Human Resources Development Canada **Développement des ressources humaines Canada**
Internal Audit Bureau **Bureau de vérification interne**

RAPPORT NATIONAL

Évaluation de la sécurité de la technologie de l'information

Project N°. : 442/98

Équipe de projet

Directeur général :	*J.K. Martin*
Directeur de la vérification :	*J.R. Clark*
Chefs d'équipe :	*P. LePage*
	F. Gloade
Vérificateurs :	*K. Jevons*
	M. Winterburn
Consultants :	*Progestic International Inc.*

AUTORISATION: **Copie originale signée par :**

DIRECTEUR: *J.R. Clark* *30 septembre 1999*
Date

DIRECTEUR GÉNÉRAL: *James K. Martin* *30 septembre 1999*
Date

Septembre 1999

TABLE DES MATIÈRES

ANNEXES

1.0 SOMMAIRE

En mars et en avril 1999, le Bureau de vérification interne (BVI) a visité certains sites nationaux, régionaux et locaux aux fins de l'Évaluation de la sécurité de la technologie de l'information à DRHC. Le BVI a procédé à cette évaluation dans le contexte du Cadre directeur de la TI pour le gouvernement fédéral (Voir l'annexe A) ainsi que des normes de sécurité de la TI de DRHC.

Comparaison faite avec d'autres organismes fédéraux et privés semblables, le BVI a conclu que les mesures de sécurité de la TI à DRHC étaient appropriées. DRHC prend actuellement un virage vers une approche plus globale à ce chapitre, comme le montre la vision/stratégie récemment adoptée (mai 1999), qui aborde la question de la sécurité de la TI. De nombreuses personnes au sein de l'organisation se partagent la prestation du soutien et des services en matière de sécurité de la TI et adoptent des méthodes variées, ce qui a pour effet de brouiller les rôles, responsabilités, obligations redditionnelles, autorités et liens hiérarchiques. Comme peu de gens connaissent l'existence des politiques et des procédures en matière de sécurité de la TI, il est important que le personnel apprenne à mieux connaître les normes et les pratiques de sécurité entourant ce domaine.

Conclusions

- Depuis la création de DRHC, les programmes et les services ministériels ont adopté leur propres méthodes de sécurité de la TI. Sur le plan hiérarchique, la sécurité de la TI incombe principalement au secteur des Systèmes de DRHC, mais la panoplie de méthodes individuelles employées font qu'elle est gérée par trop de gens qui suivent des lignes de conduite différentes.

- Comme les CTI relèvent maintenant des Systèmes à l'AC, les régions estiment ne plus être dotées d'un « agent régional de la sécurité de la TI », rôle habituellement dévolu au personnel des CTI. Par conséquent, les régions n'ont plus l'autorité hiérarchique de la gestion de la sécurité de la TI au niveau régional, provoquant ainsi un vide fonctionnel et opérationnel dans les régions.

- Bon nombre de personnes qui s'occupent de sécurité de la TI ne sont pas au courant des politiques et procédures de DRHC à ce chapitre, même si le sujet est abordé dans le site Web des Systèmes. En outre, de nombreux documents abordant le sujet sont couramment distribués au personnel de DRHC, mais il n'en demeure pas moins que les employés ont une mince connaissance de ces pratiques et procédures. À titre d'exemple, l'identification ou le mot de passe des utilisateurs permettant d'accéder aux systèmes de DRHC ne fait pas l'objet de contrôles réguliers, c'est pourquoi certains adoptent le même code ou ont des codes d'utilisateur inadéquats.

- Les séances de sensibilisation ou d'orientation sur la sécurité à l'intention du personnel de DRHC abordent rarement la question de la sécurité de la TI.

Prochaines étapes

- Adoption par la direction de DRHC des recommandations énoncées dans le présent rapport, particulièrement en ce qui a trait à simplification de la structure organisationnelle et les méthodes de gestion de la sécurité de la TI à tous les niveaux, et à l'amélioration des connaissances et de la sensibilisation du personnel de DRHC en matière de sécurité de la TI.

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

STRUCTURE ET ORGANISATION DE DRHC (1)

Multiples « intervenants » participant à la prestation des activités de sécurité de la TI au sein de DRHC

- AMS/ASR
  - Sécurité physique, personnelle, protection des renseignements personnels
  - Les ASR ne s 'occupent habituellement pas des questions de sécurité de la TI
- Infrastructure TI
  - Conception/élaboration des fonctions de sécurité de la TI (de concert avec le groupe des Communications TI)
- Opérations de la sécurité des TI
  - Soutien des opérations courantes de sécurité de la TI (de concert avec les coordonnateurs de la sécurité des CTI, OPPM, RSM, gestionnaires de réseau - AC, ACR, CRHC)
- Il n 'existe aucune entente officielle définissant les rôles, les responsabilités et les obligations redditionnelles des différents groupes.

NOTA: Le tableau de la page 6 illustre la structure organisationnelle actuelle de DRHC en matière de sécurité de la TI

AMS – Un poste d'agent ministériel de la sécurité (AMS) est officiellement créé et relève du SMA, Finances et Services administratifs (FSA). L'AMS est responsable de la protection des renseignements personnels et de la sécurité physique et du personnel.

ASR – La plupart des Agents de sécurité régionaux (ASR) estiment qu'ils ont très peu à voir avec la sécurité de la TI. Ils ont mentionné s'occuper principalement de sécurité physique et du personnel (voir plus amples détails à la prochaine diapositive).

Coordonnateur de la sécurité de la TI à l'AC – Un coordonnateur de la sécurité de la TI à l'AC relève du DG de l'Infrastructure, du secteur des Systèmes de DRHC, et s'occupe d'orientation fonctionnelle (P.ex. : premières phases du cycle de développement et de construction. Au sein de l'Infrastructure, ce sont les Communications TI (télécommunications) qui travaillent de concert avec le coordonnateur de la sécurité à l'élaboration et à la vérification des outils de sécurité de la TI liées à l'infrastructure (p.ex. : pare-feu).

Opérations de la sécurité de la TI – Les Opérations de la sécurité de la TI relèvent du DG, Opérations du secteur des Systèmes de DRHC. Leur rôle est principalement axé sur les opérations et le soutien des activités de sécurité (entretien et soutien des ordinateurs principaux). Des postes seront prochainement dotés aux fins de ces activités.

Conclusion – Il n'existe aucun accord officiel définissant les rôles, les responsabilités et les obligations de ces trois secteurs. Cela se fait cependant de façon officieuse.

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

STRUCTURE ET ORGANISATION DE DRHC (2)

Multiples « intervenants » participant à la prestation des activités de sécurité de la TI au sein de DRHC, suite

- Les ACR estiment qu'ils n'ont plus de « coordonnateur régional de la sécurité de la TI »
- Les administrateurs de réseaux locaux agissent comme coordonnateurs régionaux de la sécurité de la TI, bien que officieusement
- Les rôles, responsabilités et liens hiérarchiques varient (fonctionnel et hiérarchique)
- Lien hiérarchique flou en matière de sécurité de la TI entre **:**
  - l 'AC et l 'ACR;
  - Certaines ACR et les CRHC; et
  - la plupart des CTI et les ACR

Coordonnateur régional de la sécurité de la TI – Tous les guides de politiques et de procédure régionaux en matière de sécurité mentionnent un « Coordonnateur régional de la sécurité de la TI », ainsi que les fonctions qui lui incombent. Il n'est pas clair qu'un tel rôle existe toujours, puisque les CTI relèvent maintenant de l'AC. Les quatre régions visitées ont affirmé ne plus avoir de coordonnateur régional de la sécurité de la TI dans l'organisation régionale officielle. Les ACR, auxquelles se rapportaient autrefois les CTI, ont conservé des liens officiels avec le coordonnateur de la sécurité des CTI.

Disparités régionales – Tous les gestionnaires des systèmes régionaux (GSR) croient que les administrateurs de réseaux locaux de leur région ou de leur bureau local relèvent fonctionnellement d'eux, mais certains ne croient pas que cela s'étend la sécurité de la TI. Ces derniers croient que la sécurité de la TI incombe principalement soit à l'Infrastructure et/ou aux Opérations à l'AC.

Administrateurs de réseaux locaux – Dans les CRHC visités, les administrateurs des réseaux locaux ont été identifiés comme coordonnateurs de la sécurité de la TI. Dans toutes les régions, les administrateurs de réseaux locaux relèvent fonctionnellement des GSR, tandis que, dans certaines autres régions, il existe également un lien hiérarchique. Dans les régions où il n'existe qu'un lien fonctionnel, les administrateurs de réseaux locaux relèvent hiérarchiquement des directeurs de CRHC.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

STRUCTURE ET ORGANISATION DE DRHC (3)

Recommandation

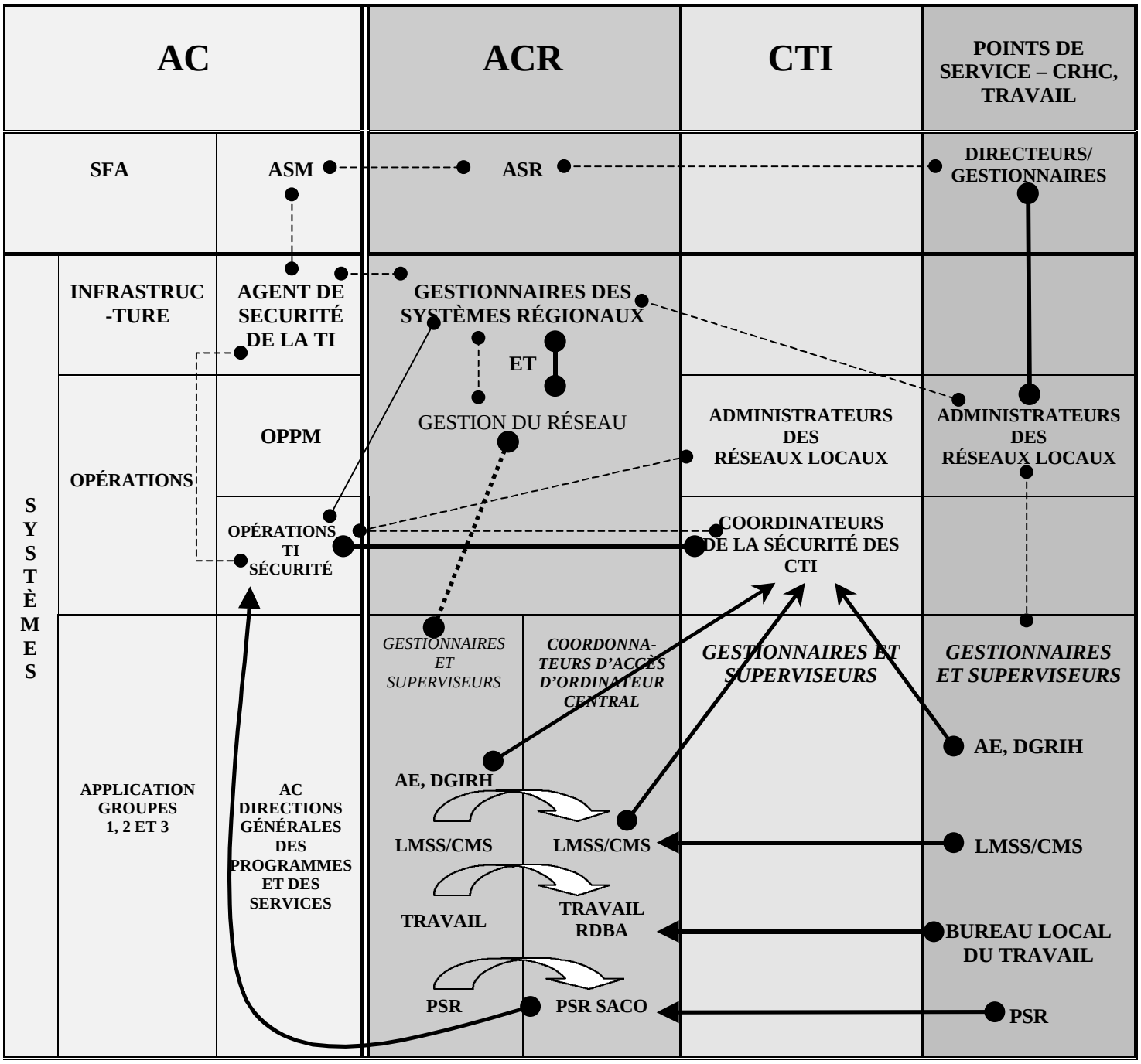
DRHC doit rationaliser la prestation des activités liées à la sécurité de la TI en précisant les rôles, les responsabilités, les autorités et les obligations et les liens hiérarchiques

- *Préciser les obligations fonctionnelles/opérationnelles des AMS, de l 'Infrastructure et des Opérations*
- *Nommer des coordonnateurs **régionaux** de la sécurité de la TI et en définir le mandat*
- *Officialiser les mécanismes de communication dans l 'ensemble de DRHC*
- *Inclure un volet « Sécurité de la TI - Structure et Organisation » dans les programmes de sensibilisation à la sécurité*

Conclusion

Compte tenu de la disparité du mode de prestation des activités liées à la sécurité de la TI dans les différents secteurs de DRHC, le BVI en a conclu que la plupart des personnes interviewées saisissaient mal le fonctionnement de la structure organisationnelle et à qui incombe la responsabilité des différents volets de la sécurité de la TI au sein de DRHC. Cette notion de « qui est responsable/comptable de quoi » est encore plus floue au niveau régional et local. Cette fragmentation a également pour effet que certains groupes ne savent pas toujours des actions ou des réalisations d'autres groupes en ce qui a trait à la sécurité de la TI.

