Non classifié **DSTI/ICCP/REG(2003)8/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **24-Sep-2004**

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

DSTI/ICCP/REG(2003)8/FINAL
Non classifié

Annule & remplace le même document du 29 juin 2004

Groupe de travail sur la sécurité de l'information et la vie privée

SYNTHÈSE DES RÉPONSES A L'ENQUÊTE SUR LA MISE EN ŒUVRE DES LIGNES DIRECTRICES DE L'OCDE RÉGISSANT LA SÉCURITÉ DES SYSTÈMES ET RÉSEAUX DE L'INFORMATION : VERS UNE CULTURE DE LA SÉCURITÉ

www.oecd.org/sti/security-privacy

JT00169910

Français - Or. Anglais

AVANT-PROPOS

Ce rapport présente les résultats de l'interprétation des réponses reçues de la part de 22 pays membres à l'*Enquête sur la mise en oeuvre des Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*, qui a été distribuée en juillet 2003. L'objectif de ce rapport est de mieux connaître les mesures effectuées par les pays membres pour la mise en œuvre de ces Lignes directrices.

Ce rapport a été preparé par le Sécretariat de l'OCDE sur la base des réponses et commentaires des pays membres. Le Comité de la politique de l'information, de l'informatique et des communications a déclassifié ce document le 10 juin 2004.

Ce rapport est publié sous la responsabilité du Secrétaire général de l'OCDE.

TABLE DES MATIÈRES

SYNTHÈSE DES RÉPONSES A L'ENQUÊTE SUR LA MISE EN ŒUVRE DES LIGNES DIRECTRICES DE L'OCDE RÉGISSANT LA SÉCURITÉ DES SYSTÈMES ET RÉSEAUX DE L'INFORMATION : VERS UNE CULTURE DE LA SÉCURITÉ

Finalité et objectifs

Estimant qu'un plan d'action coordonné était essentiel à la mise en œuvre efficace des *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* (« Lignes directrices sur la sécurité ») adoptées en 2002, les pays membres de l'OCDE ont entériné le « Plan d'application des Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information »[1] (« Plan d'application de l'OCDE ») et l'ont publié en janvier 2003. Conformément à ce Plan, un questionnaire d'enquête a été distribué aux pays membres en juillet 2003 pour dresser le bilan des mesures qu'ils avaient prises depuis la publication des Lignes directrices en août 2002.

Structure et contenu de l'enquête

Le questionnaire d'enquête suivait la structure du Plan d'application de l'OCDE.

Il comportait 24 questions portant sur les domaines suivants :

1ère partie. Missions du secteur public

A. Prérogative du gouvernement visant la politique des pouvoirs publics
B. Diffusion en direction d'autres parties prenantes et soutien de ces dernières
C. Le secteur public en tant que propriétaire et exploitant de systèmes et réseaux d'information
D. Le secteur public en tant qu'utilisateur de systèmes et réseaux d'information

2ème partie. Missions des entreprises et de la société civile

A. Les entreprises en tant que propriétaires, exploitants et/ou utilisateurs de systèmes et réseaux d'information
B. La société civile en tant qu'utilisateur de systèmes et réseaux d'information.

Le questionnaire distribué aux pays membres devait être retourné avant la mi-août 2003. Aux fins de comparaisons, les réponses devaient rendre compte des progrès accomplis jusqu'au 31 juillet 2003.

Le Groupe de travail sur la sécurité de l'information et la vie privée a convenu à sa 15e réunion, qui s'est tenue le 15 octobre 2003 à Oslo, que les pays membres qui n'avaient pas encore répondu à l'enquête le feraient avant le 14 novembre 2003, et que ceux qui y avaient répondu vérifieraient l'interprétation des informations communiquées et feraient parvenir leurs modifications au Secrétariat. Depuis lors, le Secrétariat a reçu huit nouvelles réponses de la part de pays membres. Par ailleurs, deux autres ont mis à jour leurs réponses à l'enquête. Les informations reçues ont été intégrées au présent document.

On trouvera la liste des questions à l'annexe A.

Réponses à l'enquête

Vingt-deux pays membres ont répondu à l'enquête : Allemagne, Australie, Autriche, Belgique, Canada, Corée, Danemark, Espagne, États-Unis, Finlande, France, Hongrie, Italie, Japon, Mexique, Norvège, Pays-Bas, Portugal, République slovaque, République tchèque, Royaume-Uni et Suède.

La plupart des questions de l'enquête étaient ouvertes et invitaient, le cas échéant, des commentaires. Étant donné leur diversité, les réponses des pays membres ont fourni une série d'exemples illustratifs, plutôt qu'une liste exhaustive, des mesures nationales. Il convient de voir dans les observations générales présentées ci-après, ainsi que dans la synthèse des réponses, une *interprétation* des informations obtenues.

Observations générales

Dans l'ensemble, les pays qui ont répondu à l'enquête ont effectivement pris en mains le développement d'une culture de la sécurité. En effet, de très nombreuses réponses positives ont été apportées à la plupart des questions qui demandaient aux pays membres s'ils avaient pris des mesures, conformément au Plan d'application de l'OCDE. Les réponses détaillées offrent des exemples illustratifs des mesures ou des programmes présentant un intérêt pour la mise en œuvre efficace des Lignes directrices sur la sécurité. Cet exercice est également utile en ce qu'il permet d'identifier les domaines qui ont reçu un degré de priorité élevé et ceux dans lesquels les pays membres pourraient intensifier leurs efforts. Le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) peut s'appuyer sur ces résultats pour élaborer un plan d'action en vue d'encourager le développement d'une culture de la sécurité et d'établir des priorités pour les diverses composantes du plan.

Degré de priorité élevé

Les pays qui ont répondu semblent à ce stade avoir accordé la plus haute priorité à la mise en place ou à l'amendement du cadre d'action national et à l'application des principes stratégiques des Lignes directrices sur la sécurité, notamment ceux de « sensibilisation » et de « réaction ».

- ***Mesures publiques nationales***
  - **Tous** ont élaboré une politique nationale en matière de sécurité des systèmes et réseaux d'information ou sont en train de le faire. **Tous** reconnaissent l'intérêt des Lignes directrices sur la sécurité et s'en servent comme cadre d'action de référence.
  - **La plupart** des pays ayant répondu ont promulgué un éventail complet de mesures pour combattre la cybercriminalité.

- ***Sensibilisation, éducation et formation***

  Ces domaines semblent être ceux que privilégient les pays membres en termes d'application des Lignes directrices sur la sécurité.
  - **Tous** les pays, sauf un, ont pris des mesures de sensibilisation et bon nombre d'entre eux ont accueilli des manifestations (conférences, etc.), créé des sites Web et publié de la documentation.
  - **Plusieurs** ont fait état d'initiatives intéressantes, comme la création d'un programme de certification professionnelle en sécurité des TI (technologies de l'information) et la formation correspondante ou le ciblage des cadres supérieurs et des nouveaux employés.

- **Quelques-uns** ont orienté leurs efforts sur des populations particulières : les jeunes, le grand public, les professionnels des TI ou les petites et moyennes entreprises (PME).

- ***CERT (Computer Emergency Response Team)***

  - **La plupart** des pays ayant répondu appuient la création et l'utilisation de sites inspirés des CERT. Certains rendent compte de la mise en place de CERT pour l'Administration, ou d'initiatives de cette nature destinées aux PME et/ou au grand public.

Degré de priorité inférieur

Les pays ayant répondu semblent avoir attaché, à ce stade, moins d'attention aux questions suivantes :

- ***Pratiques exemplaires***

  - **Beaucoup** de pays ont rendu compte de programmes destinés à encourager l'élaboration et l'échange de pratiques exemplaires.

- ***Partenariat entre parties prenantes***

  - **Quelques-uns** ont signalé la mise en place de partenariats entre les secteurs public et privé pour traiter le problème de la sécurité des systèmes et réseaux d'information.

- ***Normes***

  - Même si le questionnaire ne portait pas particulièrement sur l'utilisation de normes internationales, **quelques** pays ont mentionné la norme ISO/IEC 15408[2] et/ou la norme ISO/IEC 17799/BS7799[3] parmi les outils employés pour établir des règles en matière d'achats publics de TI ou pour évaluer la conformité des systèmes publics selon les principes d'« évaluation des risques », de « conception et mise en œuvre de la sécurité », de « gestion de la sécurité » et de « réévaluation » des Lignes directrices sur la sécurité.

