BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Renforcer la résilience des **Infrastructures essentielles du Canada aux risques internes**

Direction des infrastructures essentielles

Sécurité publique Canada
Public Safety Canada

Canada

En bref

Et si les clés du château étaient entre les mains de ceux contre lesquels vous tentiez de vous défendre?

Et si l'entrepreneur qui construit votre infrastructure de TI travaillait pour votre concurrent?

Et si votre actif le plus important était aussi votre plus grande vulnérabilité?

Le risque interne se rapporte aux personnes qui travaillent au sein d'une organisation dans le but de compromettre la confidentialité, l'intégrité et la disponibilité de l'information contenue à l'intérieur des murs de cette entité. Le présent guide établit huit mesures de sécurité qui peuvent être utilisées pour lancer ou améliorer l'approche d'une organisation en matière de protection contre les menaces internes.

No de cat. : PS9-12/2019F-PDF
ISBN : 978-0-660-30274-4

Table des matières

Introduction

Le présent document a pour but de fournir aux organisations canadiennes d'infrastructures essentielles des conseils sur ce qui constitue un risque interne et des recommandations sur la façon de surveiller les risques internes, d'y répondre et de les atténuer. Ce guide aidera les organisations à élaborer leurs programmes relatifs aux risques internes afin de se protéger contre les vulnérabilités humaines et techniques, y compris celles liées à leurs partenaires, à leurs fournisseurs de service et à leurs associés. À la fin de chaque mesure de sécurité se trouve une liste des normes de sécurité acceptées et établies à l'échelle internationale qui émanent d'organisations comme le National Institute of Technology (NIST) des États-Unis, le National Insider Risk Task Force (NITTF) des États-Unis et l'Organisation internationale de normalisation (ISO).

De nombreuses industries canadiennes font face à des défis liés aux menaces à la sécurité physique ou informatique de leurs organisations. Comme les processus opérationnels sont de plus en plus diversifiés et reliés à un monde axé sur la cybernétique, les propriétaires et les exploitants des infrastructures essentielles du Canada devraient être conscients de leur vulnérabilité à l'égard de toutes les formes de menaces, tant physiques que cybernétiques.

Un risque interne peut être défini comme toute personne qui possède des connaissances ou un accès à l'infrastructure d'une organisation (tant à l'infrastructure physique qu'aux réseaux informatiques) et qui, par malveillance ou par hasard, abuse de son accès pour nuire aux employés, aux clients, aux biens, à la réputation ou aux intérêts de l'organisation. Selon la définition du CERT Insider Threat Centre de l'Université Carnegie Mellon, un risque interne est une personne qui travaille au sein d'une organisation dans le but de compromettre la confidentialité, l'intégrité et la disponibilité de l'information contenue à l'intérieur des murs de cette entité.

8 mesures de sécurité recommandées

THÈME 1
Établir une approche globale de la sécurité

Mesure de sécurité nº 1
Établir une culture de sécurité[1]

La sécurité est un élément fondamental et essentiel de la gestion des risques opérationnels, comme les menaces internes liées à un employé mal intentionné ou qui cause du tort de façon non intentionnelle. Les organisations devraient élaborer et mettre en œuvre des politiques solides en matière de sécurité physique et de cybersécurité, sous la direction de la haute direction. Les politiques de sécurité organisationnelle doivent intégrer tous les secteurs d'une organisation et décrire les responsabilités de tous les employés. Les mesures suivantes soulignent cette approche holistique de la sécurité.

Mesure de sécurité nº 1

1) Établir l'engagement et la responsabilisation de la haute direction
2) Désigner un cadre supérieur responsable de la gestion des risques internes
3) Établir un engagement de l'ensemble de l'organisation à l'égard de la sécurité et mettre l'accent sur le leadership à tous les niveaux

Établir l'engagement et la responsabilisation de la haute direction

Le renforcement de la posture de sécurité d'une organisation et la mise en place d'un environnement sécurisé pour se défendre contre les risques sont au bout du compte la responsabilité de la haute direction. La cyberrésilience et la gestion des risques liés à la cybersécurité sont les principaux défis des organisations d'aujourd'hui. Les organisations reconnaissent rapidement le risque élevé de dommages financiers ou d'atteinte à la réputation causés par des atteintes à la sécurité. Pour une organisation, il est essentiel que les cadres supérieurs établissent et soutiennent une solide culture de sécurité afin d'obtenir l'adhésion des employés et leur participation au maintien d'un environnement sécuritaire.