Faute d'un solide leadership ***régional*** et d'une orientation fonctionnelle encore plus solide émanant de l'AC, les activités liées à la sécurité de la TI sont prises en charge au niveau opérationnel. Par conséquent, la qualité de cette sécurité dans l'ensemble des sites visités dépendait davantage de la sensibilisation, de la formation et de l'expérience de la personne responsable plutôt que d'une définition précise des rôles, responsabilités et directives fonctionnelles et d'obligations redditionnelles.



Légende

Compétence fonctionnelle — Autorité hiérarchique — Accès aux systèmes

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

POLITIQUES, PROCÉDURES, NORMES ET DIRECTIVES (1)
Documents
- Il existe de nombreux documents sur la sécurité de la TI (format papier, électronique, y compris des brochures) mais peu de gens en connaissent l 'existence
- Difficile de déterminer si ces documents sont à jour (faute de dates)
- **Compréhension et connaissance**
- Peu de gens comprennent ou connaissent bien les politiques, les procédures ou les normes et les pratiques en matière de sécurité de la TI

Où se trouvent-elles sur l'Intranet? – Peu d'utilisateurs (AC, ACR, CRHC et CTI) ont indiqué être au courant des sites électroniques où ils pouvaient trouver la version à jour des politiques, normes et procédures de DRHC en matière de sécurité de la TI. Depuis le début de cette évaluation, le site Intranet sur la sécurité de la TI a été mis à jour et présente maintenant un répertoire adéquat ainsi que de la documentation additionnelle. Par conséquent, le site Web de DRHC s'en trouvera également modifié.

Peu de gens sont au courant de ce qui existe – La plupart du personnel de DRHC ne comprends ou ne saisit pas très bien les politiques, directives, procédures et normes en matière de sécurité de la TI, même s'il existe un site Intranet ministériel consacré au domaine. Par conséquent, le BVI estime que cette lacune sur le plan des connaissance des politiques et des procédures à ce chapitre contribue au fait que les méthodes employées varient entre l'AC, les régions, les CTI et les CRHC (comme le mentionne la diapositive précédente).

Mesures de sécurité incohérentes – Les régions ont la perception que, n'ayant pas de coordonnateur régional de la sécurité de la TI, les ACR et les bureau locaux ont été relativement laissés à eux-mêmes en ce qui a trait à l'application des mesures de sécurité de la TI dans le cadre des opérations. Cette perception, doublée des disparités entre les connaissances, le savoir-faire et les préoccupations au sujet des mesures de sécurité de la TI à prendre selon les ACR/CRHC et administrateurs de RL, a donné lieu à des mesures de sécurité incohérentes, comme le fait que certains risques ne soient pas correctement étudiés (c.-à-d. intégrité des codes/mots de passe), et que certaines régions élaborent leurs propres programmes de sensibilisation à la sécurité, comprenant un volet sur la TI. En outre, nous avons remarqué que

les mesures de sécurité en matière de la TI employées dans les CRHC sont laissées à la discrétion des administrateurs des réseaux locaux. Comme la plupart de ceux-ci n'ont reçu aucune formation officielle en matière de sécurité de la TI, leurs préoccupations et leur savoir-faire diffèrent, ce qui a entraîné la disparité des méthodes employées au niveau local.

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

POLITIQUES, PROCÉDURES, NORMES ET DIRECTIVES (2)

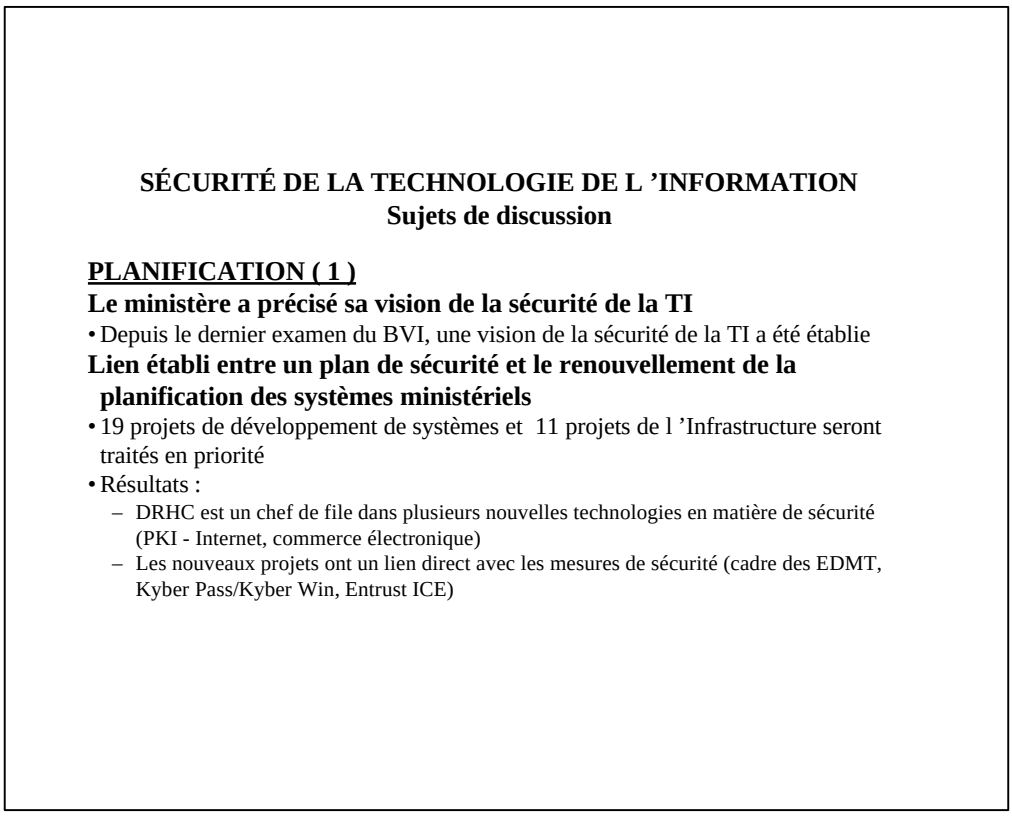
Normes relatives à l 'accès par sélection

- Il existe différents logiciels pour établir l'accès à distance (RAS, RLN...)
- La protection demeure adéquate bien que non normalisée
- Plus de détails s'imposent concernant l'accès à distance, les pare-feu, les ordinateurs portatifs et le télétravail
- ***Recommandations***
  - *Vérifier l'exactitude des documents sur la sécurité de la TI et les mettre à jour régulièrement*
  - *Dresser une liste des adresse électroniques des destinataires intéressés (P.ex. : Systèmes, GSR, AMS/ASR) afin de les aviser des changements dans les documents ou dans le site Web de DRHC sur la sécurité de la TI*
  - *Inclure des « Politiques et procédures sur la sécurité de la TI » dans les programmes de sensibilisation à la sécurité*

Il existe différents logiciels de sécurité d'accès à distance – La vérification a permis de constater l'existence de différents logiciels de sécurité d'accès à distance, comme ReachOut, Remote Access Software, Remote Link Network et Racal Guard Data Watchword, à travers DRHC. Les personnes interviewées ont mentionné diverses raisons motivant l'utilisation de ces logiciels, comme une sécurité accrue, la facilité d'utilisation et un temps de branchement plus rapide. Les normes d'accès à distance doivent être resserrées.

Documentation requise – Plusieurs personnes interviewées ont souligné la nécessité de se doter de politiques plus détaillées sur l'utilisation des ordinateurs portatifs et le télétravail, de procédures précisant la politique relative aux pare-feu, de normes relatives à l'accès à distance (accès par sélection) et de directives sur la construction de pièces réservées aux réseaux locaux et le choix de lieux de stockage externes.

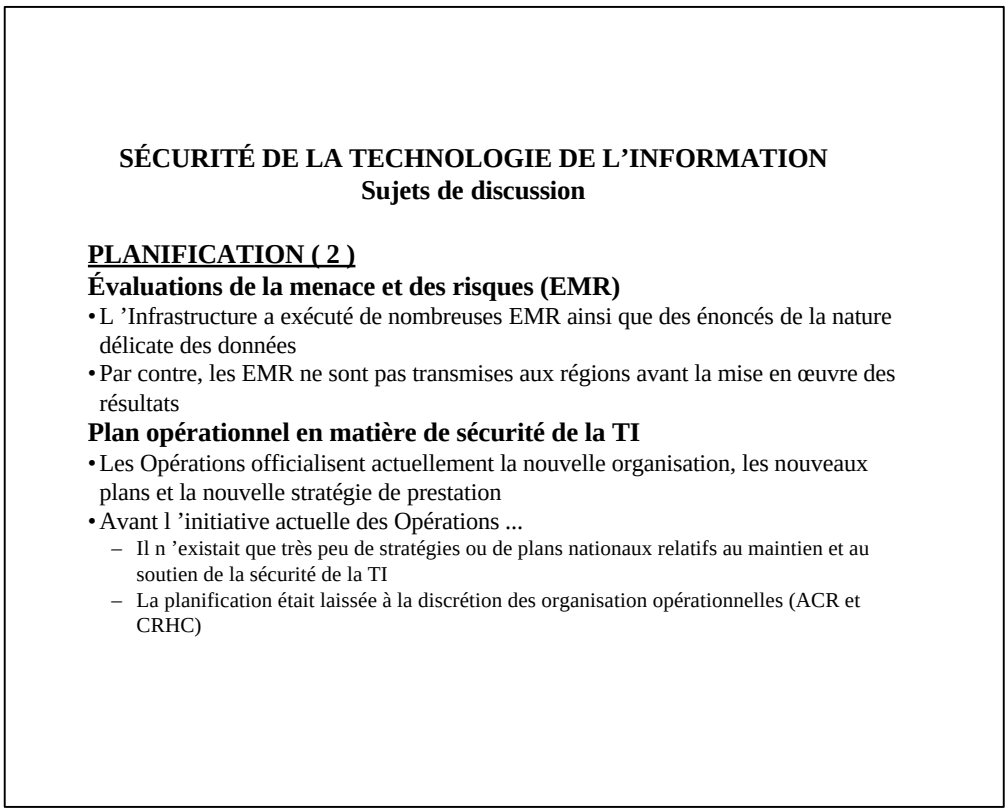
Nota : Tout plan d'action découlant des recommandations susmentionnées doit tenir compte de celles concernant la Structure et l'Organisation énoncées dans le présent rapport.



Vision de la sécurité de la TI – Dans son rapport de 1998-1999 sur la mise en œuvre de la décision du Conseil de gestion sur les systèmes de juillet 1995 et de l'enquête ponctuelle des CTI, le BVI a relevé l'absence d'une vision, d'un plan et d'une stratégie intégrés (particuliers à la sécurité de la TI). Depuis lors, l'Infrastructure a récemment élaboré une vision/stratégie en matière de sécurité de la TI (mai, 1999) qui prévoit notamment les volets suivants :

- Identification des utilisateurs individuels et procédure d'entrée en communication pour le personnel, incluant le contrôle de l'accès à l'application et aux services accessibles à l'utilisateur final;
- La possibilité de traiter les transactions émanant d'Internet de façon sécuritaire;
- Échange sécuritaire de données, y compris le commerce électronique avec les partenaires; et
- Mécanisme de sécurité conforme à ceux des institutions financières pour ce qui est des échanges avec le public canadien.