Besoin d'informations supplémentaires

- ***Surveillance de l'utilisation des systèmes et des réseaux d'information***

  - Les réponses concernant la façon dont les pays membres veillent à ce que leur utilisation des systèmes et des réseaux d'information soit conforme aux Lignes directrices ont été assez générales. **La majorité** ont mentionné la mise en place d'une politique nationale de sécurité des systèmes et réseaux d'information ou de directives conformes aux Lignes directrices. **Plusieurs** ont fait état d'un organisme national chargé de suivre et/ou de vérifier l'application des mesures de sécurité des TI. **Un pays** a signalé qu'un audit indépendant annuel était imposé à tous les organismes. D'autres détails sur les moyens employés par les pays membres pour assurer la compatibilité de l'utilisation des systèmes et réseaux d'information avec la politique nationale et les Lignes directrices sur la sécurité pourraient s'avérer utiles pour les activités ultérieures concernant l'application de ces Lignes directrices.

  - Aucune question ne portait en soi sur les effets des mesures adoptées (par exemple, le nombre d'exemplaires des Lignes directrices sur la sécurité imprimés et/ou distribués ou le nombre de téléchargements de la version électronique ; ou le nombre de personnes visées et touchées par les campagnes de sensibilisation et les conséquences mesurables de cette opération). Il serait intéressant d'obtenir ces informations en vue d'études ultérieures sur l'application des Lignes directrices sur la sécurité.

Mesures envisageables pour favoriser le développement d'une culture de la sécurité

Le GTSIVP pourrait maintenant envisager des mesures visant à assurer le suivi et la coordination d'une application uniforme des Lignes directrices sur la sécurité afin de stimuler le développement d'une culture mondiale de la sécurité. Une priorité pourrait consister à renforcer la coopération et la collaboration internationales dans les domaines qui ont jusqu'ici moins retenu l'attention et de favoriser l'échange d'expériences concrètes et de pratiques exemplaires entre les participants, ainsi qu'avec les pays non-membres. A titre d'exemple, les pays membres pourraient approfondir leur mise en œuvre des neuf principes des Lignes directrices. L'application plus poussée du principe de « gestion de la sécurité » (ou des principes du cycle de vie de la sécurité) qu'elles contiennent faciliterait l'échange d'informations sur les pratiques, mesures et procédures au niveau fonctionnel. Les pays membres pourraient aussi décider d'allouer plus de temps et de moyens à l'enrichissement et à l'entretien des informations fournies sur le site Web « *Culture of Security* » de l'OCDE.

Plusieurs moyens sont envisageables à ces fins : procéder à d'autres opérations de communication d'informations et de collecte de données, conduire des missions exploratoires ou organiser des examens par les pairs. Pour ce dernier exercice, le GTSIVP devra définir la façon de procéder en ce qui concerne : *i)* le fondement ; *ii)* l'ensemble convenu de principes, normes et critères au regard desquels examiner la politique et les pratiques de chaque pays ; *iii)* la désignation d'acteurs auxquels il incombe de mener à bien l'examen ; *iv)* l'ensemble de procédures conduisant à l'élaboration du résultat final.

Synthèse des réponses

Cette synthèse comprend pour chaque question de l'enquête un court paragraphe de commentaires interprétatifs (*en italique*) suivi d'éléments factuels.

I. Missions du secteur public

Diffusion et traduction des Lignes directrices sur la sécurité (Q1-Q3)

Tous les pays ayant répondu ont pris des dispositions pour diffuser les Lignes directrices sur la sécurité, essentiellement par les moyens habituels : imprimés, transmissions électroniques ou affichage sur des sites Web. Quelques pays ont déclaré les avoir mises à la disposition du public au travers de communiqués de presse, de la télévision ou de CD-ROM. Outre les versions anglaise et française, les Lignes directrices sont disponibles en onze langues.

La diffusion des Lignes directrices sur la sécurité a été notamment assurée par les moyens suivants :

- Édition imprimée : Australie, Canada, Corée, Danemark, États-Unis, Finlande, Hongrie, Japon, Mexique, Norvège, Pays-Bas, République tchèque, Royaume-Uni, Suède.
- Support électronique : Australie, Autriche, Belgique, Canada, Corée, Finlande, Hongrie, Italie, Japon, Mexique, Norvège, Pays-Bas, Portugal, République slovaque, République tchèque, Royaume-Uni, Suède.
- Liens renvoyant au site de l'OCDE ou à des fichiers nationaux : Allemagne, Autriche, Canada, Corée, Espagne, États-Unis, Finlande, France, Hongrie, Italie, Japon, Mexique, Norvège, Pays-Bas, Portugal, République tchèque, Royaume-Uni, Suède.
- Informations apparentées sur les sites nationaux accompagné soit d'un lien vers les Lignes directrices sur la sécurité, soit de leur texte intégral : Australie (fiche d'information par

questions/réponses), Autriche, Belgique, États-Unis, France (guide sur les Lignes directrices), Hongrie, Japon, Norvège, Portugal.

- Autres moyens : Allemagne, États-Unis et Suède (communiqué de presse), Japon (communiqué de presse, présentation télévisée, brochures), Mexique (réseau du cybergouvernement).

Sur le plan de la traduction, les Lignes directrices régissant la sécurité ont été diffusées en 12 langues, qui couvrent pratiquement toutes les langues des pays ayant répondu à l'enquête : allemand, coréen, espagnol, finnois, hongrois, italien, japonais, néerlandais, norvégien, portugais, slovaque et tchèque. Une traduction en suédois est en cours.

A. Prérogative du gouvernement visant la politique des pouvoirs publics

Politiques nationales (Q4, Q5)

Tous les pays qui ont répondu ont élaboré une politique nationale en matière de sécurité des systèmes et réseaux d'information ou sont en train de le faire. Ces politiques comportent souvent un cadre particulier pour la sécurité des systèmes et réseaux d'information des administrations publiques ou la protection d'infrastructures critiques. Tous reconnaissent l'intérêt des Lignes directrices et les utilisent comme cadre d'action de référence. En termes de priorités, quelques-uns ont mentionné la mise en place d'une culture de la sécurité, la recherche et le développement et la coopération internationale.

Les pays font état des réalisations suivantes :

- Élaboration d'une politique nationale de sécurité des systèmes et réseaux d'information dans le cadre d'une politique nationale plus vaste portant sur la société de l'information : Australie, France, Japon, Pays-Bas.
- Élaboration d'une politique nationale particulière sur la sécurité des systèmes et réseaux d'information : Corée, Finlande, Hongrie, Norvège.
- Établissement de cadres spécifiques pour les politiques concernant leurs systèmes et réseaux d'information de l'administration : Autriche, Canada, Espagne, Finlande, Italie, Japon, Royaume-Uni; et/ou la protection des infrastructures critiques : Australie, États-Unis, France, Japon, Royaume-Uni.
- Élaboration d'une politique nationale en cours : Belgique, Danemark, Portugal, République slovaque, République tchèque, ou en projet : Allemagne.

Tous les pays ayant répondu voient dans les Lignes directrices sur la sécurité un cadre d'action de référence. Le Danemark a aussi mentionné les documents d'orientation de l'Union européenne (UE) sur les systèmes d'information et la sécurité des réseaux.

L'Australie a rendu compte d'activités d'appui au sein de la Coopération économique Asie-Pacifique (APEC) et d'autres instances pour aider à l'application des Lignes directrices sur la sécurité, par exemple l'aide à l'élaboration du Projet d'APEC pour la législation sur la cybercriminalité et le développement des moyens d'exécution *(APEC Cybercrime Legislation and Enforcement Capacity Building Project).*

Mesures pour lutter contre la cybercriminalité (Q6, Q7)

La plupart des pays ayant répondu ont édicté un jeu complet de mesures pour lutter contre la cybercriminalité. Les plus fréquemment adoptées sont, par ordre décroissant : la désignation d'unités nationales responsables de la cybercriminalité ; des dispositions afin de mettre en place une institution de type CERT ; des dispositions en vue d'établir des points de contact internationaux d'assistance en haute technologie ; des mesures particulières pour la collecte de preuves de la cybercriminalité et le resserrement de la coopération entre les organismes d'application de la loi et les entreprises en ce qui concerne la sécurité des systèmes et réseaux d'information. Ces mesures sont généralement aussi complètes que celles de la Convention du Conseil de l'Europe sur la cybercriminalité et compatibles avec elle.