Désigner un cadre supérieur responsable de la gestion des risques internes

Lors de la mise en œuvre d'approches liées aux risques internes ou de la gestion de ces risques, les organisations devraient s'assurer que les responsabilités en matière de prise de décisions sont assumées par un haut fonctionnaire de l'organisation pleinement responsable. Ce fonctionnaire devrait être responsable de la production de rapports sur les risques et de leur gestion et devrait être appuyé par un groupe de travail sur les risques internes qui comprend des représentants de divers secteurs de l'organisation, notamment des secteurs des ressources humaines, juridique, de la protection des renseignements personnels, des communications, de la technologie et de la sécurité. De plus, ce fonctionnaire et le groupe de travail devraient disposer de ressources et de pouvoirs suffisants pour s'acquitter de leurs

1 Des ressources supplémentaires sur les risques internes sont disponible dans la Special Publication 800-53, Revision 4 du National Institute of Standards and Technology (NIST), AT-1, AT-2 et AT-3; dans le Carnegie Mellon CERT Resilience Model (CERT-RMM), Organizational Training and Awareness; et dans la norme ISO 27002 : Sensibilisation, apprentissage et formation à la sécurité de l'information.

fonctions et devraient envisager d'élaborer un plan de communication publique en prévision de tout problème lié au risque interne.

Établir un engagement de l'ensemble de l'organisation à l'égard de la sécurité et mettre l'accent sur le leadership à tous les niveaux

Une organisation ne peut pas être plus forte que son maillon le plus faible. Une méthode pour renforcer sa position face aux risques internes consiste à communiquer clairement à tous les employés les mesures escomptées concernant les règles et les codes de conduite de l'organisation en ce qui a trait à la sécurité. Des politiques bien conçues concernant l'utilisation acceptable des systèmes, des données et d'autres ressources de l'organisation sont essentielles à l'établissement d'un programme efficace en matière de risque interne. Tous les services concernés au sein d'une organisation devraient également participer à l'élaboration de politiques relatives à l'accès aux données et aux biens importants et de nature délicate.

La sécurité de l'organisation devrait être défendue par la haute direction, étant entendu que tous les niveaux de l'entreprise doivent jouer un rôle dans le renforcement de la résilience. Au bout du compte, un cadre supérieur de l'organisation est responsable de l'établissement de la stratégie de sécurité et de l'exécution et de la promotion d'une solide culture de la sécurité et de l'atténuation des risques.

Les organisations doivent :

Désigner un champion au sein de l'organisation pour la gestion des risques internes avec pleine responsabilité.

Désigner un cadre supérieur responsable de l'élaboration d'une politique et d'un programme de sécurité à l'échelle de l'entreprise.

Élaborer une structure de gouvernance, y compris un groupe de travail sur le risque interne, pour élaborer, exécuter et gérer un programme de risque interne.

Établir un « engagement » organisationnel pour reconnaître l'importance de la sécurité dans la réalisation d'une entreprise rentable et durable.

Concevoir des politiques et des procédures exhaustives de sécurité des réseaux physiques et cybernétiques englobant tous les départements.

Promouvoir une culture de sécurité à tous les niveaux en établissant un lien entre le rendement des employés et de la direction et les paramètres de sécurité.

Mesure de sécurité nº 2
Élaborer des politiques et des procédures de sécurité claires[2]

Dans l'environnement actuel d'interconnectivité, les risques internes peuvent provenir de n'importe qui, y compris des employés, des partenaires, des associés et des tiers fournisseurs de service d'une organisation. Toute organisation ou personne externe qui a accès au réseau interne, aux ressources, au personnel, aux installations ou aux biens numériques d'une organisation devrait être considérée comme un risque. Les mesures suivantes sont recommandées pour aider les organisations à élaborer des politiques et des procédures de sécurité claires afin d'atténuer les risques potentiels.