Lien avec de nouveaux projets visant l'élaboration d'un plan d'action en matière de TI – Les plans de DRHC en matière de sécurité de la TI ont un lien direct avec des projets précis de sécurité de la TI, qui ont été jugés prioritaires dans le cadre de la planification du renouvellement des systèmes ministériels. Le BVI a appris que, pour 1999-2000, DRHC a accordé la priorité à 19 projets d'élaboration de systèmes et 11 projets d'infrastructure dans le cadre de ces plans. Un Comité d'examen des projets évalue ces projets, et les plans et les décisions concernant la sécurité de la TI y sont ajoutés s'il y a lieu. Ces mesures de sécurité touchent directement les nouveaux projets, comme l'accès aux données de DRHC dans le cadre des EDMT, ainsi que Kyber Pass/Kyber Win, Entrust ICE et autres logiciels d'accès à distance.



EMR effectuées par l'Infrastructure – À l'AC, on a principalement recours à des Évaluations de la menace et des risques (EMR) dans le cadre de projets ayant reçu l'aval du Comité d'examen des projets. Au cours de l'année financière 1998-1999, le groupe de la Sécurité de la TI de l'Infrastructure a procédé à quelque 25 EMR visant à cerner les faiblesses et les lacunes potentielles des projets, ainsi qu'à présenter des recommandations visant à améliorer la situation et à diminuer les risques. La plupart des EMR sont des mesures proactives qui précèdent l'élaboration ou la mise en œuvre de changements aux applications des systèmes ou à l'infrastructure opérationnelle. Les régions, les CTI et les CRHC se sont montrés intéressés à recevoir les résultats des EMR, jugeant que l'information leur seraient utile à l'étape de mise en œuvre locale. Récemment, cette utilité fut bien illustrée lors de la distribution d'ordinateurs portatifs aux agents de recouvrement des trop-payés de l'a.-e. Les régions ont tenté de déterminer quelles seraient les meilleures mesures de sécurité possibles avant de distribuer les ordinateurs portatifs, ceux-ci devant contenir des informations de nature délicate et permettre l'accès à distance aux applications ministérielles. Les régions ont mentionné n'avoir reçu aucune ligne directrice de mise en œuvre et, par conséquent, qu'elles ont dû fixer leurs propres mesures de sécurité avant la distribution des équipements.

Plan de la Sécurité de la TI des Opérations – Outre la direction générale de l'Infrastructure, la direction générale des Opérations du secteur des Systèmes a aussi un rôle à jouer en matière de sécurité de la TI. Le groupe de la Sécurité de la TI des Opérations procède actuellement à la dotation de postes au sein de la nouvelle organisation, pour répondre aux besoins des composantes de sécurité des réseaux, des plateformes et du système EasyLock. Le BVI croit comprendre qu'une fois terminée la dotation de ses postes, le groupe des Opérations élaborera un plan de sécurité opérationnelle en bonne et due forme.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

PLANNIFICATION (3)

Recommandation

- *Un plan opérationnel sur la sécurité de la TI doit être élaboré conjointement par les ACR, les CTI et les CRHC.*

Nota : Tout plan d'action découlant des recommandations susmentionnées doit tenir compte de celles concernant la Structure et l'Organisation énoncées dans le présent rapport.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

SENSIBILISATION (1)
Faible visibilité

Aucun programme ministériel de sensibilisation à la sécurité de la TI
- Séances régionales de sensibilisation à la sécurité - axées sur la sécurité physique/personnelle, rarement sur la TI
- Certaines régions n 'offrent pas couramment de séances de sensibilisation à la sécurité
- La Sécurité de la TI des Opérations doit se charger d 'élaborer un programme de sensibilisation à la sécurité de la TI
- De nombreux gestionnaires ignorent leur rôle et leurs responsabilités en matière de sécurité de la TI

Aucun programme ministériel de sensibilisation à la sécurité de la TI – DRHC ne s'est pas encore doté d'un programme ministériel de sensibilisation à la sécurité de la TI. Les agents de sécurité ministériels et régionaux ne se sont toujours occupés que de sécurité physique et du personnel; la sécurité de la TI incombant au secteur des Systèmes de l'AC. Le nouveau personnel n'est pas toujours mis au courant de ses responsabilités et obligations redditionnelles concernant la sécurité de la TI, ni des règles et règlements ministériels en cette matière, puisque aucune séance de sensibilisation ministérielle n'aborde le sujet.

Initiatives de sensibilisation à la sécurité de la TI – Le BVI a constaté que certaines initiatives ont été mises de l'avant pour accroître la sensibilité à la sécurité de la TI et qu'elles ont été bien accueillies.

- Les participants à un symposium sur la sécurité organisé récemment à l'AC ont affirmé au BVI que la sensibilisation à la sécurité de la TI a été l'un des sujets abordés. Par contre, comme le symposium s'adressait aux employés du secteur des Systèmes de l'AC (Opérations, CTI), les régions n'ont pas été en mesure d'y participer.

- Un porte-parole des Opérations de l'AC a été invité à aborder précisément la sécurité de la TI lors d'une conférence sur les technologies des réseaux locaux (« LAN Tech 99 Conference », organisée par la région de l'Ontario.

- Un ARS a pris l'initiative d'inviter un coordonnateur de la sécurité d'un CTI à participer à des séances régionales/locales de sensibilisation à la sécurité traitant précisément de la sécurité de la TI.

- Le BVI a également constaté que la région du Nouveau-Brunswick collabore étroitement avec la GRC, qui l'aide à traiter les incidents touchant la sécurité de la TI.

- DRHC a conclu une entente avec la GRC pour la tenue d'ateliers sur la sécurité de la TI dans l'administration des réseaux locaux.

Responsabilités du personnel et des gestionnaires en matière de sécurité – Le BVI a constaté que la sécurité de la TI n'occupe pas une place importante et n'est pas ancrée dans la culture institutionnelle de DRHC. Bien que la plupart des gestionnaires et du personnel soient au courant de l'importance du sujet, il importe de faire en sorte que chacun comprenne bien son rôle, ses responsabilités et ses obligations redditionnelles à ce chapitre.

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

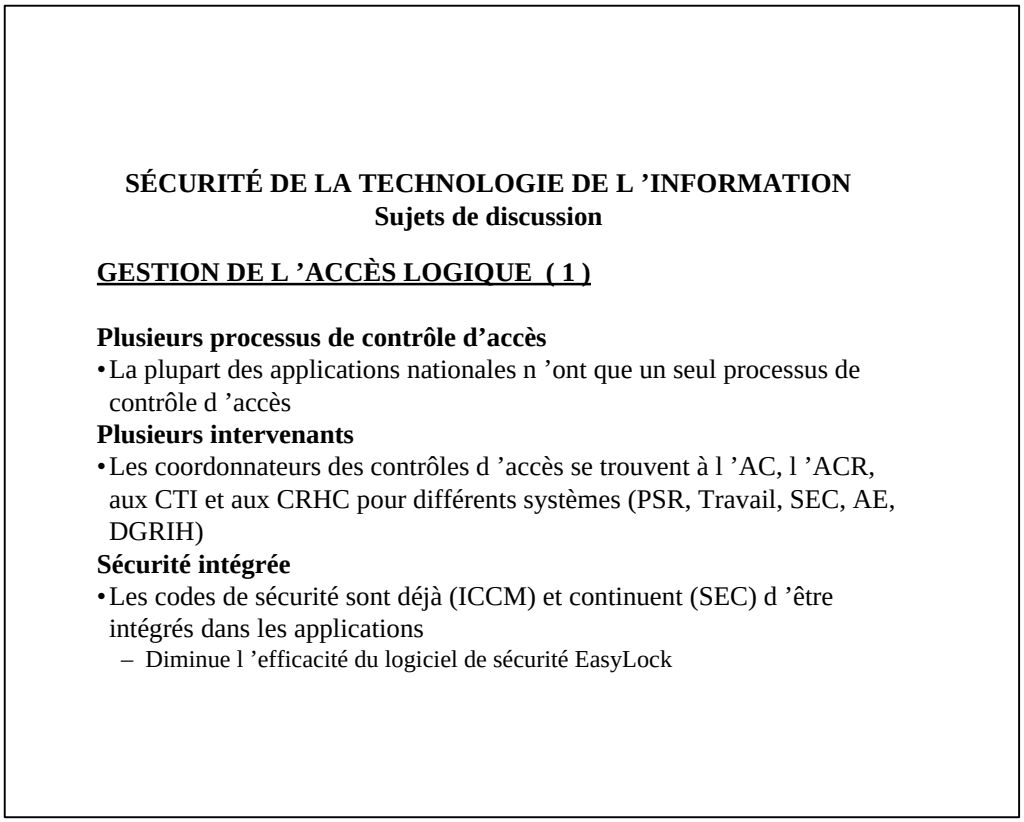
SENSIBILISATION (2)

Recommandation

- *DRHC doit adopter comme priorité l 'élaboration d'un programme officiel de sensibilisation à la sécurité de la TI et l 'offrir à intervalles réguliers au personnel national, régional et local.*

Ignorance des responsabilités et des obligations redditionnelles en matière de sécurité de la TI – Les directeurs et les gestionnaires de CRHC sont au courant des responsabilités qui leur incombent en matière de sécurité quant à la protection des lieux physiques, des biens et de la sécurité personnelle des employés et des clients. Par contre, la sécurité de la TI est principalement perçue comme étant d'ordre technique et gérée par l'administrateur du réseau local ou une personne ou un groupe relevant de l'ACR et/ou de l'AC. En outre, le personnel ne connaît pas exactement ses responsabilités quant à la sécurité de la TI. Comme l'a souligné la GRC, toute culture de gestion dynamique qui reconnaît l'importance de la sécurité de la TI reconnaît habituellement aussi celle de sensibiliser l'organisation à ce sujet.

Avantages d'un programme de sensibilisation – Les avantages de tenir des séances de sensibilisation à la sécurité de la TI en bonne et due forme sont notamment qu'elles permettent la diffusion de politiques, de pratiques et de responsabilités à jour. L'importance d'une telle sensibilisation prend tout son sens dans le virage de DRHC vers des technologies et des produits axés sur le Web, comme le commerce électronique et les infrastructures à clés publiques. Un certain nombre de personnes interviewées ont affirmé au BVI que le programme de sensibilisation à la sécurité de DRHC devrait également être offert aux tiers chargés de la prestation des programmes ainsi qu'aux employés provinciaux chargés de l'application des EDMT.



Le processus de contrôle d'accès logique est imprécis – Le processus de contrôle d'accès logique varie d'un secteur ministériel à l'autre, parce que les différents coordonnateurs du contrôle d'accès répartis dans divers sites utilisent des logiciels variés (EasyLock, Top Secret et systèmes d'exploitation des réseaux locaux) pour différents systèmes. Un telle variété de pratiques ne fait qu'accroître les coûts administratifs et l'inefficacité des opérations.

Le processus lié à l'octroi d'identificateurs de l'utilisateur, de mots de passe et de droits d'accès spécifiques à des applications ministérielles varie selon chaque organisation – Le processus de traitement des codes d'utilisateur ou mots de passe pour accéder aux applications des ordinateurs centraux (OC) varie selon le système et l'organisation. Un coordonnateur des contrôles d'accès est nommé pour chacune des applications nationales données. Ils travaillent à l'AC, dans les ACR, les CTI et les CRHC. Comme le mentionne le chapitre sur la structure et l'organisation, l'administration des codes d'accès et des mots de passe liés aux applications ministérielles et aux réseaux locaux est inégale à travers les différents secteurs de DRHC. Voici quelques exemples.

- Les gestionnaires autorisés des CRHC et des ACR transmettent directement aux coordonnateurs de la sécurité du CTI les demandes concernant les applications de l'AC et de la DGRIG, tandis que les demandes d'accès au SEC sont d'abord soumises à la vérification d'un coordonnateur régional et ensuite transmises aux coordonnateurs de la sécurité du CTI.

- Les demandes relatives au Régime de pensions du Canada (RPC) et à la Sécurité de la vieillesse (SV) des PSR sont d'abord transmises aux agents de la sécurité des contrôles d'accès des PSR, qui travaillent indépendamment des CTI. Ces agents transmettent ensuite les demandes à l'AC (Systèmes/Opérations – Sécurité).

- Les demandes relatives au Système d'information des agents du Travail (SIAT) et les systèmes des agents mobiles de l'adaptation du travail, bien qu'il ne s'agisse pas d'applications d'un OP, sont expédiées à l'un des cinq administrateurs régionaux de bases de données, qui travaillent également chacun de leur côté et ne profitent pas de l'efficacité du logiciel EasyLock des CTI.