Les mesures destinées à combattre la cybercriminalité comprennent :

- La désignation d'unités nationales responsables de la cybercriminalité : Allemagne, Australie, Autriche, Belgique, Corée, Espagne, Finlande, France, Hongrie, Italie, Japon, Mexique, Norvège, Pays-Bas, République tchèque, Royaume-Uni, Suède.
- Des mesures particulières pour la collecte de preuves de la cybercriminalité: Allemagne, Australie, Autriche, Belgique, États-Unis, Finlande, France, Italie, Mexique, Norvège, Pays-Bas, Royaume-Uni. Le Japon est en train d'élaborer des mesures de cette nature. Le CTRC coréen (*Cyber Terror Response Center)* surveille les sites Web qui diffusent du contenu illégal destiné aux adultes.
- Des mesures législatives telles que la conservation des données de trafic pour appuyer les mesures d'application de la loi afin de lutter contre la cybercriminalité : Australie, France, Italie, Pays-Bas, Royaume-Uni. La Finlande, la Corée et le Japon préparent actuellement de telles mesures. La loi suédoise prévoit la rétention volontaire des données de trafic par les FAI sur une période pouvant aller jusqu'à douze mois.
- Des dispositions pour mettre en place des institutions, publiques ou privées, qui échangent des évaluations des risques et des vulnérabilités (sur le modèle des CERT nationaux) : Allemagne, Australie, Autriche, Belgique, Canada, Corée, Espagne, Finlande, France, Hongrie, Italie, Japon, Mexique, Norvège, Pays-Bas, Royaume-Uni, Suède.
- Une coopération entre les pouvoirs publics et les entreprises dans les domaines de la sécurité des systèmes et réseaux d'information et de la lutte contre la cybercriminalité, notamment des accords portant sur la sécurité des systèmes et réseaux d'information entre les organismes chargés de l'application de la loi et les entreprises : Allemagne, Australie, Autriche, Corée, Finlande, Italie, Japon, Mexique, Norvège, Pays-Bas, Royaume-Uni, Suède.
  - Une coopération avec les entreprises en ce qui concerne la protection des infrastructures critiques : Australie, Japon.
  - Une collaboration avec les FAI (fournisseurs d'accès Internet) : Allemagne, Autriche, Corée, Mexique.
  - Une coopération avec les entreprises dans le cadre d'un « Conseil sur la sécurité de l'information » : Suède.
- La désignation de points de contact internationaux d'assistance en haute technologie : Allemagne, Australie, Autriche, Corée, États-Unis, Finlande, France, Italie, Japon, Mexique, Norvège, Pays-Bas, Royaume-Uni, Suède. Des discussions sont actuellement en cours en Belgique quant à la création de tels points de contact.

- D'autres initiatives associées à la coopération internationale :
  - Accords d'assistance mutuelle : Australie, États-Unis.
  - Participation au *Telecommunications and Information Working Group* de l'APEC, offre de formation aux pays non-membres : Australie.
  - Mesures et outils stratégiques mis au point par les organismes pour intensifier la coopération internationale, par exemple des bases de données permettant de mieux détecter les fraudes : États-Unis.

La République tchèque a signalé qu'elle participera au programme de l'UE, *Plan d'action pour un Internet plus sûr*,[4] lorsqu'elle deviendra membre de l'Union européenne en mai 2004.

Les pays ayant répondu à l'enquête jugent les dispositions nationales énumérées ci-dessus aussi complètes que celles de la Convention du Conseil de l'Europe sur la cybercriminalité, et compatible avec elle. La Finlande, la Norvège, le Portugal et la Suède sont en train d'amender leur législation de manière à la mettre en conformité avec la Convention.

B. Diffusion en direction d'autres parties prenantes et soutien de ces dernières

Sensibilisation (Q8)

Tous les pays ayant répondu au questionnaire, sauf un, rendent compte d'opérations de sensibilisation. Les plus fréquemment mentionnées sont les manifestations de type conférence, les sites Web et les publications. On citera parmi d'autres initiatives intéressantes la distribution de plus d'un million de CD-ROM au travers de magazines et de programmes préinstallés sur de nouveaux ordinateurs. Plusieurs pays ont aussi fait état de projets visant des populations particulières, notamment le grand public et les nouveaux utilisateurs de TI, les PME et les jeunes internautes. Un pays a publié un numéro spécial du magazine de bande dessinée « *Donald Duck* » sur l'utilisation sûre de l'Internet, et un autre a créé un portail sur la sécurité des systèmes et réseaux d'information pour les PME.

Les opérations de sensibilisation comprennent les activités suivantes :

- Ateliers, séminaires, formations, conférences et articles et études associés : Allemagne, Australie, Corée, États-Unis, France, Hongrie, Japon, Mexique, Pays-Bas, Portugal, République tchèque.
- Sites et portails Internet : Allemagne, Australie, Corée, Espagne, États-Unis, Finlande, France, Japon, Pays-Bas, Portugal, Royaume-Uni, Suède.
- Publications, guides, manuels et brochures: Allemagne, Australie, Danemark, États-Unis, Finlande, France, Pays-Bas, Suède.
- Médias : Corée, États-Unis, Finlande, Pays-Bas.
- CD-ROM : Allemagne.
- Lignes directrices/recommandations, méthodologies, pratiques exemplaires : Finlande, France, Hongrie.
- Participation à des associations, fédérations, sociétés (comme l'Institut Fraunhofer) : Allemagne.
- Création d'un comité responsable de la sensibilisation : Italie.
- Lettres d'information : Pays-Bas.

- Permanences téléphoniques : États-Unis.
- Concours d'idées « Sécurité des systèmes et réseaux d'information » destiné au grand public : Corée.
- Tournées de présentation : Australie.
- Dans le cadre de la mise en œuvre de son programme de cybergouvernement, l'Autriche va lancer une opération « confiance et sécurité » en 2004.
- A ce stade, la République slovaque n'a pas engagé de programmes et d'opérations dans ce domaine.

Plusieurs pays ont mis au point des produits destinés à des populations particulières :

- Citoyens et nouveaux usagers des TI et de l'Internet : Allemagne (le contenu d'un site Web est aussi préinstallé sur les nouveaux ordinateurs personnels Fujitsu-Siemens); Japon; Pays-Bas; Royaume-Uni, Suède ; et États-Unis (sites Web destinés aux usagers finaux).
- Entreprises : le Canada a présenté les lignes directrices, pendant leur rédaction et après leur adoption, aux membres de l'Association canadienne de la technologie de l'information (ACTI), qui représente 1 300 entreprises du secteur des technologies de l'information et des communications et tient des consultations sur les questions associées à la sécurité avec diverses associations professionnelles.
- PME :
  - L'Australie a créé un programme spécial de sources d'information et un portail de sécurité.
  - Les Pays-Bas ont publié un guide de la sécurité à l'usage des PME.
  - La Suède a diffusé (via un site Web et des publications) des informations sur la sécurité Internet destinées aux PME.
  - Le gouvernement britannique a établi un partenariat avec l'industrie, le « *UK Online for Business* ».
  - Le « *Computer Security Resource Center* » américain gère un programme à l'intention des petites entreprises.
- Jeunes utilisateurs : l'Allemagne a lancé un site Web qui leur est destiné ; les Pays-Bas ont financé un numéro spécial du magazine de bande dessinée « *Donald Duck* » sur l'utilisation sûre de l'Internet. La Corée a lancé un concours de slogans et de posters sur la sécurité des systèmes et réseaux d'information auprès des écoliers des classes élémentaires, intermédiaires et supérieures.

Divers organismes et ministères sont chargés d'organiser des opérations de sensibilisation. On citera par exemple l'Office fédéral pour la sécurité de l'information (Allemagne), le Conseil pour la sécurité des TI (Danemark), le Ministère de la science et de la technologie (Espagne), la *Federal Trade Commission* (FTC, États-Unis) et les *National Institutes of Standards and Technology* (NIST, États-Unis), le Ministère des finances (Finlande), l'Agence de police nationale (Japon), le Ministère du commerce et de l'industrie et le Ministère de la justice (Norvège).

Pratiques exemplaires et partenariats (Q9, Q10)

Bon nombre des pays qui ont répondu disposent de programmes visant à favoriser le développement de pratiques exemplaires et de partenariats entre les parties prenantes. Une initiative intéressante, entre autres, récompense les entreprises qui appliquent les meilleures pratiques en matière de sécurité des systèmes et réseaux d'information. La plupart des pays favorisent par ailleurs l'échange de pratiques exemplaires pour permettre aux usagers de mieux comprendre et de mieux appliquer des mesures de sécurité efficaces et récentes. On citera à cet égard la participation à des ateliers et à des groupes de travail, et/ou leur parrainage. Quelques pays mentionnent la mise en place de partenariats public-privé et le recours à des normes.

