribunaux pourraient commencer à imposer des sanctions en responsabilité aux fournisseurs et aux utilisateurs de logiciels. Cela commence à se produire. Un juge américain a contraint le " Department of Interior " à isoler son réseau, parce qu'il ne pouvait garantir la sécurité des données sur les Indiens d'Amérique dont il avait la charge. Plusieurs cas ont eu pour résultat des sanctions contre des entreprises qui ont utilisé des données de clients en violant leurs engagements de protection des données ("privacy promises"), ou qui ont recueilli des données en trompant ou fraudant. Des juges ont produit des assignations contraignantes contre des entreprises aux réseaux peu sûrs qui sont utilisées comme vecteurs d'attaques contre d'autres.

Pourtant cela avance, et [la clarification de la répartition] des responsabilités change tout. Actuellement, il n'y a aucune raison pour une entreprise de logiciels de ne pas offrir [encore] plus de fonctions, et plus de complexité. La prise de responsabilités contraindrait les entreprises de logiciels à réfléchir à deux fois avant de modifier quelque chose. La prise de responsabilité conduit les entreprises à protéger les données qu'on leur confie.

**Deuxième étape: permettre de aux acteurs de transférer leurs responsabilités.**
Ceci arrivera automatiquement, parce que c'est que font les assureurs. L'industrie de l'assurance transforme les risques qui sont des coûts variables en dépenses fixes. Elle va se placer dans l'assurance de la société de l'information ("cyberassurance") avec utilisant les grands moyens. Et quand elle le fera, elle pilotera l'industrie informatique de sécurité... tout comme elle pilote l'industrie de sécurité dans le monde du ciment et de la brique.

Une entreprise n'achète pas de sécurité pour ses entrepôts —les serrures fortes, les fenêtres à barreaux, ou un système d'alarme— pour se sentir plus sûre. Elle achète de la sécurité parce que ses primes d'assurance diminuent. La même chose se vérifiera pour la sécurité informatique. Une fois que suffisamment de polices sont souscrites, les assurances commenceront à différentier les primes en fonction des différents niveaux de sécurité. Même sans loi sur [la clarification des] responsabilité, le PDG commencera à noter les changements de ses primes d'assurance. Et une fois que le PDG commence à acheter les produits de sécurité en fonctions de ses primes d'assurance, l'industrie de l'assurance disposera d'un

pouvoir énorme sur le marché. Elle va déterminer quels sont les produits de sécurité universels, et ceux qui sont marginaux. Et puisque les sociétés d'assurance payent pour la véritable responsabilité, elles ont une grande motivation pour être rationnelles dans leurs analyses des risques et de l'efficacité des produits de sécurité.

Les entreprises de logiciel en prendront note, et augmenteront la sécurité afin d'obtenir des primes d'assurance abordables avec leurs produits .

**Étape trois: Fournir des mécanismes de réduction des risques.**
Ceci arrivera automatiquement, et sera entièrement piloté par le marché, puisque l'industrie de l'assurance le veut. De plus, elle veut que cela soit fait dans des modèles normalisés qui puissent être réutilisés pour construire des polices/*politiques*[2]. Elle va examiner [les organisations et] procédés de sécurité: les processus de développement de logiciels sûrs avant livraison des systèmes, et les processus de protection, de détection, et de réponse pour les réseaux et les systèmes d'entreprises. Et de plus en plus, elle ira examiner dans la direction de services sous-traités.

L'industrie de l'assurance préfère la sous-traitance en sécurité, parce qu'elle peut écrire des politiques de sécurité et souscrire des polices d'assurances dans cette zone. C'est beaucoup plus facile de concevoir l'assurance d'une série normalisée de services de sécurité livrés par un fournisseur externe que d'être obligé d'adapter une politique/*police* pour chaque réseau spécifique.

**En fait, ce n'est pas un programme en trois étapes.** C'est un programme en une étape avec deux conséquences inévitables. Renforcer la prise de responsabilité, et tout en découlera. Cela doit se faire.

Une grande part de la sécurité d'internet est un bien commun: un domaine utilisé par une communauté comme un tout. Comme tout bien commun, le maintenir en fonctionnement bénéficie à tous, mais n'importe quel individu peut tirer profiter de son exploitation. (Penser au système de la justice pénale dans le monde réel.) Dans notre société, nous protégeons nos biens communs —notre environnement, nos conditions de d'hygiène et sécurité au travail, la sécurité alimentaire et celle des médicaments, l'ordre public dans les rues, les pratiques comptables saines— en renforçant par la loi ces biens [communs] et en rendant les entreprises responsables pour toutes les prises d'avantages injustifiées en utilisant ces biens communs. Ce mode de raisonnement est ce qui fait que les ponts ne s'écroulent pas, que l'air et l'eau sont propres, et les restaurants respectent les règles d'hygiène. Nous ne vivons pas dans une société du type "acheteur méfie toi" (“ Buyer beware ”); nous tenons les entreprises pour responsables quand elles tirent avantage des acheteurs.

Il n'y a aucune raison pour traiter autrement les logiciels que d'autres produits. Aujourd'hui, quand Firestone produit un pneu avec une seule erreur système, il est tenu pour responsable, et Microsoft peut produire un système d'exploitation avec de nombreuses erreurs de système découvertes chaque semaine et ne pas être tenu pour responsable. Ceci n'a pas de sens et c'est la première raison pour laquelle la sécurité [des SI] est si mauvaise aujourd'hui.

[2] NdT : jeu de mot sur la confusion polices d'assurances et politiques de sécurité = policy