Les règles et la structure de contrôle sont intégrées dans les applications ministérielles – Avant EasyLock, les règles d'accès et la structure de contrôle étaient intégrées à chacune des applications nationales. Pour profiter de la procédure unique d'entrée en communication de EasyLock, certaines anciennes applications devront être dotées de fonctions de sécurité intégrées pour que ce logiciel puissent être installé. Actuellement, les mécanismes de sécurité des applications telles le SEC sont intégrées au programme. De telles pratiques diminuent l'efficacité de EasyLock et ce genre de mécanisme de sécurité doit être repensé.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

GESTION DE L'ACCÈS LOGIQUE (2)

Codes d 'utilisateur multiples pour une seule personne
- Différents niveaux d 'un même système exigent des codes d 'utilisateur différents

Contrôle inégal des droits d 'accès logiques aux applications nationales
- Les rapports EasyLock ont une valeur restreinte
- Des mesures réactives sont souvent employées pour annuler ou supprimer les droits d 'accès

Protection pare-feu satisfaisante
- Les essais de pénétration effectués au printemps de 1999 ont été concluants.

Codes d'utilisateur multiples – De plus, chaque application ministérielle a son identification de l'utilisateur, mot de passe et contrôle d'accès. Certains employés ont besoin d'accéder à différents niveaux du système (p.ex. SAGE) dans le cadre de leur travail, c'est pourquoi une même personne ne peut avoir de multiples codes d'utilisateur et mots de passe. La prolifération de ces codes et mots de passe à travers DRHC pour accéder aux applications ministérielles en est le résultat.

Contrôle inégal – En ce qui a trait aux applications nationales fonctionnant à partir des ordinateurs centraux Unisys, les CTI doivent dresser des rapports EasyLock mensuels énumérant les utilisateurs par centre de responsabilité et application utilisée, et indiquant la dernière date de changement du mot de passe. Par contre les CTI ne produisent pas tous le rapport EasyLock sur une base mensuelle. La plupart des destinataires du rapport estiment qu'il leur est peu utile comte tenu de son mince contenu et souhaitent qu'il indique également le profil et le rôle de l'application pour chaque utilisateur. À titre d'exemple chaque coordonnateur régional du SEC a affirmé qu'il serait utile de savoir à quels écrans (définis comme « Rôles » dans le SEC) ont accès chacun des utilisateurs. Un tel niveau de détail permettrait de savoir si un utilisateur a des codes d'accès conflictuels à un même ou à différents systèmes, pouvant ainsi compromettre l'intégrité des systèmes ou se livrer à des activités illégales. Le BIV a appris qu'autrefois, certains rapports (p.ex. Reporter III) identifiaient les profils/rôles dans le cadre de chaque application et permettaient aux régions d'éliminer les anciens profils d'utilisateurs et de les remplacer par de nouveaux, assurant ainsi l'intégrité des capacités à travers les applications. L'une des régions continue de demander ce rapport annuellement, compte tenu de son utilité sur le plan de la sécurité de la TI.

Des **mesures réactives** sont couramment adoptées pour corriger les problèmes de droits d'accès logique. Le processus actuel est décentralisé et la responsabilité incombe au gestionnaire du CR, qui informe tous les intéressés (finances, personnel, TI et autres) des mouvements de personnels. Les administrateurs de RL ont affirmé pouvoir agir lorsqu'ils sont mis au courant de codes d'utilisateurs ou de mots de passe inactifs, mais que les rapports en faisant état ne sont pas facilement disponibles. Une marche à suivre officielle s'impose pour faire en sorte que DRHC puisse supprimer ou modifier les droits d'accès logiques en temps opportun.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

GESTION DE L'ACCÈS LOGIQUE (3)

Les contrôles d'accès au réseau varient

- l 'intégrité des demandes des gestionnaires reçues par courrier électronique est difficilement vérifiable
- le suivi des codes d 'utilisateur des RL et des « utilisateurs privilégiés » n 'est pas toujours effectué

Bonne mesures de sécurité proactives pour contrôler l 'accès à l 'Internet

- DRHC est doté de bonne méthodes de contrôle d 'utilisation d 'Internet
- Les journaux Internet peuvent ne pas permettre de confirmer qui est la personne ayant fait un mauvais usage d 'Internet

Intégrité des demandes faites par courrier électronique – Il arrive souvent que les gestionnaires fassent parvenir par courrier électronique aux services intéressés (p.ex. Travail, EDMT, ACAR des PSR, coordonnateurs de la sécurité des TCI) leurs demandes d'autorisation d'accès à certains niveaux d'une application donnée pour un membre de leur personnel. Le BVI a appris que seuls les gestionnaires et les administrateurs de réseaux locaux autorisés (et quelques autres personnes) étaient autorisés à transmettre ces demandes par courrier électronique. Comme leurs lieux de travail sont très dispersés, les autorités compétentes ne sont pas toujours en mesure de vérifier l'intégrité de ces messages électroniques; la plupart sont acceptés tels quels et traités normalement. Par contre, le BVI a noté qu'il arrive souvent que ces gestionnaires autorisés confient leurs mots de passe à un collègue, comme un adjoint administratif, chargé de vérifier les messages électroniques reçus en leur absence. Cette pratique permettrait à une personne non autorisée d'expédier un message électronique aux autorités compétentes pour demander l'accès à une application de DRHC.

Suivi des codes d'utilisateur des RL – Certains administrateurs de RL passent en revue la liste des utilisateurs qui ont accès à leurs réseaux, d'autres pas. Aucun administrateur de RL n'était au courant de l'existence de lignes directrices opérationnelles sur la fréquence à laquelle les listes et les journaux d'accès doivent être contrôlés. Les gestionnaires sont censés informer leurs administrateurs de RL lorsque le changement de statut d'un employé justifie un changement de droits et de niveau d'accès. Toutefois, tel n'est pas toujours le cas. Un administrateur de RL a affirmé au BVI que le moyen le plus répandu de se tenir au courant des changements dans le statut des employés ou les droits ou niveaux d'accès au RL était d'assister à la réception en l'honneur du « départ » ou de la « promotion » de l'employé qui quitte. Les administrateurs de

RL ne sont malheureusement pas toujours invités à ces réceptions, particulièrement dans les grands bureaux.

Suivi des « utilisateurs privilégiés » - Les « utilisateurs privilégiés » sont principalement les employés des systèmes qui ont besoin de droits d'accès exclusifs aux logiciels des gros ordinateurs, aux systèmes d'exploitation et aux applications ministérielles de DRHC pour effectuer des travaux techniques (p.ex. gestion de bases de données). Les représentants des CTI ont indiqué au BVI que les rapports ne sont pas actuellement formatés pour indiquer quels codes d'utilisateur « privilégiés » n'ont pas été utilisés depuis un certain temps. La création de tels rapports permettrait aux responsables de la sécurité des CTI de faire le suivi des gestionnaires/utilisateurs pour veiller à l'intégrité des codes d'utilisateurs « privilégiés » inactifs. En outre, rien n'indique qu'il n'en est pas également ainsi pour ce qui est des systèmes du Travail (LOIS) et des PSR (RPC, SV).

Surveillance de l'Internet – attention aux statistiques présentées – La plupart des régions ont installé Netscape directement dans les postes de travail (disque dur) plutôt que d'en offrir l'accès par l'entremise du serveur du RL. Cette ancienne pratique permet à un utilisateur d'accéder à Internet à partir de n'importe quel poste de travail en outrepassant (« annulant ») la procédure d'ouverture de session. Dans un tel cas, les journaux de vérification peuvent identifier l'ordinateur (Adresse IP) qui a contacté un site Web donné, mas pas l'utilisateur, puisque le processus d'identification de l'utilisateur (ouverture d'une session) n'a pas eu lieu. L'une des régions visitées a installé Netscape sur le serveur du RL. Tout utilisateur désirant se brancher à Internet doit suivre une procédure officielle, qui identifie l'utilisateur (à moins que l'utilisateur ait communiqué sont code d'utilisateur ou son mot de passe à quelqu'un d'autre).

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Sujets de discussion

GESTION DE L'ACCÈS LOGIQUE (4)

Contrôle déficient des départs et des mouvements de personnel

- Les méthodes varient et il est impossible de confirmer que les droits d 'accès ont été annulés
- Le certificat de cessation d 'emploi de DRHC ne précise pas l 'annulation des droits d 'accès logiques
- Les risques sont proportionnelles à l 'accroissement du télétravail et de l 'accès à distance

Utilisation irrégulière de l 'option du programme économiseur d'écran

- Économiseur d 'écran - outil sécuritaire facile à utiliser (et efficace)… mais qui l'est rarement

Départs et mouvements de personnel – Les procédures liées aux départs et aux mouvements de personnel ne permettent pas d'attester que leurs droits d'accès logique ont été annulés ou modifiés. Les mécanismes actuels concernant la fin d'emploi sont axés sur le formulaire ADM 5017 « Certificat de cessation d'emploi ». À l'examen de ce processus, le BVI a constaté que ce formulaire ne précise aucune mesure particulière concernant la TI qui permettrait de s'assurer que les droits d'accès logiques des employés qui quittent ont été modifiés, s'il y a lieu.

Tous les employés de DRHC ont accès à l'Internet et plusieurs ont des droits d'accès à distance leur permettant d'utiliser le courrier électronique, l'Internet ou les applications ministérielles dans le cadre du télétravail. Il est urgent de veiller à ce que tous ces droits d'accès soient modifiés aussitôt que possible lorsqu'un employé change de statut.

Les **économiseurs d'écran** sont des outils électroniques offrant de bonnes mesures de sécurité s'ils sont utilisés conjointement avec l'option permettant d'adopter un « mot de passe ». Dans un tel cas, lorsque l'utilisateur s'éloigne de son poste de travail, l'accès à son ordinateur de bureau ou portatif est interdit à moins que ne soit inscrit le bon mot de passe qui désactive l'économiseur d'écran. Le BVI a constaté que l'utilisation de cette option est laissée à la discrétion des utilisateurs, qui l'utilisent rarement. Dans l'une des régions visitées, les utilisateurs doivent utiliser l'option économiseur d'écran du logiciel « Microsoft/Windows 95 » plutôt qu'un autre économiseur personnalisé. Outre l'aspect sécuritaire additionnel, cet économiseur d'écran autorisé par DRHC simplifie l'architecture du système et normalise les produits utilisés.

SÉCURITÉ DE LA TECHNOLOGIE DE L 'INFORMATION
Sujets de discussion

GESTION DE L 'ACCÈS LOGIQUE (5)

Recommandations

- *DRHC doit revoir ses mécanismes de gestion des codes et des mots de passe d 'utilisateurs ainsi que des droits d 'accès, afin de minimiser les coûts administratifs, normaliser les processus, favoriser le contrôle et la responsabilisation et veiller à ce que le personnel soit au courant de ses responsabilités sécuritaires en ce qui concerne leus codes d 'utilisateur et leurs mots de passe.*
- *DRHC doit améliorer les mécanismes entourant les départs ou les mouvements de personnel de manière à modifier rapidement tous les codes d 'utilisateur et mots de passe ainsi que les droits d 'accès logique.*
- *En ce qui concerne les mots de passe des économiseurs d 'écran, le groupe de la sécurité de la TI des Opérations devrait*
  - *s 'assurer que le sujet figure aux programmes de sensibilisation à venir et souligner les avantages d 'une telle mesure de sécurité supplémentaire*
  - *concevoir une directive nationale pour inciter les régions et les CRHC à inviter tout leur personnel à adopter cette mesure de sécurité.*

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Sujets de discussion

BIENS PROPRES À LA TI - MATÉRIELS ET LOGICIELS (1)

L'inventaire des biens propres à la TI est à jour

- l'approche de l'an 2000 a eu pour effet que les biens ont été inventoriés
- « NetWizard » devrait aider à tenir l'inventaire à jour

Les mesures de sécurité concernant les ordinateurs portatifs s 'améliorent

- Diffusion nationale de 600 exemplaires du logiciel cryptographique Entrust ICE
- Les logiciels antivirus pour les ordinateurs portatifs ne sont peut-être pas aussi à jour que ceux des ordinateurs de bureau.

Fiabilité de l'inventaire des biens propres aux TI – L'un des projets entrepris par DRHC en vue du passage à l'an 2000 a permis de dresser l'inventaire des biens propres aux TI. Le défi est maintenant de tenir cet inventaire à jour, et c'est dans ce but que l'AC a choisi NetWizard, un logiciel facilitant la mise à jour des inventaires. DRHC procède actuellement à la mise en place de NetWizard.