On trouvera ci-dessous quelques exemples de programmes visant à favoriser le développement de pratiques exemplaires :

- Élaboration et/ou publication de pratiques exemplaires ou de recommandations : Allemagne, Autriche (secteur public), Corée, États-Unis, Finlande, France, Hongrie, Norvège.
- Mise en place de partenariats public-privé pour réunir des intervenants et des experts de divers domaines afin de réfléchir aux moyens de minimiser les risques associés à l'utilisation de l'Internet (Pays-Bas) ou de fournir aux PME des avis impartiaux sur le commerce électronique et les technologies de l'information et des communications (TIC) (Royaume-Uni). Partenariats avec des groupes et des consortiums et parrainage du Forum des responsables de programmes de sécurité des systèmes et réseaux d'information pour examiner les questions d'intérêt commun (États-Unis).
- Création d'un programme pour récompenser les entreprises qui appliquent des pratiques optimales en matière de sécurité des systèmes et réseaux d'information et d'un Comité pour la pratique de la sécurité des systèmes et réseaux d'information chargé de promouvoir les partenariats entre les participants : Corée.
- Constitution d'un groupe réunissant les spécialistes de la cybercriminalité des différents bureaux du gouvernement fédéral, les prestataires de services, les entreprises et les instituts d'enseignement : Mexique.
- Établissement d'un groupe de travail entreprises-administrations sur l'infrastructure critique : Australie.

L'échange de pratiques exemplaires est favorisé par les moyens énumérés ci-dessus ainsi que par la création de sites Web (Corée, États-Unis, Royaume-Uni), l'organisation d'ateliers et de séminaires (Finlande) et le parrainage (États-Unis).

S'agissant des normes internationales, le Royaume-Uni a fourni le Secrétariat du Groupe d'usagers de la norme BS7799/ISO 17799. Le gouvernement japonais a mis en place un dispositif d'évaluation et de certification fondé sur la norme ISO/IEC 15408 pour aider les usagers des TI à acheter des systèmes et des produits informatiques sécurisés. Il a également établi le Programme d'évaluation de la conformité des systèmes de gestion et le Système d'audit de la sécurité des systèmes et réseaux d'information (tous deux fondés sur la norme SS-ISO/IEC 17799) afin d'améliorer la gestion de la sécurité des systèmes et réseaux d'information. L'Agence suédoise pour l'administration publique a publié des lignes directrices à l'appui des bureaux disponibles 24h/24 et 7 jours/7, qui expliquent l'emploi de la norme SS-ISO.IEC 17799. L'Espagne a financé des études portant sur l'utilisation de la norme ISO/IEC 17799 dans les entreprises espagnoles.

Les États-Unis ont mentionné l'existence de directives élaborées par les associations professionnelles, comme le Comité consultatif économique et industriel (BIAC), la *Business Software Alliance* (BSA) et la *Information Technology Association of America* (ITAA).

Le Danemark va ultérieurement orienter ses efforts sur les pratiques exemplaires. A ce stade, la République slovaque n'a élaboré aucun programme de diffusion et d'échange de pratiques optimales.

Éducation et formation (Q11)

Tous les pays ayant répondu, sauf un, financent des programmes d'éducation et d'information sur la sécurité des systèmes et réseaux d'information. Plusieurs ont fait état d'initiatives intéressantes, comme la création d'un programme de certification professionnelle sur la sécurité des TI et de la formation correspondante, ou de programmes destinés aux cadres supérieurs et aux nouveaux embauchés. A une exception près,[5] aucun exemple d'application pratique des principes d'« éthique » et/ou de « démocratie » dans l'éducation et la formation n'a été donnée.

Outre les outils mentionnés au paragraphe traitant de la sensibilisation, on citera les programmes, informations ou instruments éducatifs sur la sécurité des systèmes et réseaux d'information suivants :

- Programmes visant à intégrer la sécurité des systèmes et réseaux d'information aux programmes éducatifs destinés aux cadres supérieurs et aux nouveaux employés : Finlande.
- Guides et formation correspondante en matière de sécurité des TI : Allemagne, France.
- Programme de certification professionnelle en matière de sécurité des TI et formation correspondante : Japon.
- Aide à la qualification de « responsable de la sécurité de l'information des réseaux » pour les professionnels des TI : Japon.
- Appui à un Atelier annuel qui analyse les tendances actuelles en matière d'enseignement de la sécurité des systèmes et réseaux d'information dans d'autres pays et à la normalisation des programmes d'études des établissements d'enseignement intermédiaire et supérieur et l'avenir de la formation à la sécurité des systèmes et réseaux d'information ; « concours de matériel didactique » destiné aux enseignants des écoles de niveau élémentaire, intermédiaire et supérieur en prélude à la mise en place d'un programme d'études uniforme sur la sécurité des systèmes et réseaux d'information : Corée.
- Modules éducatifs destinés aux écoles primaires et aux collèges et mesures visant à intégrer l'enseignement de la sécurité des systèmes et réseaux d'information au niveau des facultés et universités dans des domaines tels que la gestion de la santé et des entreprises : Norvège.
- Promotion de l'amélioration des programmes de l'enseignement secondaire pour accroître la sensibilité et la connaissance des élèves dans le domaine des TIC : Portugal.
- Outil de sécurité en ligne « *Health Check* » : Royaume-Uni.
- Création et diffusion via Internet d'un dictionnaire sur la sécurité des systèmes et réseaux d'information regroupant un millier de définitions et leurs interprétations : Hongrie.
- Partenariat public-privé : États-Unis (*GetNetWise* – site Web consacré à la sécurité des systèmes et réseaux d'information et à la protection de la vie privée).
- La Hongrie se prépare à conduire une étude sur l'enseignement de l'informatique et le développement de la formation technique traitant des questions de sécurité des systèmes et

réseaux d'information. De nouveaux documents didactiques et les critères d'examen correspondants vont être rédigés sur ce thème. Une formation régulière et obligatoire à la sécurité des TI, destinée aux experts en TI et aux administrateurs de systèmes travaillant pour les administrations publiques, est également en élaboration.

- La France a mis en place un centre de formation pour les besoins de l'administration.
- L'Espagne appuie différents programmes éducatifs portant sur la sécurité des systèmes et réseaux d'information, tant au niveau de l'enseignement informatique de base que de l'université.
- La Belgique a publié des conseils pour la protection contre les virus qui constituent un point de départ pour le développement de mesures d'éducation et de sensibilisation par la future agence Belge pour la sécurité des systèmes et réseaux d'information.
- A ce stade, la République slovaque n'a pas financé de programmes d'enseignement et d'information sur la sécurité des systèmes et réseaux d'information.

Le programme du Danemark pour la sécurité des TI est axé sur l'éducation, mais aucun programme de sensibilisation et de formation particulier n'a été lancé à ce stade.

CERT, « *SysAdmin, Audit, Network, Security* » (SANS), Centres d'analyse et d'échange d'informations (ISAC) et autres sites utiles[6] (Q12)

La plupart des pays ayant répondu financent l'établissement et l'utilisation de sites de type CERT. Certains rendent compte de la création de CERT pour l'Administration ou d'initiatives analogues visant les PME et/ou le grand public. Quelques-uns ont signalé la mise en place d'une structure semblable à l'ISAC ou manifesté leur intérêt à cet égard. Aucun pays n'a particulièrement mentionné de sites de type SANS. Les programmes visant à encourager la coopération internationale dans ce domaine sont évoqués par un petit nombre de pays.

S'agissant des sites de type CERT, les pays font état de ce qui suit :

- Mise en service de sites de type CERT ou coopération avec eux : Allemagne, Australie, Espagne, France, Hongrie, Mexique, Norvège, Portugal, Royaume-Uni, Suède.
- Établissement de CERT réservés à l'Administration : Corée, France, Italie (en cours), Pays-Bas.
- Mise en place de services de type CERT destinés à des populations particulières : Corée (grand public, spécialistes des TI), Pays-Bas (PME). A titre d'exemple, le service d'alerte national néerlandais pour les virus et les incidents ayant trait à la sécurité informatique avertit le grand public et les PME en publiant des alertes sur un site Web et par messages électroniques et SMS, selon la gravité du problème. Une permanence téléphonique permet aux usagers de signaler les incidents.
- Loi en préparation pour rendre obligatoire d'informer le CERT des infractions graves à la sécurité des systèmes et réseaux d'information : Finlande.
- Discussions en cours sur la création d'un CSIRT (Computer Security Incident Response Team) au sein de la future agence nationale pour la sécurité des systèmes et réseaux d'information : Belgique.
- Appui à la coopération des CERT dans la région Asie-Pacifique : Japon.
- Soutien à plusieurs initiatives au niveau international (APEC, OCDE, G8 par exemple) et avec le secteur privé : États-Unis.