Mesure de sécurité nº 2

1) Définir des attentes et des résultats clairs
2) Déterminer les niveaux de risques des postes au sein de l'organisation
3) Harmoniser l'accès des employés avec les niveaux de risque des postes

Définir des attentes et des résultats clairs

Les politiques de sécurité mises en œuvre par une organisation doivent énoncer clairement les règles et les lignes directrices à l'intention des employés en ce qui a trait aux domaines suivants :

- gestion de l'accès aux comptes;
- contrôle et intégrité des mots de passe;
- droits d'accès aux données ou aux documents internes physiques et numériques;
- utilisation personnelle d'Internet, accès aux médias sociaux et téléchargement et stockage de données personnelles dans les réseaux de l'entreprise;
- participation des employés à des exercices de formation réguliers et appropriés;
- mesures correctives et formation supplémentaire.

Déterminer les niveaux de risques des postes au sein de l'organisation

Les organisations devraient attribuer des niveaux de risque à tous les postes au sein de l'organisation en fonction de l'accès du poste aux renseignements de nature délicate et aux installations matérielles. Cette pratique devrait s'appliquer à tous les employés, ainsi qu'aux entrepreneurs et aux sous-traitants. Il est également important de procéder à des évaluations de poste périodiques afin de cerner tout changement possible aux exigences, aux règles ou aux responsabilités du poste et d'ajuster le niveau de risque de poste en conséquence.

---

2 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, RA-1, RA-3, PM-9; dans le National Insider Threat Task Force, B-2 et C-6; et dans la norme ISO 27002 : risques liés aux parties externes, aux clients et aux ententes avec des tiers

Harmoniser l'accès des employés avec les niveaux de risque des postes

L'examen des nouveaux employés devrait être proportionnel au niveau de risque évalué pour accomplir les fonctions et les tâches attendues de ces employés. Par exemple, les postes ayant un plus grand accès aux renseignements de nature délicate devraient faire l'objet de vérifications de sécurité plus rigoureuse. Outre que les procédures de sécurité normales comprenant la vérification du crédit et des antécédents criminels, les organisations devraient également enquêter, au besoin, sur les indications sur le rendement, les renseignements du curriculum vitæ et les entrevues en personnes. L'examen et la vérification de tous les renseignements disponibles concernant un candidat potentiel faciliteront le fait de lui donner un accès sécurisé à l'information et aux systèmes organisationnels.

Les organisations doivent :

Définir clairement les politiques de sécurité ministérielle, les afficher et en faire part aux employés.

Effectuer la présélection des employés en fonction des exigences du poste.

Attribuer des niveaux de risque appropriés aux employés en fonction de la criticité et de l'importance de l'information, des systèmes et du secteur auxquels ils ont accès.

Mesure de sécurité nº 3
Réduire les risques des partenaires et des tiers fournisseurs[3]

Compte tenu de l'élargissement des réseaux, de l'accès accru des utilisateurs et de l'empreinte de stockage des données, il est important d'intégrer des mesures de sécurité et des attentes dans toutes les ententes de service avec des fournisseurs tiers. Pour réduire et atténuer les risques, il est essentiel de comprendre où se trouvent les principaux biens et systèmes et comment ils sont structurés, et de comprendre la façon dont les partenaires et les tierces parties accèdent au réseau et aux installations de l'organisation. Les mesures suivantes sont recommandées pour aider une organisation à réduire les risques potentiels de la part de tiers.

Mesure de sécurité nº 3

1) Comprendre les principaux biens et systèmes
2) Connaître vos partenaires
3) Connaître vos risques

Comprendre les principaux biens et systèmes

Les organisations tierces, les entrepreneurs, les consultants et les fournisseurs de services externes qui ont un accès physique à une entreprise, à ses données ou à ses systèmes informatiques devraient être examinés comme des sources potentielles d'accès interne. Cela peut se faire principalement si l' organisation a déterminé ses biens et ses données essentiels, l'endroit où ils se trouvent, et qu'elle a mis en œuvre des contrôles pour en limiter l'accès. La mise en œuvre de contrôles et de surveillance de l'accès aux réseaux et aux données est très importante pour réduire les risques potentiels liés aux partenaires et aux tiers fournisseurs de service.