Sécurité des ordinateurs portatifs – Le personnel de DRHC n'a pas toute la même perception en ce qui concerne les mesures de sécurité associées aux ordinateurs portatifs. Le BVI a constaté que la partie du Guide sur la politique et les procédures de sécurité de DRHC consacrée au télétravail aborde les mesures de sécurité relatives à l'utilisation d'ordinateurs portatifs et de l'information qu'ils contiennent. Par contre, certains points précis comme le cryptage de données sur disque dur et les accessoires de courrier électronique ne sont pas abordés. Le BVI croit comprendre que DRHC procède actuellement à l'essai des logiciels Entrust ICE et RSA SecurPC pour ce qui est du cryptage des disques durs.

Des inquiétudes ont été soulevées quant à la fiabilité des logiciels antivirus utilisés dans les ordinateurs portatifs. Certains croient que les ordinateurs personnels ne sont pas mis à niveau avec la même diligence que les ordinateurs des postes de travail et les serveurs. Bon nombre des personnes interviewées ont indiqué qu'elles n'étaient au courant d'aucune politique ministérielle particulière visant les ordinateurs portatifs, même si le Guide sur la politique et les procédures de sécurité de DRHC consacre une partie entière aux « ordinateurs portatifs ».

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Sujets de discussion

BIENS PROPRES À LA TI - MATÉRIELS ET LOGICIELS (2)

- **Aucune certitude que les disques durs de DRHC sont nettoyés avant leur élimination**
- La marche à suivre pour l 'effacement du contenu des disques dure varie
- **Des mesures réactives sont souvent utilisées pour récupérer des biens propres à la TI**
- Les méthodes de récupération varient
- Le certificat de cessation d 'emploi de DRHC ne précise rien au sujet des « biens propres à la TI »
- Une plus grande diligence s 'impose en raison de l 'accroissement de popularité des ordinateurs portatifs, du télétravail et de l 'accès à distance et du nombre d 'ordinateurs de DRHC se trouvant à la résidence d 'employés.

Nettoyage des disques durs – Pour suivre l'évolution des nouvelles technologies, DRHC remplace régulièrement les ordinateurs de bureau, les ordinateurs portatifs et les serveurs. Avant d'éliminer le matériel, il est important de veiller à ce que l'information que contiennent les disques durs soit effacée. Rien ne permet de certifier que tous les disques durs sont vidés de données potentiellement délicates appartenant à DRHC avant que ne soit éliminé le matériel, puisque le processus de démagnétisation ou de « nettoyage » n'est pas appliqué uniformément au sein du ministère. L'évaluation a révélé l'existence de procédures différentes et, dans certains cas, la personne interviewée ne pouvait confirmer l'existence d'une telle procédure.

Lorsque le BVI a demandé la politique de DRHC sur la question, l'AC nous a fourni un exemplaire du document « Procedure for Wiping Protected Information on Hard Disks, Employment and Immigration Canada, September, 1992 ». Nulle personne rencontrée lors de nos visites aux sites régionaux ou locaux ne connaissait ce document.

Mesures réactives souvent utilisées pour récupérer des biens de TI – Un fois qu'un employé quitte un centre de responsabilité (CR), il arrive souvent que le gestionnaire se rende compte « après coup » que l'employé pourrait avoir en sa possession un ordinateur portatif ou autre matériel de TI. Lorsqu'ils quittent un CR, les employés doivent s'assurer d'avoir rempli le formulaire « Certificat de cessation d'emploi – ADM 5017 ». Les gestionnaires de CR utilisent ce formulaire pour attester que l'employé a remis ses cartes d'appel, laissez-passer de sécurité, cadenas, clés et autres. Par contre, ce formulaire ne mentionne pas expressément les biens de TI. Par conséquent, il arrive parfois qu'une personne quitte DRHC et soit toujours en possession d'un ordinateur portatif, d'une imprimante, d'un logiciel d'accès à distance et autres. Il est déjà arrivé que l'on ait demandé à un ancien employé de DRHC de retourner un ordinateur portatif

après son départ du ministère, et que l'employé ait affirmé l'avoir déjà fait; cet ordinateur portatif n'a jamais été retrouvé.

Compte tenu du mode de fonctionnement actuel, il arrive fréquemment que les employés aient chez eux un ordinateur portatif, un ordinateur de bureau ou autre matériel de TI appartenant à DRHC. Des mécanismes de contrôle officiels de ces biens de TI doivent être adoptés pour que les mesures adéquates soient prises en temps opportun et pour veiller à ce que DRHC soit en mesure de récupérer ces biens.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Sujets de discussion

BIENS PROPRES À LA TI - MATÉRIELS ET LOGICIELS (3)

Recommandations

- *Il est souhaitable que la Sécurité de la TI des Opérations examine :*
  - *les processus de mise à niveau des logiciels antivirus destinés aux ordinateurs portatifs;*
  - *les politiques set les procédures liées à l élimination des données des disques durs; et*
  - *les méthodes entourant les départs ou les mouvements de personnel de sorte que tous les biens propres à la TI soient préalablement récupérés.*

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Sujets de discussion

DIVERS POINTS TOUCHANT LA SÉCURITÉ (1)

Les mesures touchant la sécurité physique et le méthodes de sauvegarde sont généralement acceptables

- Les agents de la sécurité régionale procèdent à des EMR - surtout d 'ordre « physique » et sans rapport avec la « TI »
- Les CTI, les ACR et les CRHC suivent les procédures de secours établies par DRHC

Les mesures concernant le stockage externe varient

- Les méthodes employées par les CTI sont convenables
- Quelques ACR et CRHC n 'entreposent pas leurs copies de sauvegarde à l 'extérieur

Les spécifications physiques des pièces réservées aux RL et des installations de stockage externe sont inconnues

- Au cours des visites, personne ne connaissait les spécifications d'une pièce réservée à un RL, ni celles des installations de stockage externe

Sécurité physique – Autrefois, les projets de TI de DRHC ne faisaient pas tous l'objet d'une EMR. Depuis que le coordonnateur de la sécurité de la TI de l'AC siège au Comité d'examen des projets (CEP), tous les projets de ce comité sont examinés pour faire en sorte que les questions de conformité et les préoccupations concernant la TI sont abordées. Toutefois, rien ne garantit que les autres projets de TI qui ne seront pas soumis au CEP seront soumis à une EMR.

Au niveau régional et local, les ASR se chargent de procéder aux EMR, à la demande de leur ACR ou de leur bureau local. Ils ont déclaré que ces EMR étaient principalement axées sur des questions de sécurité physique et que le volet de la TI n'était souvent pas abordé. Dans les deux régions visitées, le modèle d'EMR décrit dans le guide régional de procédures et de politique en matière de sécurité sert à l'élaboration des EMR. L'une des régions a l'intention de procéder à des EMR dans dix CRHC différents.

Les EMR qui incluent un volet touchant la TI sont habituellement plus complexes à réaliser puisqu'elles exigent des compétences spécialisées en la matière, que la plupart des ASR n'ont pas. Les guides régionaux de procédures et de politique en matière de sécurité indiquent que les EMR incombent au coordonateur régional de la sécurité de la TI. Par contre, puisque certaines régions croient n'avoir aucun employé assumant ce rôle au sein de leur organisation régionale, les méthodes d'EMR employées au niveau régional et local font peut-être mal ressortir les risques et les menaces associés à la TI.

DRHC a récemment adopté une nouvelle politique de fonctionnement des RL exigeant un cycle de sauvegarde et de stockage externe de 20 jours. Le BVI a remarqué que la mise en œuvre de cette politique en est à un stade ou l'autre dans toutes les régions visitées.

Durant ses visites aux ACR, aux bureaux locaux et aux CTI, le BVI a visité plusieurs pièces réservées aux RL ainsi que plusieurs installations de stockage externe, ce qui lui a permis de constater les différentes caractéristiques des mesures de sécurité physique en place.

De l'avis de l'équipe de vérification, chaque endroit semblait posséder des mécanismes de protection physique adéquats. Par contre, personne n'était en mesure d'identifier ou de présenter de norme ni de directive nationale en matière de sécurité physique en ce qui a trait à la construction de salles réservées aux RL, le choix d'installations de stockage externes ni sur la conduite d'examens de sécurité de la TI et d'EMR.

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION

Sujets de discussion

DIVERS POINTS TOUCHANT LA SÉCURITÉ (2)

Brèche de la sécurité de la TI

- L 'expression « brèche de la sécurité de la TI » n 'a pas été proprement définie
- Les « brèches de la sécurité de la TI » ne sont pas toujours rapportées
- **Personnel (embauche)**

16(2)(c)

La définition des brèches de sécurité de la TI n'a pas encore été énoncée clairement et aucun système officiel permettant d'en faire rapport n'a encore été établi. Les personnes à qui l'on a demandé de définir et de décrire ce qui constituait une « brèche de sécurité de la TI » ne connaissaient ni la signification exacte de l'expression, ni la manière d'en faire rapport. Le BVI a noté que tous les guides de procédures et de politique régionaux en matière de sécurité de DRHC (liste de contrôle EMR, partie G, Sécurité de la TI, no 2. RL) mentionnaient la question suivante : « *Les préoccupations et les incidents touchant la sécurité sont-ils rapportés aux responsables de la Sécurité de la TI* ? ». Toutefois, puisque les régions n'estiment pas être dotées d'un coordonnateur régional de la sécurité de la TI, la plupart d'entre elles ne savaient pas trop comment composer avec de tels incidents. Par conséquent, le BVI en a conclu que plusieurs brèches de sécurité de la TI à DRHC pourraient ne pas être documentées, rapportées ni comptabilisées, malgré que la PGS du gouvernement stipule que les brèches de sécurité (incluant la TI) doivent être rapportées au sous-chef de l'organisation.

La plupart des employés de DRHC possèdent la cote de sécurité Vérification de fiabilité approfondie (VFA). Cela les autorise à accéder à des données « protégées B » selon la nécessité de connaître ces renseignements pour l'exercice de leurs fonctions. Les directives du Conseil du Trésor précisent que tous les employés doivent être soumis à une enquête de VFA, quoique la procédure puisse être outrepassée dans le cas d'étudiants ou d'employés embauchés pour une courte durée (moins de six mois).

16(2)(c)

16(2)(c)

SÉCURITÉ DE LA TECHNOLOGIE DE LA L 'INFORMATION

Sujets de discussion

DIVERS POINTS TOUCHANT LA SÉCURITÉ (3)

Mesures de contrôle de sécurité incohérentes

- Il existe des directives sur le contrôle du rendement au sujet de l 'Internet, des ordinateurs centraux et des RL
- Les directives sur le contrôle de la sécurité ne sont pas aussi bien définies
- Les journaux de sécurité des RL ne sont pas activés de façon uniforme dans tous les secteurs de DRHC

Recommandations

- *La Sécurité de la TI des Opérations doit prendre les mesures nécessaires pour améliorer les situations rapportées dans la présente partie.*
- *Plusieurs lacunes rapportées peuvent être contrées par un simple rappel de politique ou la rédaction de lignes directrices et doivent faire partie d'un ensemble de mesures de sensibilisation.*

Il existe des incohérences en ce qui a trait au contrôle et à l'examen des questions de sécurité de la TI, parce qu'il n'existe aucune ligne directrice nationale ou régionale en la matière.

Les journaux opérationnels des réseaux sont produits par voie électronique, comme dans le cas de ceux sur les sites Internet qui ont été visités, les fichiers auxquels on a accédé par le biais des postes de travail, les résultats des demandes d'ouverture de sessions des usagers et les statistiques sur les temps de réponse. Outre le fait que les journaux sur la performance des RL soient examinés de près, les journaux sur la sécurité de la TI ne sont pas examinés couramment. Certains administrateurs de réseaux locaux ont affirmé ne pas activer les journaux de sécurité au niveau du serveur puisqu'ils « n'éprouvaient aucune difficulté sur le plan de la sécurité de la TI ». Toutefois, ces mêmes personnes ont concédé être incapables d'en faire la preuve puisqu'ils n'ont pu présenter ni contrôler aucun journal de vérification ou de sécurité de RL. En outre, aucun administrateur de RL n'était au courant de lignes directrices ou de politiques opérationnelles précisant quels journaux de sécurité ou de vérification pouvaient être tenus, ni la période durant laquelle de tels journaux devaient être conservés.