Pour ce qui est des sites de type ISAC, l'Australie a appuyé la création de groupes consultatifs sectoriels sur la protection des infrastructures pour favoriser l'échange d'informations entre les propriétaires et les exploitants d'infrastructures critiques. Le Japon finance un « *ISAC Telecom* ». Le gouvernement autrichien est partenaire du CIRCA (*Computer Incidents Response Coordination Austria)* formé par des responsables de réseaux et de la sécurité de FAI et d'autres fournisseurs de réseaux (publics et privés). L'Allemagne précise que même si elle ne dispose pas de mécanisme de cette nature, les organismes compétents s'emploient à promouvoir la coopération nécessaire entre les pouvoirs publics et l'industrie.

L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) créée à l'échelon de l'Union européenne a également été citée parmi les entités susceptibles de jouer un rôle informatif majeur en matière de sécurité des systèmes et réseaux d'information.

Recherche et développement (Q13)

La majorité des pays ayant répondu appuient la recherche et le développement (R-D) pour renforcer la sécurité, mais les méthodes pour fournir cet appui varient d'un pays à l'autre. On relève néanmoins un recours plus fréquent aux programmes de R-D, ainsi qu'à la certification matérielle, logicielle et à celle des auditeurs.

L'aide des pouvoirs publics à la R-D revêt les formes suivantes :

- Programmes de R-D : Australie, Corée, Danemark, Espagne, France, Hongrie, Japon, Norvège, Pays-Bas, République tchèque, Royaume-Uni. A titre d'exemple, le programme de R-D de longue durée des Pays-Bas, Sentinel, a pour objectif de fournir un cadre intégral de conception et de mise en réseau de systèmes sécurisés.
- Certification matérielle/logicielle : France, Italie, Suède.
- Certification des auditeurs : Allemagne.
- Systèmes cryptographiques et solutions matérielles et logicielles, pour les PME par exemple : Allemagne.
- Régime fiscal d'aide à la R-D : Japon.
- Lois visant à consolider le rôle de la R-D en vue d'améliorer la sécurité et d'encourager les pratiques exemplaires : États-Unis.
- Création et financement du Centre autrichien pour une technologie de l'information sécurisée (A-SIT) afin de surveiller les technologies et les risques en matière de sécurité et de conduire des études dans ce domaine : Autriche.

Le Mexique appuie la R-D pour développer les procédures opérationnelles optimales. La Finlande n'a pas de programme autonome d'aide à la R-D dans le domaine de la sécurité des systèmes et réseaux d'information, mais apporte un soutien à l'innovation dans le cadre de son programme global d'assistance.

C. Le secteur public en tant que propriétaire et exploitant de systèmes et réseaux d'information

Politique de gestion de la sécurité de ses propres systèmes et réseaux (Q14, Q15, Q16)

Presque tous les pays ayant répondu ont élaboré une politique, des normes, des recommandations ou des manuels sur la gestion de la sécurité des systèmes et réseaux de leur secteur public. Un exemple intéressant, entre autres, est celui de la mise au point d'un outil d'auto-évaluation et la requête que tous les systèmes soient associés à un plan de sécurité, accrédités et certifiés. Plusieurs pays signalent que la formulation de leur politique de sécurité des systèmes et réseaux d'information publique s'effectue à un niveau centralisé.

Les principes du cycle de vie de la sécurité - « évaluation des risques », « conception de la sécurité », « gestion de la sécurité » et « réévaluation » - sont implicitement ou explicitement pris en compte dans la gestion de la sécurité des systèmes et réseaux publics, le plus souvent au travers de la publication de directives par un organisme national, ou par une politique ou une loi nationales. Un pays signale l'obligation que ces principes soient appliqués conformément à une norme internationale (ISO/IEC 17799/BS7799) et un autre mentionne la possible référence à des normes internationales dans sa future politique sur la sécurité des systèmes et réseaux d'information.

En ce qui concerne la sécurité des systèmes et réseaux publics :

- Tous les pays qui ont répondu ont adopté une politique en matière de gestion de la sécurité des systèmes et réseaux de leur secteur public, ou sont en train de le faire (Belgique, Mexique, Portugal).
- La politique de sécurité est énoncée sous forme de recommandations (Finlande, France), de normes (Danemark), de manuels (Allemagne, Australie, Autriche), de lignes directrices (Corée, Japon) ou de documents de politique de sécurité nationale comme la « *National Strategy to Secure Cyberspace* » des États-Unis.

Les États-Unis ont mis au point un outil d'auto-évaluation que tous les organismes sont tenus d'utiliser, et exige que tous les systèmes publics soient associés à un plan de sécurité, accrédités et certifiés avant d'être pleinement mis en service.

La Belgique travaille à l'élaboration d'une politique nationale pour la sécurité des systèmes et réseaux du gouvernement qui pourrait être basée sur la norme ISO 17799:2002. La mise en œuvre opérationnelle de la politique sera fondée sur les processus de gestion ITIL (*Information Technology Infrastructure Library*).[7]

Presque tous les pays ayant répondu, à l'exception de l'Italie, de la Norvège et de la République slovaque, ont élaboré de manière centralisée des politiques nationales en matière de sécurité des systèmes et réseaux d'information publics ou vont le faire prochainement. Ces politiques sont formulées via la publication d'un document de politique nationale approuvé par le gouvernement ou par le parlement et/ou par la diffusion de directives, de recommandations, de normes ou de manuels à l'intention des administrations publiques. Certains pays soulignent que la mise en œuvre de la politique est décentralisée (Belgique, Canada, Corée, Danemark, France, Hongrie, Japon, Norvège, Pays-Bas, République tchèque, Suède). Trois signalent que leur politique publique à cet égard a été élaborée de façon décentralisée. La Norvège précise que les organismes qui possèdent et exploitent les infrastructures communes ont établi des politiques de sécurité communes à toutes les entités utilisatrices (par exemple un réseau et des services centraux pour les ministères, ou un réseau commun pour les administrations régionales).

L'Australie a mis sur pied un « Groupe de la sécurité de l'information » chargé de fournir aux administrations des renseignements et une assistance sur les questions se rapportant à la sécurité et à l'intégrité des informations officielles. Les principes d'« évaluation des risques », de « conception et mise en œuvre de la sécurité », de « gestion de la sécurité » et de « réévaluation » énoncés dans les Lignes directrices sur la sécurité sont implicitement ou explicitement pris en considération dans les systèmes et réseaux publics de gestion de la sécurité, par différents moyens dont les suivants :

- Directives, recommandations, instruments ou manuels diffusés par les organismes nationaux : Allemagne, Australie, Autriche, Espagne, États-Unis, Finlande, France, Hongrie.
- Organismes spéciaux d'assistance aux organismes en matière de sécurité des systèmes et réseaux d'information (centre d'incidents relatifs aux TI, Agence de gestion des situations d'urgence) : Suède.
- Document de politique nationale : Japon, Pays-Bas.
- Loi nationale : Corée, Finlande.
- Conformité exigée à la norme ISO/IEC 17799/BS7799 : Royaume-Uni.

La politique belge pour la sécurité des systèmes et réseaux d'information actuellement en discussion sera alignée avec les principes mentionnés ci-dessus. L'Italie réfléchit actuellement à la façon de prendre ces principes en compte. Le « Plan de sécurité des TI » du Danemark ne comprend pas ces principes, mais ils seront intégrés au stade de la mise en œuvre.

L'influence du gouvernement sur les autres intervenants (Q17, Q18)

Les pays qui ont répondu ont fourni des réponses très diverses quant à leur manière de donner l'exemple ou de mettre au point des pratiques exemplaires et d'autres améliorations opérationnelles dans l'intérêt de toutes les parties intéressées. La majorité d'entre eux publient des directives. Plusieurs mettent en avant l'échange d'informations entre les organismes publics et les mesures particulières obligatoires. D'autres signalent un certain degré de coopération et d'échange d'informations avec les parties prenantes.

La plupart des gouvernements se servent de leur capacité d'achat pour influencer les autres parties intéressées. La majorité des pays signalent la conformité requise ou recommandée à des normes ou l'existence de directives pour la passation de marchés dans le domaine des TI. Deux pays disposent d'un organisme spécialisé chargé de gérer les achats publics ou d'aider les organismes à choisir leurs produits.