Connaître vos partenaires

Des ententes de sécurité entre l'organisation et ses partenaires d'affaires et associés qui régissent des domaines comme la propriété des données, la confidentialité, la propriété intellectuelle et les ententes de non-divulgation devraient être envisagées. La posture de sécurité des tiers fournisseurs de service devrait incomber au tiers. Cependant, il est important de vérifier de façon indépendante les processus de sécurité des partenaires, ce qui comprend des vérifications des antécédents des employés et des fonctions qui, le cas échéant, sont confiées à d'autres entités. En outre, il est important d'établir des relations de confiance à long terme et d'intégrer des clauses de garanties dans les contrats avec des tiers afin de réduire les risques pour la sécurité dans la chaîne d'approvisionnement d'une organisation.

---

3 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, RA-3 et PM-9; dans le National Insider Threat Task Force, B-2 et C-6; dans le CERT-RMM dans les sections « external dependencies », « human resources », et « access control »; et dans la norme ISO 27002.

Connaître vos risques

Une évaluation complète des risques à l'échelle de l'entreprise constitue une occasion idéale d'évaluer les exigences en matière de sécurité et le contexte de menace d'une organisation. La connaissance de l'environnement de sécurité au sein d'une organisation et la détermination des menaces potentielles aideront à l'élaboration de politiques de sécurité appropriées concernant l'accès aux données et la gestion des comptes réseau. De plus, une évaluation interne des risques permettra de déterminer les biens essentiels qui sont jugés les plus importants pour les activités opérationnelles de l'organisation ainsi que les menaces potentielles pour ces biens. L'identification des biens est importante dans toute décision visant à déterminer les risques associés au fait de donner à de tiers accès aux systèmes et aux biens essentiels.

Les organisations doivent :

Procéder à une évaluation des risques à l'échelle de l'organisation pour déterminer tous les principaux biens et systèmes essentiels; cerner toutes les préoccupations en matière de sécurité liées à l'accès de tiers à ses réseaux, données et systèmes.

Vérifier de façon indépendante la posture de sécurité des tiers fournisseurs de services, y compris la vérification des antécédents des employés ayant accès aux installations ou aux réseaux essentiels d'une organisation.