Les journaux de sécurité de la TI sont utiles lorsqu'il s'agit d'établir des statistiques pouvant servir à dégager des tendances et étayer des enquêtes sur une brèche de sécurité de la TI. L'ASR de la région du Québec travaille en étroite collaboration avec le coordonnateur de la sécurité du CTI de Montréal et utilise fréquemment des journaux TI courants et spéciaux pour enquêter dans des cas de fraude. L'an dernier, l'ASR a mis à jour 75 cas de fraude perpétrées par un mauvais usage de la TI. Le BVI est d'avis que des résultats semblables pourraient être obtenus si d'autres régions utilisaient les journaux de sécurité et de vérification plus diligemment pour déceler les cas de fraude.

ANNEXE A

CADRE DIRECTEUR DE LA TI POUR LE GOUVERNEMENT FÉDÉRAL

CONTEXTE

Nécessité de mettre en œuvre la sécurité pour la TI

Durant la dernière décennie, le gouvernement fédéral a passablement accéléré ses investissements dans le domaine de la technologie de l'information (TI). Ces investissements ont eu des retombées importantes en ce qui concerne l'amélioration de la productivité en matière de services au public, un accroissement de la compétitivité à l'échelle internationale dans la nouvelle économie mondiale et, ce qui est encore plus important, une amélioration des services aux Canadiens.

Il est important de souligner, toutefois, que cet investissement ne s'est pas fait sans entraîner de nouveaux risques. Il suffit de mentionner la tendance à la migration continue de la puissance informatique qui passe des systèmes centralisés aux ordinateurs de bureau et même au-delà aux points de service. De nombreuses mesures de protection, qui avaient atteint une certaine maturité dans les systèmes fermés, c'est-à-dire l'environnement informatique des ordinateurs centraux, n'ont toujours pas d'équivalent dans la nouvelle architecture ouverte, c'est-à-dire l'environnement client/serveur. Par conséquent, des informations et des services de valeur qui font appel à la TI et qui étaient auparavant protégés contre les violations de la confidentialité de même que les atteintes à l'intégrité et à la disponibilité sont désormais exposés à des risques plus importants.

Il est par conséquent d'une importance cruciale que les ministères mettent complètement en œuvre la politique du gouvernement concernant la sécurité et la norme opérationnelle en matière de Sécurité de la TI.

Besoins de surveillance liés à la PGS

La Politique du gouvernement concernant la sécurité (PGS) a été publiée pour la première fois en juin 1986. Elle a été révisée en 1987, et encore une fois en janvier 1990. La Politique sera de nouveau révisée et élargie au début de 1994. Une partie des nouvelles exigences liées à la Sécurité de la technologie de l'information (STI), notamment celles ayant trait à la sécurité des réseaux, reflètent les risques introduits par ces nouvelles technologies. L'une des principales exigences découlant de la PGS est celle de la surveillance. Cette exigence est habituellement satisfaite par la tenue de vérifications périodiques de la performance.

Les ministères doivent effectuer une vérification interne des éléments suivants :
- leur conformité à la politique; et
- l'efficacité et l'efficience avec laquelle ils la mettent en œuvre, au moins une fois tous les cinq ans; cette première vérification a été réalisée à la fin de 1993.

Même si l'exigence relative à la vérification pour l'ensemble de la PGS ne revient qu'une fois tous les cinq ans, des domaines en évolution aussi rapide que la STI devraient faire l'objet d'une vérification plus fréquente, si possible.

Le Secrétariat du Conseil du Trésor (SCT) utilise ces vérifications de même que les rapports produits par la GRC, le Centre de sécurité des télécommunications (CST), la Commission de la fonction publique et les Archives nationales pour surveiller la conformité des ministères à la politique du gouvernement concernant la sécurité.

La Direction générale de la vérification interne DHRC effectue des vérifications de la mise en œuvre de la PGS et de la norme opérationnelle liée à la STI.

Les vérificateurs du BVI – DRHC se proposent d'évaluer, au sens large, les éléments suivants :
- la conformité du ministère à la politique du sécurité et à la norme opérationnelle en matière de STI;
- l'efficacité de la mise en œuvre de la Politique concernant la sécurité et de la normes opérationnelle en matière de STI; et
- l'efficience de la mise en œuvre de la Politique concernant la sécurité et de la norme opérationnelle en matière de STI.

Aux fins du présent document, les définitions suivantes sont utilisées :
- par efficacité on entend, l'atteinte des objectifs visés ou des niveaux de service prévus avec un minimum de résultats négatifs. Pour être efficace, un programme ou une activité de la STI doit aussi demeurer pertinent; et
- par efficience on entend, l'atteinte des résultats désirés au meilleur coût. L'efficience correspond au rapport entre les ressources utilisées (dollars, années-personnes, information et autres biens) et les résultats obtenus.

De manière plus spécifique, les objectifs, les critères et les procédures de la vérification permettront aux vérificateurs d'évaluer les éléments suivants :
- s'il existe une structure administrative et organisationnelle adéquate à l'appui de l'environnement STI;
- s'il existe des politiques, pratiques et procédures pertinentes et officielles concernant l'environnement STI;
- s'il existe un cadre de gestion des risques pertinent en matière de sécurité pour l'environnement TI; et
- si la direction réalise une économie appropriée dans l'environnement STI.

ENVIRONNEMENT DE SÉCURITÉ

Cadre de responsabilisation – Un principe fondamental de la PGS est la responsabilisation des sous-ministres en ce qui concerne la sécurité au sein de leurs ministères respectifs. À la fois la politique et les normes opérationnelles précisent les exigences auxquelles les ministères doivent se conformer. Les normes opérationnelles recommandent également l'application de mesures de protection à moins que l'évaluation de la menace et des risques (EMR) n'indique le contraire.

Les ministères peuvent excéder les normes en mettant en place des mesures de protection additionnelles si le sous-ministre les juge nécessaires afin de protéger l'information et les biens de nature sensible.

Si les ministères veulent mettre en œuvre des programmes qui soient à la fois efficients et efficaces, ils doivent être en mesure de les administrer dans le cadre de leurs mandats particuliers et en fonction de leurs priorités, leurs budgets et leurs cultures et environnements organisationnels. La Politique reconnaît cet élément en définissant les exigences globales visant à assurer un certain niveau de sécurité à l'intérieur du gouvernement ou d'un ministère tout en laissant la latitude nécessaire pour s'adapter aux conditions financières et autres.

Modèle de sécurité du gouvernement - Les normes du gouvernement en matière de sécurité décrivent un modèle de programme de sécurité ministériel possédant les caractéristiques suivantes :

- structure organisationnelle;
- procédures administratives; et
- trois (3) sous-systèmes :
    1. sécurité physique,
    2. sécurité de la technologie de l'information, et
    3. sécurité des personnes.

L'efficacité et l'efficience du programme global de sécurité dépend de la performance atteinte dans chacun de ces sous-systèmes. Par conséquent, lorsque la responsabilité des divers sous-systèmes est attribuée à diverses unités organisationnelles, ou encore lorsque cette responsabilité est décentralisée, les sous-systèmes devraient être structurés de manière à permettre la planification, la gestion et l'administration coopérative.

Modèle STI - La STI est souvent décrite comme la protection résultant d'un ensemble intégré de mesures conçues pour garantir la confidentialité de l'information stockée, traitée ou transmise sous forme électronique, l'intégrité de l'information et des procédés électroniques connexes, et la disponibilité des systèmes, réseaux et services.

La norme opérationnelle de la STI décrit un modèle possédant les caractéristiques suivantes :
- organisation et administration;
- opérations; et
- sept (7) autres sous-éléments :
    1. sécurité des personnes;
    2. sécurité physique,
    3. sécurité des matériels,
    4. sécurité des logiciels;
    5. sécurité des communications;
    6. sécurité en ce qui concerne les fuites d'information; et
    7. sécurité des réseaux.

L'efficacité et l'efficience du programme de sécurité de la STI dépend de la performance de chacun de ces sous-éléments. Par conséquent, lorsque la responsabilité des divers sous-éléments de la sécurité est attribuée à diverses unités organisationnelles, comme une sous-section de la sécurité informatique, et une sous-section de la sécurité des communications, ou encore lorsque cette responsabilité est décentralisée, les sous-éléments devraient être structurés de manière à permettre la planification, la gestion et l'administration coopérative.

La STI est optimale lorsqu'elle est acceptée comme faisant partie d'un ensemble d'autres exigences importantes que les développeurs de systèmes et les spécialistes de la maintenance doivent considérer. La STI n'est pas un élément à ajouter. Elle doit être considérée comme faisant partie intégrante de toute infrastructure de TI. Lorsqu'elle est gérée de manière appropriée, elle permet aux propriétaires de systèmes et de données d'obtenir un rendement sur leur investissement.

RÔLES ET RESPONSABILITÉS

1. **Représentant principal de la sécurité** – Les ministères doivent nommer un haut fonctionnaire qui représente le sous-ministre dans ses rapports avec le SCT concernant la politique et les normes en matière de sécurité. Le fonctionnaire nommé n'est pas nécessairement l'agent ministériel de la sécurité (voir ci-après).

2. **AMS** – Les ministères doivent aussi nommer un agent ministériel de la sécurité (AMS). L'AMS est aussi responsable de l'élaboration, la mise en œuvre, la mise à jour, la coordination et la surveillance d'un programme de sécurité ministériel conforme à la politique et aux normes en matière de sécurité.

3. **Coordonnateur STI** – Les ministères doivent nommer un coordonnateur de la Sécurité de la TI. Ce poste doit avoir au moins un rapport fonctionnel avec l'agent ministériel de la sécurité (AMS). Antérieurement, le coordonnateur STI correspondait au coordonnateur de la sécurité informatique; on peut toujours utiliser ce titre, si le ministère le souhaite.

4. **Autorité en matière de sécurité des communications** – La coordination de la sécurité concernant les fuites d'information et de la sécurité cryptographique doit faire partie du rôle de l'autorité en matière de sécurité des communications (agent de la sécurité des communications). Ce rôle peut être joué par le coordonnateur STI, une personne occupant un poste distinct ou encore par le CST qui agit au nom du ministère.

5. **Organismes responsables de la STI** – Il existe deux organismes responsables de la STI : la GRC et le CST. L'Équipe d'inspection et d'évaluation de la sécurité (EIES) de la GRC effectue des inspections de la Sécurité de la TI conformément à l'échéancier qui figure dans la norme opérationnelle de la STI. Le CST inspecte, teste et évalue les systèmes et procédures de SECOM. En outre, le Bureau national central des archives du CST vérifie les comptes SECOM ministériels; après quoi, il produit un rapport faisant des recommandations à l'intention du ministre ou du premier dirigeant.

Comités interministériels de la STI – Il existe deux comités interministériels de la STI qui traitent particulièrement des questions de la STI. Le Comité de la sécurité des communications fournit une orientation stratégique aux ministères participant concernant la gestion des matériels et des systèmes SECOM. Le Comité de la STI conseille la GRC, le CST et le CT en matière de STI.

Cadre de gestion des risques – La politique de sécurité exige des ministères qu'ils évaluent la menace et les risques auxquels s'exposent l'information et les biens de nature sensible, à sélectionner des mesures permettant d'éliminer ces risques, à mettre en œuvre des mesures de protection rentables, à élaborer des plans d'urgence et de reprise des activités, au besoin. La méthodologie du cycle de vie du développement des systèmes de TI devrait inclure les étapes appropriés pour :
- évaluer la menace et les risques pour les biens de TI; et
- choisir, certifier, accréditer, assurer la maintenance, surveiller et ajuster les mesures de protection.

S'il est correctement mis en œuvre, le processus de gestion des risques confirmera la nécessité de mettre en place des mesures minimales de protection et il indiquera s'il est nécessaire de mettre en place d'autres types ou d'autres niveaux de protection. Il permettra également d'obtenir une valeur ajoutée parce qu'il améliorera la sensibilisation et le soutien à l'égard du programme de la STI.

QUESTIONS LIÉES À LA TECHNOLOGIE DE L'INFORMATION – TENDANCES

Alors que les systèmes et les réseaux de TI des secteurs public et privé deviennent de plus en plus présents, décentralisés et interconnectés et que leur utilisation se libère de plus en plus des contraintes, la société devient plus vulnérable à l'augmentation de la menace qui peut entraîner des pertes au niveau de la confidentialité, de l'intégrité et de la disponibilité des données. La présente vérification recouvre plusieurs tendances, nous en décrirons dix ci-après.