Pour devenir un « propriétaire modèle » et donner l'exemple, et pour mettre au point des pratiques exemplaires et d'autres améliorations opérationnelles dans l'intérêt de toutes les parties prenantes, les pays ont recours aux méthodes suivantes :

- Rédaction et/ou publication de directives, de recommandations, de manuels et de pratiques exemplaires : Allemagne, Australie, Autriche, Danemark, Finlande, Hongrie, Japon, Pays-Bas, Royaume-Uni.
- Échange d'informations entre les organismes publics et/ou actions spécifiques requises de la part des fonctionnaires et des organismes publics, notamment :
  - Mise en place de groupes de travail à différents échelons : Corée, Danemark, Pays-Bas, République tchèque.
  - Établissement d'un comité stratégique de gestion de l'information favorisant une collaboration étroite entre les administrations et obligation pour les organismes publics

d'élaborer des mesures afin de garantir la protection de leurs systèmes informatiques : Australie.

- Mise à jour permanente des usagers de l'Administration et échange entre les ministères : Italie.
- Imposition de mesures spécifiques telles que l'analyse et l'évaluation annuelles de la vulnérabilité ou la désignation d'un responsable de la sécurité informatique dans chaque ministère : Corée.

- Coopération et échange d'information avec les entreprises et les milieux concernés, par exemple :
  - Échange de pratiques exemplaires pendant le déroulement de projets pluriorganismes et publication des conclusions : Finlande.
  - Conformité à la loi : Mexique (Transparence et accès à l'information publique).
  - Échanges avec les milieux intéressés quant à l'expérience acquise dans le cadre de projets (dans la mesure du possible) : Norvège.
  - Mise au point de pratiques exemplaires dans le cadre de partenariats et promulgation de ces pratiques exemplaires pour aider les fournisseurs et les usagers à dialoguer avec les pouvoirs publics : Royaume-Uni.
  - Entretien de contacts avec l'industrie en ce qui concerne la mise au point de pratiques exemplaires et le renouvellement des procédures publiques : États-Unis.
- Mise en œuvre d'un projet de cybergouvernement (Danemark) et développement et promotion de l'accès sécurisé aux services d'administration en ligne (Belgique).
- Création d'organismes spéciaux chargés de donner des avis et de publier des rapports pour apporter une aide à d'autres organismes en matière de sécurité des systèmes et réseaux d'information (Suède), ou de coordonner les mesures en matière de cybergouvernement et d'économie numérique au sein des administrations publiques (France).
- Incitation à utiliser des produits certifiés ou recommandés de norme ISO/IEC 15408 au sein de l'Administration : France, Japon. L'Agence suédoise de gestion des situations d'urgence envisage une étude sur l'utilisation des critères communs en tant que modèle pour les spécifications de sécurité applicables aux achats de produits de sécurité. La Belgique intégrera les bonnes pratiques dans les modèles et standards ayant trait à la gestion opérationnelle de la sécurité informatique.

Pour influencer les autres participants au moyen de leur pouvoir d'achat, les pays qui ont répondu ont déclaré faire appel aux mesures suivantes :

- Conformité requise ou recommandée des achats de TI aux normes internationales comme la norme ISO/IEC 15408/critère commun (Espagne, Japon, Royaume-Uni) ou la norme ITSEC[8] (Royaume-Uni), aux normes nationales (Corée[9], États-Unis, République tchèque), ou à des directives (Finlande).
- Achat exigé ou recommandé de produits certifiés : Allemagne, Australie.
- Désignation d'un organisme spécial pour gérer les achats publics et d'un organisme chargé d'assister les administrations dans le choix des produits : Australie, Royaume-Uni.
- Recours à des obligations ou à des règles contractuelles communes pour les achats de TI : Autriche, Finlande, Hongrie.

- Rédaction et publication d'une documentation commune diffusée par le gouvernement et que certains organismes sont tenus d'utiliser : France.
- Recommandation d'intégrer la part du budget allouée à la sécurité des systèmes et réseaux d'information aux lignes directrices portant sur l'élaboration du budget : Corée.
- Établissement par le gouvernement d'une infrastructure à clé publique afin de sécuriser les communications internes et avec des tiers : Pays-Bas.
- Exiger l'utilisation d'une signature électronique pour répondre en ligne aux appels d'offre : Belgique.
- Coordination des achats de l'administration publique et élaboration d'obligations communes en matière d'achats : Portugal.

La Corée, le Danemark et la Norvège ne se servent pas de leur capacité d'achat pour encourager directement la mise au point de produits plus sûrs. L'Italie examine actuellement cette question.

D. Le secteur public en tant qu'utilisateur de systèmes et réseaux d'information (Q19, Q20)

La majorité des pays ayant répondu veille à ce que leur utilisation des systèmes et réseaux d'information soit conforme aux Lignes directrices sur la sécurité. Plusieurs ont un organisme national qui surveille et/ou vérifie l'application de la politique en matière de sécurité des TI. A l'exception d'un pays, qui signale l'obligation pour tous les organismes d'effectuer un audit indépendant annuel, aucun détail n'a été fourni quant aux moyens employés pour garantir que l'utilisation des systèmes et réseaux d'information par l'Administration est conforme aux politiques nationales et aux Lignes directrices sur la sécurité.

La plupart des pays ont mis en œuvre des programmes et des outils de formation pour sensibiliser leurs employés aux problèmes de sécurité, leur faire prendre conscience de leurs responsabilités personnelles et développer leur aptitude à réagir judicieusement à des incidents de sécurité. Un pays a précisé que la formation des nouveaux employés est obligatoire aux termes de la loi. L'emploi d'outils de cyberformation pour la formation de fonctionnaires locaux mérite d'être mentionné, de même que l'outil d'auto-évaluation fourni par un autre gouvernement.

Les pays veillent à ce que leur utilisation des systèmes et réseaux d'information soit conforme aux Lignes directrices sur la sécurité par les moyens suivants :

- Ils fondent leur politique nationale en matière de sécurité des systèmes et réseaux d'information sur ces lignes directrices (Danemark, Finlande, Hongrie, Italie, Pays-Bas, République tchèque) et/ou disposent de directives publiques de sécurité qui leur sont conformes (Australie, Royaume-Uni), ou exigent que chaque ministère ou organisme les respectent dans le cadre de leurs travaux (Japon).
- Ils disposent d'un organisme national chargé de :
  - Suivre le développement de la sécurité des TI dans les secteurs public et privé : Danemark.
  - Vérifier la compatibilité des systèmes publics avec la loi relative à la protection des données : France.
  - Coordonner et conseiller les autorités, échanger les pratiques exemplaires, produire des rapports d'analyse des tendances, représenter le gouvernement dans les organismes de normalisation nationaux et internationaux et mettre en service des réseaux sécurisés au sein de l'Administration : Allemagne.

  - Superviser l'application de la politique nationale : Hongrie, Pays-Bas.
  - Vérifier que la sécurité des systèmes et réseaux d'information est mise en œuvre dans les systèmes et réseaux publics et informer les usagers de leurs responsabilités en matière de sécurité : Royaume-Uni.
- Ils imposent à tous les organismes un audit annuel indépendant : États-Unis.
- Élaboration d'un label de qualité pour le cybergouvernement : Autriche.
- Élaboration d'un cadre pour l'organisation fonctionnelle de la sécurité des systèmes et réseaux d'information qui distingue trois niveaux (politique et planification, contrôle de la sécurité, audit) : Belgique.

À ce stade, la Norvège n'a pas coordonné ses activités en vue d'une application diligente des Lignes directrices sur la sécurité.

La majorité des pays ont mis à la disposition de leurs employés des outils et des programmes de formation en matière de sécurité. La Belgique développe actuellement de tels programmes. Un de ces pays signale qu'aux termes de la loi, cette formation est obligatoire pour les nouveaux embauchés (États-Unis).

Les programmes de formation sont organisés par chaque ministère/organisme (Allemagne, Autriche, Norvège, Pays-Bas, République tchèque, Royaume-Uni,), avec l'aide de l'organisme national de sécurité des systèmes et réseaux d'information (France), ou relèvent de la responsabilité d'une seule administration (Australie).

Ils peuvent aussi être mis à exécution dans le cadre de projets coopératifs et multifonctionnels de sécurité des systèmes et réseaux d'information (Finlande).

Dans certains cas, les programmes de formation sont destinés aux responsables de la sécurité des TI (Royaume-Uni), à des populations particulières dotés de compétences et de besoins organisationnels donnés (États-Unis) ou à des fonctionnaires locaux (Japon). Dans ce dernier cas, le programme fait appel à des outils de cyberformation, il a été suivi par 7 000 personnes et va être élargi aux fonctionnaires publics.