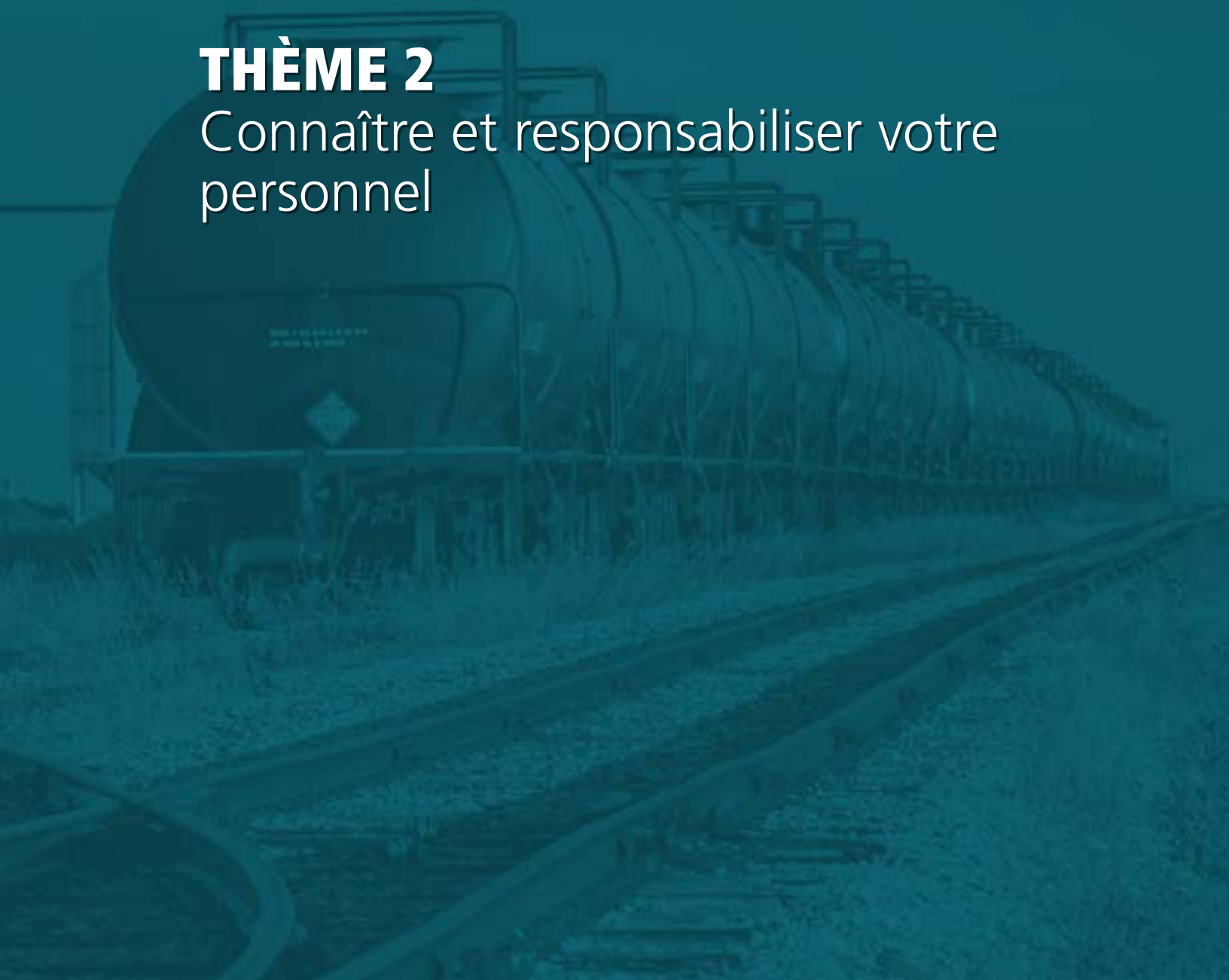
Veiller à ce que des ententes de sécurité exhaustives soient conclues avec les tierces parties contenant des clauses de garanties afin de réduire les risques liés à la chaîne d'approvisionnement.

Établir des relations de confiance à long terme avec les principaux fournisseurs de services.

8 mesures de sécurité recommandées

THÈME 2

Connaître et responsabiliser votre personnel



Mesure de sécurité nº 4
Mettre en œuvre un cycle de vie de filtrage de sécurité du personnel[4]

Les employés sont à la fois le plus grand atout d'une organisation et sa plus grande vulnérabilité. Les dirigeants d'une organisation devraient adopter une approche globale de gestion des ressources humaines et devraient prendre des mesures pour réduire au minimum leur exposition aux risques internes. Les mesures suivantes sont recommandées pour renforcer la gestion des ressources humaines

Effectuer les vérifications préalables à l'emploi

La réduction du risque de menaces internes devrait commencer au début du processus d'embauche, car un certain nombre de mesures peuvent être prises à cette étape. Des vérifications des antécédents criminels, du crédit et des références devraient être effectuées afin de cerner tout secteur ou indicateur de préoccupation potentiel. La réalisation de recherches préliminaires, dont un examen approfondi des médias sociaux, peut aider à déterminer le profil de risque d'un employé en ce qui a trait à son accès à des renseignements ou à des systèmes essentiels, confidentiels ou exclusifs au sein de l'organisation.

Mettre en place un filtrage de sécurité continu des employés

Les organisations devraient examiner et mettre à jour leurs évaluations de sécurité des employés à des intervalles réguliers (p. ex., tous les cinq ans) ou lorsque la situation le justifie. Il est important de reconnaître que les niveaux de risque peuvent changer au fil du temps et que, par conséquent, des vérifications périodiques des antécédents et du crédit par rapport au niveau de sécurité d'un poste donné peuvent révéler des activités et des comportements inhabituels qui auraient autrement pu passer inaperçus. Par exemple, si un employé assume de nouvelles responsabilités ou est muté à un poste présentant un profil de risque plus élevé, une vérification plus approfondie des antécédents pourrait être nécessaire.