Même si ces tendances s'appliquent à la fois aux secteur public et privé, certaines ont été décrites en adoptant davantage le point de vue du secteur public. La technologie de l'information a connu une expansion vers l'extérieur qui a changé tous les aspects des services gouvernementaux – des inspections effectuées dans les établissements des clients en passant par les centres de libre-service informatisés. Du point de vue de la STI, il est important de bien comprendre ces changements; d'identifier toute nouvelle vulnérabilité et menace qui peut découler de ces changements et de compenser tout risque inacceptable par la définition, la sélection, l'application et la surveillance de mesures de protection.

1. **Améliorer l'expertise de l'utilisateur final** – Les utilisateurs connaissent de mieux en mieux les ordinateurs et les télécommunications. Même si en un sens, c'est très positif, parce que cela permet d'obtenir un environnement très productif en matière de technologie de l'information, ce progrès comporte aussi ses mauvais côtés. On a longtemps dit que « une connaissance limitée peut avoir des effets désastreux ». Ce n'est pas moins vrai dans un environnement informatique et de télécommunications. Des personnes qui maîtrisent très bien la technologie et qui sont résolues à occasionner des pannes ou la dislocation des systèmes de technologie de l'information et de leurs données peuvent le faire avec une assez grande facilité. Donc, il est important de le noter, nous assistons aussi à une augmentation du nombre d'attaques dirigées contre les systèmes et les réseaux et ces attaques sont de plus en plus complexes.

2. **L'environnement de la TI change rapidement et devient de plus en plus complexe** – Les experts ont déclaré que toute l'information dans le monde double à peu près tous les quatre ans. On s'attend à ce qu'elle double tous les 18 mois d'ici l'an 2000. Avec cette accélération, il est nécessaire que la technologie de l'information arrive à faire plus, plus rapidement et encore mieux. Les nouvelles offres de produits et de services sont produites par les entreprises de haute technologie à un rythme rapide.

   Il est fréquent que la technologie de l'information soit mise à jour ou remplacée. Une vérification de la sécurité devrait faire en sorte que les évaluations de la menace et des risques soient mises à jour après des changements importants dans le domaine de la TI.

   En outre, il est de plus en plus difficile pour le personnel de la TI, et plus particulièrement pour le personnel de la STI, de se tenir à jour avec tous ces changements et cette complexité. Le personnel de la STI provient pour la plupart d'abord d'un environnement de la TI, et ensuite de la sécurité. Une formation appropriée et continue dans les deux champs de spécialité devrait être mise en place.

3. **Migration de la puissance informatique** – L'une des tendances les plus importantes est la migration de la puissance informatique qui passe des systèmes centralisés du gouvernement jusqu'aux ordinateurs de bureau, et va même plus loin jusqu'aux points de service. Le contrôle de la technologie est passé des groupes d'informatique centrale vers l'extérieur et s'est réparti de façon diffuse dans toute l'organisation. Les choses ne sont pas différentes à DRHC. Plusieurs intervenants doivent participer à l'élaboration des plans et des stratégies en TI de même qu'à la prise de décision en matière d'acquisition et de mise en œuvre. Les

personnes ne travaillent plus dans l'isolement : avec la mise en réseau, le groupe est devenu le point d'appui de l'unité de travail.

Mais toute cette approche fondée sur l'autonomie, et l'amélioration de la productivité et des niveaux de qualité qui en découle, n'est pas arrivée sans créer de remous. Parmi les nouveaux problèmes, on inclut notamment l'incompatibilité, l'impossibilité de s'interconnecter, l'affaiblissement des infrastructures de soutien et l'avènement de menaces et de vulnérabilités nouvelles et accrues. Les mesures de protection, qui avaient atteint une certaine maturité dans le système fermé de l'environnement des gros ordinateurs n'ont toujours pas trouvé d'équivalents dans la nouvelle architecture ouverte de l'environnement client/serveur. Cela signifie que des informations et des services valables qui reposaient largement sur AIT@ et qui étaient auparavant protégés raisonnablement contre les fuites d'information, les attaques contre l'intégrité et la disponibilité, sont désormais davantage exposés à certains risques.

4. **Convergence des réseaux et des ordinateurs** – Les ordinateurs ne sont plus des « îlots de puissance de traitement », comme ils l'étaient dans le passé. De même, les circuits de télécommunications ne sont plus des « bouts de fil ». Graduellement, les deux arrivent à un point de convergence. Maintenant que les services de télécommunications sont numériques, ils sont devenus en effet des ordinateurs eux-mêmes. Et les ordinateurs qui contrôlent ces réseaux sont programmés pour offrir un large éventail de services. Les deux éléments favorisent l'avènement d'une toute nouvelle génération de services à valeur ajoutée, comme le commerce électronique, les vidéo-conférences, le courrier électronique et les boîtes vocales. Cette gamme de services est illimitée, étant donné que les télécommunications évoluent des communications de base jusqu'à un service public d'information.

   Avec ce changement, il est de plus en plus difficile de déterminer quelle unité organisationnelle est responsable de certains domaines précis de la STI. Il est possible que trois organisations ou plus partagent les mêmes responsabilités : l'organisation de l'informatique centrale, l'organisation traditionnelle de SECOM et la traditionnelle organisation de la sécurité informatique. Il en résulte un possible chevauchement et une redondance dans l'application de la STI; ou même pire, les nouvelles menaces à la STI peuvent avoir le champ libre sans que personne ne s'en aperçoive. Ce changement a aussi entraîné une certaine fusion des unités organisationnelles traditionnelles de la sécurité informatique et de la SECOM en une seule unité de STI afin d'essayer d'uniformiser l'application des services et d'éviter la redondance.

5. **Impartition** – On définit par impartition le transfert de la totalité ou d'une partie des fonctions informatiques ou de télécommunications à un entrepreneur externe. L'impartition est devenue de plus en plus populaire, les organisations s'efforçant de trouver de nouveaux moyens d'économiser et de se concentrer encore davantage sur les fonctions liées aux activités fondamentales. Bon nombre de grandes organisations du secteur privé et des ministères ont déjà procédé à l'impartition de larges segments de leur environnement de TI : des opérations au développement des applications, en passant par la maintenance des logiciels. Même si l'impartition comporte de nombreux avantages, elle n'est pas sans avoir de mauvais côtés. Parmi ceux-ci, notons les coûts élevés du passage à la sous-traitance et une participation accrue de la haute direction. Encore plus important, du point de vue de la TI,

l'impartition signifie une perte de contrôle. Et il découle de cette perte de contrôle des vulnérabilités nouvelles et des menaces potentielles.

Il est donc d'une importance cruciale, avant de procéder à toute impartition, d'évaluer la menace et les risques pour la sécurité, de définir les besoins en matière de sécurité, de les intégrer dans le contrat avec l'entrepreneur, de les mettre en œuvre et finalement de les certifier. Des plans d'urgence éprouvés devraient être mis en place pour le cas où le fournisseur ne serait pas en mesure de poursuivre ses activités. Finalement, le contrat d'impartition devrait prévoir des inspections régulières et surprise, afin de pouvoir confirmer que les mesures de protection exigées en matière de STI sont en place.

6. **Microtisation** – Par microtisation, on entend une tendance relativement nouvelle à diminuer l'effectif d'une organisation, de même que de ses centres de données et ses installations afin d'obtenir une productivité optimale. La microtisation remplace la rationalisation qui visait simplement à faire passer les applications des gros ordinateurs aux mini-ordinateurs ou encore aux réseaux locaux (LAN). La microtisation se concentre sur les objectifs de la réduction des dépenses et l'amélioration du service à la clientèle.

   DRHC doit prendre soin de conserver suffisamment de personnel pour garantir que certaines tâches seront accomplies séparément. Dans certains cas de microtisation, il peut s'avérer impossible de maintenir une division adéquate des tâches dans tous les cas. Lorsque cela se produit, il faudrait prévoir d'autres mesures de protection.

7. **STI – Un argument de vente** – La STI devient de plus en plus un argument de vente en soi. Il s'agit là d'une conséquence directe de plusieurs tendances récentes.

   Dans le cadre de la restructuration et du recentrage du gouvernement, des organisations, y compris DRHC deviennent de plus en plus axées sur le client. Ces organisations sollicitent activement les clients pour qu'ils fassent connaître leurs besoins, dans le contexte de certaines offres de services précises. Parmi les clients externes, on inclut les Canadiens et les autres ministères.

   Par suite de l'attention soutenue qu'on leur accorde dans les médias, les personnes et les organisations sont de plus en plus au courant de la menace et des risques qui existent dans le nouveau village global électronique. Les médias s'intéressent fréquemment aux problèmes liés à l'informatique, comme les virus, les attaques perpétrées par un pirate informatique ou une tragédie vécue par une personne ou une entreprise ayant été victime d'une violation de l'intégrité d'un système ou encore la perte d'un service critique occasionnée par des pannes d'ordinateur.

   Les Canadiens et les clients internes du gouvernement ont des attentes croissantes en matière de qualité des services.

Toutes ces tendances réunies créent un environnement de clients qui insistent pour obtenir une protection adéquate de l'information qu'ils ont confiée et qui s'attendent à ce qu'on leur garantisse une protection complète de l'intégrité et de la disponibilité des services offerts qui reposent largement sur la TI.

La tendance voulant que la STI soit un avantage commercialisable se maintiendra aussi longtemps qu'il y aura une menace et des risques sérieux latents et inacceptables dans l'environnement de la TI.

Les vérificateurs devraient s'assurer que les développeurs de la TI demandent à leurs clients si ceux-ci désirent que la sécurité (qui s'exprime parfois par les clients par la paix de l'esprit ou la confiance) soit intégrée dans leurs systèmes.

8. **Investissement accru dans la TI** – Le vaste programme du gouvernement a créé le besoin d'améliorer constamment des services de haute qualité pour les Canadiens, dans un contexte de restrictions. Par conséquent, les ministères qui cherchent des moyens novateurs de relever ces défis découvrent qu'ils peuvent réaliser des gains substantiels en matière de productivité, de qualité des services et de coûts des opérations par des investissements dans la TI. À cette fin, le gouvernement canadien a dépensé 11 milliards de dollars pour faire l'acquisition de biens et de services en TI, entre 1986 et 1992. Cet investissement ne cesse de croître, en moyenne de 8 % par année. En 1993, il représentait une dépense d'environ 2 milliards de dollars qui se répartissent également entre l'informatique et les télécommunications.

   Sans un soutien qualifié et disponible pour maintenir cet investissement dans la TI, les systèmes et les réseaux ne pourront pas répondre aux attentes et remplir leurs promesses. On pourra subir rapidement des pertes inacceptables. Les ministères devraient élaborer des formules qui les aideront à calculer les dépenses nécessaires en matière de services de soutien à la TI, y compris ceux de la STI. De toute évidence, l'investissement dans la STI ne peut rester dans son état actuel pendant que l'ensemble des investissements réalisés dans la TI s'accélèrent chaque année, sans que cela n'entraîne des répercussions importantes.

9. **Systèmes partagés du gouvernement** – La politique gouvernementale favorise la transition vers des systèmes administratifs intégrés et communs en finance, ressources humaines, gestion des actifs et du matériel. La mise en œuvre de ces systèmes permettra d'utiliser de façon optimale des ressources limitées et des gestionnaires de soutien en nombre restreint et favorisera le transfert électronique de l'information. La TI partagée sera utilisée pour soutenir l'infrastructure du gouvernement par l'entremise d'outils comme le courrier électronique, les systèmes administratifs susmentionnés, les babillards électroniques et le commerce électronique.

   L'une des conséquences de cette transition est que le système partagé deviendra extrêmement réparti. On estime que le seul Système de rémunération de la fonction publique (SRFP) sera éventuellement accessible dans plus de 140 ministères, situés dans plus de 500 emplacements différents de même qu'à plus de 25 000 employés de la fonction publique. Cette répartition aura des répercussions profondes sur la STI. La conception, la mise en oeuvre et la maintenance de la STI deviennent de plus en plus complexes. Il faudra pouvoir compter sur

une collaboration interministérielle considérablement améliorée pour garantir une application uniforme des mesures de protection de sorte qu'il subsiste très peu de maillons faibles dans la chaîne. Les lacunes d'un ministère au niveau de la sécurité peuvent rapidement devenir le catalyseur qui entraînera la perte de données critiques appartenant à un autre ministère qui partage le système.

Les gestionnaires de systèmes partagés doivent analyser clairement et définir les mesures de protection liées à la STI dans le domaine des responsabilités partagées. Les ministères utilisateurs devraient par la suite procéder en toute confiance à la mise en oeuvre de ces mesures de protection et en assurer la surveillance.