II. Missions des entreprises et de la société civile

A. Les entreprises en tant que propriétaires, exploitants et/ou utilisateurs de systèmes et réseaux d'information (Q21, Q22)

Dans la plupart des pays, le dialogue entre les pouvoirs publics et les entreprises en vue d'encourager ces dernières à prendre les principes des Lignes directrices sur la sécurité en considération se déroule dans des cadres divers : ateliers, débats sur les lois en préparation, et à la norme ISO/IEC 17799 ou au partenariat public-privé. Deux d'entre eux ont fait état de régimes autorégulations.

La plupart des pays rendent compte de programmes spéciaux destinés à aider les entreprises à assurer la conformité de leurs systèmes et réseaux d'information aux Lignes directrices. Il peut s'agir de la promotion des normes internationales, de la création d'un label de confiance pour l'accès à l'Internet ou d'une participation gouvernementale à une association chargée de conseiller les entreprises et de les aider à organiser des formations du personnel conformes aux Lignes directrices.

Le dialogue entre les pouvoirs publics et les entreprises se tient dans les cadres suivants :

- Manifestations diverses (séminaires et ateliers par exemple) : États-Unis, Finlande, Hongrie.

- Débats dans le cadre de l'élaboration des lois : Corée, France.
- Mise en place d'un « Groupe de travail gouvernement-entreprises sur les infrastructures critiques » : Australie.
- Création de partenariats public-privé : Hongrie, Pays-Bas.
- Promotion de la norme ISO/IEC 17799 (Australie) et soutien au Secrétariat du groupe des usagers de cette norme (Royaume-Uni).
- Participation dans les domaines de coopération entre les entreprises et les pouvoirs publics et aval aux mesures de sensibilisation prises par les associations professionnelles : Norvège.
- Élaboration et mise en œuvre d'un programme de cybergouvernement : Autriche.

Le Mexique s'efforce d'établir un dialogue de cette nature entre les entreprises et l'Administration.

La Hongrie invite des représentants des entreprises et de la société civile à des consultations au cas par cas au sous-comité sur la sécurité des TI de son Comité de coordination interdépartemental pour la société de l'information (IDCCIS).

Sur le plan de l'autorégulation, le Royaume-Uni a mentionné le « tScheme », un programme établi par le secteur privé pour mettre en place des critères d'évaluation rigoureux en fonction desquels l'organisme tScheme donnera son approbation à des services de confiance. Les États-Unis ont également signalé des alliances professionnelles comme le Dialogue mondial des affaires sur le commerce électronique (GBDe) et le Dialogue commercial transatlantique (DCT) qui ont déployé beaucoup d'efforts pour diffuser les Lignes directrices sur la sécurité au travers de liens, de cadres d'action et de recommandations.

Huit pays disposent de programmes particuliers pour aider les entreprises à vérifier que leur utilisation des systèmes et réseaux d'information est conforme aux Lignes directrices. Il s'agit des programmes suivants :

- Promotion des normes internationales ISO/IEC : Australie, Japon.
- Enquête sur les risques de sécurité pour les PME : France.
- Loi en préparation pour encourager la formation en matière de sécurité, les contrôles de sécurité périodiques, les évaluations et l'utilisation de produits sécurisés dans les entreprises : Corée.
- Création d'un label de confiance pour l'accès à l'Internet : Japon.
- Financement d'études sur la sécurité des systèmes et réseaux d'information dans les entreprises nationales selon la norme ISO/IEC 17799 : Espagne.
- Participation à une association réunissant des représentants des entreprises et des pouvoirs publics pour donner aux entreprises des conseils conformes aux Lignes directrices et préparer la formation des employés : Norvège.
- Publication ultérieure de lignes directrices sur la sécurité des systèmes et réseaux d'information destinées aux entreprises : Corée.
- Création d'un site Web pour les entreprises dans le cadre d'un partenariat public-privé : Royaume-Uni.

L'Autriche n'a pas encore mis de programme à exécution mais prévoit des opérations de cette nature en 2004.

B. La société civile en tant qu'utilisateur de systèmes et réseaux d'information (Q23, Q24)

La plupart des pays ayant répondu ont établi un dialogue avec la société civile pour encourager celle-ci à prendre en considération les principes des Lignes directrices sur la sécurité. La plupart des interventions ont un objectif de sensibilisation, comme la semaine nationale pour la protection des consommateurs organisée sur le thème « Sécurité des systèmes et réseaux d'information ».

La majorité des gouvernements sont en contact avec la société civile afin de promouvoir les principes des Lignes directrices ou le seront ultérieurement (Autriche, Mexique, Norvège). Pour établir et maintenir ce dialogue, ils font appel aux moyens suivants :

- Publication d'informations/recommandations sur le Web: Allemagne, Australie, États-Unis, Finlande, France.
- Organisation d'ateliers et de conférences : États-Unis, France.
- Campagnes d'information, par exemple sur la façon de choisir un mot de passe : États-Unis.
- Création d'un Comité auquel participent des sociétés de sécurité et des groupes de la société civile afin d'examiner la mise en place de pratiques exemplaires dans les domaines de la sécurité des systèmes et réseaux d'information et de la protection de la vie privée : Corée.
- Recommandations du commissaire à la protection des données : Finlande.
- Traitement fiscal préférentiel et prêts de l'État pour encourager les PME à investir dans les technologies de sécurité des systèmes et réseaux d'information: Japon.
- Programme de cybergouvernement offrant des services sécurisés aux citoyens et aux entreprises : Royaume-Uni.

La Belgique, la Finlande, la République slovaque, la République tchèque et la Suède n'ont pas de programmes spéciaux.

Pour s'assurer que l'utilisation des systèmes et réseaux d'information par les particuliers est conforme aux Lignes directrices sur la sécurité, les pays membres :

- N'ont pas de programme particulier (Australie, Autriche, Corée, Finlande, Mexique, Norvège, République tchèque) mais signalent que des opérations vont être ultérieurement mises en place à cet effet, par exemple un programme organisé dans le cadre d'un partenariat public-privé, dénommé « Cyber-instruction nationale », qui offre des stages d'informatique aux débutants et pourrait comporter à l'avenir des modules sur la sécurité des systèmes et réseaux d'information (République tchèque).
- Ou mentionnent des programmes ou outils de sensibilisation (Allemagne, États-Unis, Japon, Suède).

NOTES

1. Le Plan d'application de l'OCDE a été approuvé par les pays membres de l'OCDE en 2002 et a été republié, après de nouvelles révisions, sous forme de document déclassifié, sous la cote DSTI/ICCP/REG(2003)5/REV1, pour le Forum mondial de l'OCDE sur la sécurité des systèmes et réseaux d'information d'Oslo.

2. La norme ISO/IEC 15408 « Critères pour l'évaluation de la sécurité des technologies de l'information » est aussi connue sous le nom de « Critères communs » ou « CC ».

3. La norme ISO/IEC 17799 est un code de pratiques standard qui fournit aux entreprises des lignes directrices par défaut quant aux types de contrôles de la sécurité qu'elles devraient appliquer pour protéger leurs actifs. La norme BS7799 est une spécification de gestion standard pour les systèmes de gestion de la sécurité des informations. Elle indique aux entreprises les mesures nécessaires à l'établissement d'un cadre de gestion.

4. Le Plan d'action pour un Internet plus sûr est un programme de l'Union européenne destiné à financer les activités associées à la gestion du contenu indésirable sur l'Internet. Pour plus d'information, voir www.europa.eu.int/information_society /programmes/iap/index_en.htm, accédé le 14 mai 2004.

5. GetNetWise (États-Unis). Voir plus loin.

6. CERT type fournit des conseils techniques et coordonne les réponses aux compromis de sécurité, détermine les tendances en matière d'intrusion informatique, travaille avec des experts pour définir des solutions aux problèmes de sécurité et diffuse les informations à une vaste communauté. Il peut aussi analyser les vulnérabilités des produits, publier des documents techniques et proposer des stages de formation. Voir www.cert.org. Un ISAC est parrainé par un secteur particulier de l'industrie. Il a pour mission de recueillir, d'analyser et de communiquer à ses membres une vue d'ensemble des vulnérabilités, risques et incidents touchant les systèmes informatiques et autres infrastructures qui présentent un intérêt pour le secteur qui le parraine. Il peut aussi organiser l'échange de pratiques et de solutions optimales en matière de sécurité entre ses membres. Voir, par exemple, *e.g.* https://www.it-isac.org, accédé le 14 mai 2004. Le SANS est un organisme de recherche et de formation coopératif. Il offre aux professionnels de la sécurité, aux auditeurs, aux administrateurs de systèmes et de réseaux des systèmes et réseaux d'information en matière de sécurité (bulletins d'actualité, études synthétiques, alertes informatiques et articles) et des formations. Voir www.sans.org.