Incorporer les procédures de départ et de roulement interne

Lorsqu'un employé quitte une organisation, des procédures et des politiques doivent être en place pour s'assurer que ses comptes sont désactivés et que l'accès physique aux locaux de l'entreprise et aux systèmes informatiques ou aux données est annulé. Cela comprend la responsabilisation du gestionnaire pour toutes les procédures de cessation d'emploi des employés qui quittent l'organisation. Les mots de passe donnés à ces employés doivent être annulés, les cartes d'accès et d'identité doivent être retournées à l'agent

Mesure de sécurité nº 4

1) Effectuer les vérifications préalables à l'emploi
2) Mettre en place un filtrage de sécurité continu des employés
3) Incorporer les procédures de départ et de roulement interne
4) Établir des politiques de sécurité transparentes

4 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, PS-1, PS-2, PS-3 et PS-8.

de sécurité désigné et les ordinateurs portables, les téléphones mobiles ou tout autre type d'appareil doivent être recensés. Ces procédures réduiront le risque qu'une personne accède aux biens matériels ou aux réseaux internes après avoir quitté l'organisation. En plus des procédures pour les employés qui quittent l'organisation, les organisations devraient modifier les privilèges d'accès pour les employés qui changent de secteur fonctionnel au sein d'une même organisation.

Établir des politiques de sécurité transparentes

L'adoption de politiques de sécurité transparentes à l'échelle de l'organisation aidera à réduire les risques internes. Les politiques de vérification des antécédents devraient s'appliquer à tous les employés et doivent être non discriminatoires. Les renseignements découverts au cours d'une vérification des antécédents doivent être bien évalués en regard de la tolérance au risque de l'organisation et les employés doivent avoir la possibilité de contester tout renseignement qui pourrait être inexacte. De plus, une organisation devrait disposer d'une procédure officielle et établie de règlement des griefs si les employés souhaitent en appeler d'une décision.

Les organisations doivent :

Effectuer une présélection approfondie et continue de tout le personnel en utilisant toutes les ressources disponibles, y compris les médias sociaux.

Mettre à jour l'accès et les autorisations de sécurité pour les employés en fonction des rôles et responsabilités de leur poste.

Modifier les privilèges d'accès pour les employés qui ont été mutés à de nouveaux postes au sein de l'organisation.

Promouvoir un programme de sécurité transparent auprès de tous les employés pour gérer les attentes en matière de sécurité physique et de sécurité du réseau.

Mesure de sécurité nº 5
Offrir de la formation, accroître la sensibilisation et mener des exercices[5]

Reconnaissant que les employés sont les « premiers intervenants » de l'organisation dans la détection et la notification des risques internes potentiels, un programme de formation solide est essentiel pour renforcer la sécurité des organisations.Les trois recommandations suivantes sont suggérées dans le but d'améliorer la formation de sensibilisation aux risques à l'intention des employés.

Offrir une formation régulière pour réduire les risques d'infractions non intentionnelles à la sécurité

Pour s'assurer que les employés comprennent l'environnement de risque, il est essentiel d'offrir une formation efficace et continue sur la sensibilisation à la sécurité. Comme les menaces potentielles peuvent se manifester dans les domaines physique et cybernétique, les organisations doivent adopter une approche globale. Par exemple, en ce qui concerne les risques internes non intentionnels, les employés devraient recevoir une formation sur un certain nombre de domaines, notamment la reconnaissance des stratagèmes d'hameçonnage, l'intégrité des mots de passe, l'utilisation de supports portatifs et l'accès aux médias sociaux. Les employés doivent être informés que les médias sociaux servent souvent à établir des profils cibles et à avoir accès aux justificatifs d'identité des employés ou aux informations de l'entreprise.