10. **Systèmes interconnectés** – Les alliances conclues avec d'autres paliers du gouvernement, avec les entreprises et les salariés deviennent de plus en plus un modèle de coopération reconnu et largement utilisé. L'échange de données informatisées (EDI), le transfert électronique de fonds (TEF) et le commerce électronique (CE) (en général) sont en train de devenir des stratégies commerciales ordinaires. Un sous-ensemble de cette tendance, est le besoin croissant d'interconnecter les systèmes et les réseaux du gouvernement avec d'autres systèmes du gouvernement et du secteur privé afin de permettre le transfert des données.

    Les ministères doivent s'assurer que les interconnexions de leurs systèmes ne mettent pas en péril le profil de sécurité de leurs propres systèmes. Par exemple, une analyse préalable soignée et, si possible, des mesures de protection additionnelles devraient être mises en oeuvre avant que des données désignées pour le traitement informatique à niveau dominant de sécurité puissent être reliées à des données non protégées destinées à être traitées par des systèmes informatiques à multiniveaux.

    De plus, lorsque l'on partage des données confidentielles avec d'autres organisations qui ne sont pas tenues de se conformer à la politique sur la sécurité, il faut prévoir le respect de plusieurs exigences particulières liées à la politique et aux normes de sécurité.

ANNEXE B

DISPARITÉS DES PROCÉDURES DE SÉCURITÉ DE LA TI À DRHC

Structure organisationnelle

- Deux des quatre régions visitées ont entrepris de collaborer avec l'agent de sécurité du CTI à la mise en œuvre d'un programme mixte de sensibilisation à la sécurité de la TI et à la sécurité physique; dans le cadre de ce programme, les ASR collaborent étroitement avec la Sécurité du CTI pour sensibiliser le personnel à la sécurité de la TI au cours de leurs visites des bureaux.

Planification

- Pour compenser l'absence de vision nationale et de direction fonctionnelle énergique en matière de sécurité de la TI ressentie par la majorité des bureaux régionaux et locaux, le BVI a remarqué que certaines personnes avaient pris l'initiative d'élaborer des plans de sécurité de la TI par n'importe quel moyen à leur disposition. À titre d'exemple, un ASR a rationalisé avec succès une hausse du budget régional consacré à la sécurité. Cette hausse servira notamment à accroître le nombre de visites de bureaux qui seront essentiellement axées sur la sécurité de la TI. Pour pallier son manque d'expérience en matière de TI, l'agent en question est demeuré en communication constante avec le groupe responsable de la sécurité de la TI – Opérations – du CTI. Dans le cadre d'une entente informelle, l'ASR visitera les bureaux en compagnie d'un collègue de la sécurité de la TI du CTI; au cours de ces visites, la sécurité de la TI sera expliquée en détail au personnel.

Accès logique

- Étant donné la disparité des procédures relatives aux codes et aux mots de passe d'utilisateurs, différents groupes de DRHC ont pris des mesures pour uniformiser la gestion des codes et des mots de passe d'utilisateur. Un CTI a adressé aux administrateurs de réseau local de sa région la version provisoire d'un *Guide de l'administrateur pour la gestion de l'accès à l'ordinateur central* de DRHC.

- À l'échelle nationale, on prévoit l'utilisation d'un formulaire électronique qui constituera éventuellement l'unique procédure pour faire une demande de code et de mot de passe d'utilisateur.

- Le CTI de Montréal et de la région du Québec a mis au point un système régional (ordinateur central) similaire au formulaire électronique proposé. Ce système doit toutefois être retiré en prévision du passage à l'an 2000. Si le formulaire électronique de demande de codes et de mots de passe d'utilisateur n'est pas encore prêt à la date prévue du retrait, le CTI de

Montréal/région du Québec devra soit améliorer son propre système en vue du passage à l'an 2000, soit revenir au courriel ou à la procédure manuelle.

Départs et mouvements de personnel

- Un administrateur de réseau local de DRHC a indiqué que le moyen le plus répandu de se tenir au courant des départs d'employés était d'assister à leur fête d'adieu, après quoi l'administrateur du réseau local supprimait le code et le mot de passe de l'employé. Dans les gros bureaux comme les BR, les administrateurs de réseau local ne sont malheureusement pas toujours invités aux fêtes d'adieu en l'honneur des employés qui quittent leur poste.

Surveillance et examen

- Un administrateur de réseau local a fait savoir qu'après son entrée en fonction, il avait effectué un examen de l'environnement TI en place à DRHC. Il a découvert que son prédécesseur accordait à tout le personnel du Ministère l'accès au système de soutien aux agents (SSA). Tous les employés avaient ainsi la capacité d'administrer la base de données, une fonction qui aurait dû être réservée exclusivement à quelques utilisateurs privilégiés. En outre, en vérifiant l'identité des utilisateurs du réseau local, ce même administrateur a découvert qu'un utilisateur n'était pas un employé de DRHC. Il s'agissait, semble-t-il, du représentant d'un fournisseur de services qui avait obtenu l'accès au réseau local et dont le code n'avait jamais été supprimé. Curieusement, cet administrateur a cessé d'examiner le journal des accès au réseau local aux fins de vérifications des utilisateurs.

- Un administrateur de réseau local d'un autre CRHC a prétendu qu'il faisait des inspections visuelles mensuelles des journaux du réseau local mais le BVI n'a pu obtenir aucun journal documenté aux fins d'analyse. Un autre administrateur de réseau local travaillant dans un différent CRHC a toutefois fourni un rapport documenté de ses inspections mensuelles.

Rapport « EasyLock »

- Un CTI a déclaré produire le rapport bimensuel mais l'administrateur de réseau local d'un CRHC prétend avoir communiqué avec le CTI en question parce qu'il n'avait reçu aucun rapport depuis quatre mois. Après examen du dernier rapport, l'administrateur du réseau local a demandé au CTI de supprimer 15 codes et mots de passe.

- Dans une autre région, un administrateur de réseau local dit qu'après n'avoir reçu aucun rapport pendant six ans, il venait d'en recevoir un. Après examen de ce rapport, il a envoyé au CTI plus de cinquante « demandes de suppression du droit d'accès d'anciens employés ».

- Une personne a informé le BVI qu'il y a environ deux ans, elle avait obtenu l'accès « temporaire » à la base de donnée LOIS de Travail. À la fin de son affectation, comme elle n'avait plus besoin de consulter le LOIS, la personne a supposé que son code et son mot de passe temporaires avaient été supprimés. Deux ans plus tard, en voulant accéder de nouveau au LOIS, elle a appris que ses anciens code et mot de passe étaient toujours actifs.

- Un gestionnaire a indiqué au BVI qu'il recevait le rapport EasyLock mais qui ne l'utilisait pas parce qu'il ne le comprenait pas. Ce gestionnaire n'a pas pris le temps de chercher à « comprendre » le rapport et n'a chargé personne de s'assurer que le rapport faisait l'objet d'une surveillance et d'un examen adéquats.

- L'administrateur du système EasyLock peut visionner les mots de passe du SAGE en langage clair.

Sécurité physique

- Le BVI a visité un CDRH qui entreposait les bandes de sauvegarde dans un coffre-fort à l'épreuve du feu. Cette mesure protège adéquatement le papier contre le feu, mais rien ne garantit que la chaleur provenant d'un incendie ne fera pas fondre les bandes magnétiques de plastique.

- Lors d'une visite dans un autre CDRH, le BVI a remarqué que les bandes utilisées pour les sauvegardes étaient de deux marques différentes. L'administrateur du réseau local a expliqué au BVI qu'il avant changé de marques parce qu'il préférait celle qu'il utilisait à la maison. Il ne savait pas s'il existait des normes ministérielles ou gouvernementales (p. ex., concernant la qualité ou les caractéristiques techniques) relatives au type de bandes qu'il fallait utiliser pour les sauvegardes.

- Un BR faisait quotidiennement des copies de sauvegarde du réseau local et possédait une quantité suffisante de cycles de sauvegarde. Toutefois, les bandes de sauvegarde n'étaient pas entreposées à l'extérieur et n'étaient même pas placées dans un endroit protégé à l'intérieur du BR.

ANNEXE C

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Objectifs et portée

Objectifs
- Évaluer les pratiques courantes en matière de sécurité de la TI
- Déterminer les améliorations requises

Portée
- Conformément à la politique gouvernementale en matière de sécurité, l'évaluation portait sur
  - la gestion de la sécurité
  - la sécurité physique
  - la sécurité logique

L'évaluation visait les objectifs suivants :

- Fournir à la direction une opinion sur

  - la situation actuelle concernant les pratiques généralement acceptées à DRHC en matière de sécurité de la TI, les cadres de responsabilisation et de contrôle et
  - la manière dont la Sécurité de la TI s'insère dans la structure directrice de DRHC en matière de sécurité;

- déterminer la pertinence des politiques, pratiques et normes de gestion et la conformité à celles-ci;

- déterminer les incohérences et les risques liés aux composants ou aux procédés majeurs dans le cadre de tous les processus liés à la Sécurité de la TI et faire des recommandations pratiques visant l'amélioration.

La portée de l'évaluation était la suivante :

- ***Gestion de la sécurité*** **–** cadre de gestion - organisation et structure, ressources, responsabilisation, leadership, planification, contrôle, communication, fonction de contrôleur, indicateurs de rendement, acceptation/priorités/culture de la haute direction, sensibilisation ou culture des utilisateurs, politiques et procédures opérationnelles ou documentation

- ***Sécurité physique*** **–** sécurité physique des biens et des ressources de TI - ordinateurs portatifs, salles du réseau local, installations extérieures d'entreposage, accès limité, conditions ambiantes - réglage de la température, purification de l'air, halon, etc., BRA/reprise des activités, planification d'urgence.

- ***Sécurité logique*** **–** chemins d'accès (p. ex., *.*), identification d'utilisateur et authentification, codes et mots de passe d'utilisateur, logiciel de contrôle d'accès (p. ex., Easylock), bibliothèque de fichiers et copies de sauvegarde, intégrité des fichiers, sécurité des PC/serveurs, sécurité des ordinateurs centraux et pare-feu.

ANNEXE D

SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION
Méthodologie

- Évaluation des pratiques de sécurité de la TI dans les bureaux suivants
  - AC
  - quatre bureaux régionaux (CB, ONT, QUÉ et NB)
  - bureaux locaux sélectionnés (au moins un CDRH par région)
  - CTI (un par région)
- Conduite d'entrevues
- Examen et analyse de documents et des journaux de vérification et de sécurité
- Tenue de sessions de débreffage

MÉTHODOLOGIE

On a effectué des recherches et des entrevues auprès de membres du personnel de l'administration centrale (AC) dont quatre Centres de technologie de l'information (CTI) (Vancouver, Belleville, Montréal et Moncton), quatre bureaux régionaux (BR) (Colombie-Britannique/Yukon, Ontario, Québec et Nouveau-Brunswick) et un bureau local dans chacune des régions. Les entrevues ont été menées auprès

- d'agents de sécurité des bureaux nationaux, régionaux et locaux (p. ex., coordonnateurs de la sécurité ou leurs représentants au Ministère, dans les régions et les CTI);

- de gestionnaires et employés de la TI (p. ex., Systèmes AC, GSR, agents de contrôle de l'accès à la sécurité du PSR, administrateurs régionaux de bases de données de Travail, administrateurs de réseau local) et

- de gestionnaires et employés non affectés à la TI (PSR, Travail, AE, DGIRH, RH, SFA, PSP) mais qui utilisent la TI (matériel, logiciels, télécommunications, applications nationales/ systèmes locaux, etc.) quotidiennement dans le cadre de leurs fonctions.

- Sur place, le BVI a demandé à consulter les rapports ou les journaux pertinents de sécurité de la TI concernant notamment l'accès à l'ordinateur central, l'identité des utilisateurs privilégiés, les infractions à la sécurité de l'ordinateur central, les infractions à la sécurité du réseau local et du réseau étendu et l'accès au réseau local.

- Lorsque les rapports étaient disponibles, le BVI en faisait l'examen détaillé avec l'aide du destinataire ou de l'auteur (p. ex., raison ou objectif, intégrité de l'information, fréquence, utilisateurs, etc.).

Le BVI a également procédé à des inspections visuelles sommaires des locaux où sont entreposés les bandes et les fichiers de sauvegarde du réseau local ainsi que des locaux abritant le matériel informatique. Enfin, le BVI a inspecté les installations extérieures utilisées par les CTI pour l'entreposage.