7. « ITIL fournit un ensemble cohérent de bonnes pratiques provenant des secteurs public et privé internationaux. Il est soutenu par un schéma de qualification complet, des organismes de formation accrédités et des outils de mise en œuvre et d'évaluation. Les bonnes pratiques promues par ITIL soutiennent et sont soutenues par la norme sur la gestion des services informatiques (IT Service Management) du British Standards Institution (BS15000) ». Voir : www.ogc.gov.uk/index.asp?id=2261, accédé le 14 mai 2004.

8. L'ITSEC (critères d'évaluation de la sécurité des technologies de l'information) est reconnue dans toute l'Europe. Elle constitue une norme uniforme unique adoptée par la France, l'Allemagne, les Pays-Bas, le Royaume-Uni et la Commission européenne, et réduit de ce fait la nécessité d'évaluer les produits dans chaque pays. La norme CC (Critère commun) est une norme de l'ISO (ISO15408), plus largement reconnue que l'ITSEC. Voir www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=1, accédé le 14 mai 2004.

9. Les produits de sécurité, comme les pare-feu, les systèmes de détection d'intrusion (IDS) et les réseaux privés virtuels (VPN), doivent être certifiés par le Service national de renseignements coréen (NIS) pour être utilisés dans l'administration publique. L'utilisation des critères communs, au lieu des normes nationales coréennes, est envisagée pour l'avenir.

ANNEXE A: QUESTIONS DE L'ENQUÊTE

I. Missions du secteur public

Q1. Votre gouvernement rend-il les Lignes directrices publiquement disponibles ? Dans l'affirmative, par quels moyens ? Imprimés. Support électronique. Lien renvoyant vers le site Web de l'OCDE. Autres (veuillez préciser).

Q2. Les Lignes directrices ont-elles été traduites dans la (ou les) langue(s) de votre pays ? Dans l'affirmative, veuillez en donner la liste.

Q3. Si les Lignes directrices sont disponibles dans les langues de votre pays, sont-elles, en même temps que les autres informations utiles, consultables sur le Web ?

Q4. Votre gouvernement reconnaît-il et utilise-t-il les Lignes directrices comme un cadre pour la politique régissant la sécurité de l'information ?

A. Prérogative du gouvernement visant la politique des pouvoirs publics

Q5. Votre gouvernement a-t-il élaboré une politique nationale sur la sécurité de l'information ? Dans l'affirmative, veuillez en donner une description.

Q6. Votre gouvernement a-t-il promulgué un ensemble complet de mesures de fond en matière de poursuite criminelle, de procédures et d'assistance mutuelle pour lutter contre la cybercriminalité et assurer la coopération transfrontière […]

Q7. Ces mesures sont-elles aussi détaillées que les dispositions prévues dans la Convention du Conseil de l'Europe sur la cybercriminalité et compatibles avec elles ?

B. Diffusion en direction d'autres parties prenantes et soutien de ces dernières

Q8. Quel type de programmes et d'initiatives votre gouvernement a-t-il élaboré pour accroître la sensibilisation et faciliter les actions de l'ensemble des parties prenantes qui utilisent des systèmes et réseaux d'information ou interviennent dans leur fonctionnement ?

Q9. Votre gouvernement mène-t-il un programme pour encourager l'élaboration de pratiques exemplaires et/ou de partenariats entre parties prenantes pour prendre en compte la sécurité de l'information ?

Q10. Votre gouvernement encourage-t-il l'échange de pratiques exemplaires afin que les utilisateurs soient mieux à même de comprendre et de mettre en œuvre des mesures de sécurité efficaces et à jour ?

Q11. Votre gouvernement soutient-il des programmes d'éducation et d'information sur la sécurité de l'information ? Par exemple, votre gouvernement mène-t-il des programmes de sensibilisation faisant appel à l'éducation, la formation, les sites Web, les annonces publiques, et autres initiatives offrant des outils et des panoplies pour promouvoir une culture de la sécurité ? Dans l'affirmative, dans quelle mesure intègre-t-il les valeurs de chacun des principes des Lignes directrices sur la sécurité, notamment concernant l'éthique et la démocratie ?

Q12. Votre gouvernement encourage-t-il la création et l'utilisation de sites utiles [comme ceux du CERT ou du SANS et divers centres privés d'analyse et d'échange d'information (ISAC)] ? Dans l'affirmative, quel type d'initiatives votre gouvernement encourage-t-il ou soutient-il ?

Q13. Votre gouvernement soutient-il des activités de recherche-développement visant à accroître la sécurité par un renforcement de la sécurité dans le logiciel et le matériel et par des procédures pratiques fondées sur des pratiques exemplaires ?

C. Le secteur public en tant que propriétaire et exploitant de systèmes et réseaux d'information

Q14. En tant que propriétaire et exploitant de systèmes et réseaux d'information, votre gouvernement a-t-il développé une politique de gestion de la sécurité de ses propres systèmes et réseaux ?

Q15. Comment votre gouvernement formule-t-il sa politique nationale concernant la sécurité des systèmes et réseaux d'information gouvernementaux ? Celle-ci est-elle centralisée ou décentralisée entre les différents Ministères ?

Q16. Comment la gestion par votre gouvernement de la sécurité des systèmes et réseaux gouvernementaux reflète-t-elle les principes de Lignes directrices, notamment ceux liés à l'évaluation des risques, à la conception de la sécurité, à la gestion de la sécurité et à la réévaluation ?

Q17. Comment votre gouvernement utilise-t-il ses systèmes et réseaux pour devenir un propriétaire modèle et ouvrir la voie par l'exemple ? Comment votre gouvernement élabore-t-il des pratiques exemplaires et autres améliorations opérationnelles au profit de l'ensemble des parties prenantes ?

Q18. Votre gouvernement utilise-t-il sa capacité d'achat dans les systèmes et réseaux d'information pour encourager le développement et une plus large disponibilité de produits et services plus sûrs ? Dans l'affirmative, comment ? Votre gouvernement a-t-il défini des principes directeurs et/ou normes en matière de sécurité qui doivent être suivis pour les marchés publics de systèmes et réseaux d'information ?

D. Le secteur public en tant qu'utilisateur de systèmes et réseaux d'information

Q19. En tant qu'utilisateur de systèmes et réseaux d'information, comment votre gouvernement s'assure-t-il que ses utilisations son conformes aux Lignes directrices ?

Q20. Votre gouvernement a-t-il développé un programme quelconque pour améliorer l'environnement, la formation et les outils en matière de sécurité, de telle manière que ses employés soient sensibilisés aux questions de sécurité, conscients de leurs responsabilités personnelles et capables de réagir de manière appropriée aux incidents de sécurité ?

II. Missions des entreprises et de la société civile

A. Les entreprises en tant que propriétaires, exploitants et/ou utilisateurs de systèmes et réseaux d'information

Q21. Votre gouvernement dialogue-t-il avec les entreprises pour encourager celles-ci à prendre en compte les principes des Lignes directrices de l'OCDE sur la sécurité ? Encourage-t-il notamment les entreprises à prendre des initiatives d'autodiscipline et à agir de façon indépendante ou en partenariat avec les pouvoirs publics et/ou la société civile pour promouvoir les pratiques exemplaires, l'éducation et le développement responsable de produits et de services conformément aux orientations des principes des Lignes directrices sur la sécurité ? Dans l'affirmative, veuillez en donner une description.

Q22. Votre gouvernement mène-t-il un programme ou une activité quelconque pour aider les entreprises à assumer la responsabilité de s'assurer que leur utilisation des systèmes et réseaux d'information est conforme aux Lignes directrices ?

B. La société civile en tant qu'utilisateur de systèmes et réseaux d'information

Q23. Votre gouvernement dialogue-t-il avec la société civile pour encourager celle-ci à prendre en compte les principes des Lignes directrices sur la sécurité de l'OCDE ? Notamment, encourage-t-il la société civile à agir de façon indépendante ou en partenariat avec les entreprises et/ou les pouvoirs publics pour promouvoir les pratiques exemplaires, l'éducation et le développement responsable de produits et de services, conformément aux orientations des principes des Lignes directrices sur la sécurité ? Dans l'affirmative, veuillez en donner une description.

Q24. Votre gouvernement mène-t-il un programme ou une activité quelconque pour aider la société civile à assumer la responsabilité de s'assurer que l'utilisation par les particuliers des systèmes et réseaux d'information est conforme aux Lignes directrices ?