Accroître la sensibilisation aux signes avant-coureurs

Il est important que les organisations fassent connaître aux employés les répercussions potentielles que les risques internes peuvent avoir sur une organisation, ainsi que les signes avant-coureurs possibles concernant le comportement des employés. Même si aucun profil particulier n'a été établi pour repérer facilement un risque interne malveillant ou non intentionnel, les employés devraient être formés pour reconnaître les comportements au sein de l'organisation qui pourraient mener à la manifestation d'une activité de risque interne malveillante. Voici une liste d'attributs et d'actions qui pourraient être pris en compte pour déterminer si une personne pourrait devenir un risque interne :

---

5 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, AT-1, AT-2 et AT-3; et dans la norme ISO 27002 : 8.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

- abus d'alcool ou d'autres drogues;
- personnalité argumentative ou agressive au travail;
- changements dans la situation financière;
- non-respect des politiques et des procédures;
- tentatives fréquentes d'accès à des fichiers ou des systèmes non autorisés;
- cessation d'emploi ou démission inattendue;
- absentéisme;
- déplacements non autorisés;
- contacts non autorisés avec des représentants étrangers ou des concurrents.

Cette liste n'est pas exhaustive et les personnes qui affichent certains de ces comportements ne risquent pas nécessairement de devenir des acteurs malveillants. Le but de la sensibilisation est d'inciter les gens à prendre en considération et à cerner les menaces potentielles avant qu'elles se concrétisent et la liste mentionnée ci-dessus présente des caractéristiques communes trouvées dans des cas antérieurs de risques internes.
Les organisations devraient également développer des mécanismes d'aide aux employés pour les aider à éviter que les employés deviennent à risque de compromission.

Favoriser une culture de vigilance et responsabiliser les employés

Les organisations doivent favoriser une culture de sécurité pour s'assurer que ses politiques et programmes sont efficaces. Pour bâtir cette culture de la sécurité, il est important que les employés fassent partie de la solution et qu'ils reconnaissent qu'une approche combinée et organisationnelle de la sécurité est avantageuse à tous.

Mesure de sécurité nº 5

1) Offrir une formation régulière pour réduire les risques d'infractions non intentionnelles à la sécurité
2) Accroître la sensibilisation aux signes avant-coureurs
3) Favoriser une culture de vigilance et responsabiliser les employés

L'étape la plus importante pour une organisation est d'aider ses employés à repérer les signes avant-coureurs qui pourraient signaler des actes futurs d'activités de risque interne. Par exemple, la philosophie « si vous voyez quelque chose, signalez-le » a été adoptée par de nombreux pays, dont le Canada, et permet à tous les citoyens d'être vigilants face aux menaces potentielles. Un tel appel à l'action devrait être non intrusif et faire partie intégrante de la culture d'entreprise et de la formation afin de ne pas créer un climat de méfiance. Les employés et la direction doivent comprendre que chacun a un rôle à jouer en matière de sécurité et que, parfois, les plus petits indicateurs peuvent être pertinents pour cerner une menace plus importante.

Une activité inhabituelle liée au risque interne pourrait se caractériser par tout comportement observé indiquant un préjudice malveillant potentiel ou perçu pour l'organisation. Certaines de ces activités pourraient être innocentes. Cependant, il appartient au personnel formé en matière

d'application de la loi et de sécurité de déterminer si le comportement justifie une enquête. Si une activité inhabituelle est observée, il faut encourager les gens à la signaler à la direction ou à la haute direction de l'organisation pour qu'elle prenne les mesures appropriées. Si une activité inhabituelle est observée, les témoins sont encouragés à fournir les éléments suivants :

- qui a été vu ou qu'est-ce qui a été vu;
- quand l'a-t-on vue;
- où l'activité s'est-elle produite;
- pourquoi est-ce inhabituel.

Les organisations doivent :

Élaborer un programme de formation en sécurité pour tous les employés.

Accroître la sensibilisation aux indicateurs de préoccupations potentielles en matière de sécurité.

Donner accès aux programmes d'aide aux employés pour les aider à éviter que les employés ne courent un risque de compromission.

Développer et promouvoir une culture de vigilance en matière de sécurité en encourageant les employés à signaler ce qu'ils voient, le cas échéant.

Effectuer des exercices périodiques pour vérifier la position en matière de sécurité au sein d'une organisation.

8 mesures de sécurité recommandées

THÈME 3

Déterminer ce qui est essentiel et le protéger

Mesure de sécurité nº 6
Déterminer les biens essentiels et les protéger[6]

Un bien essentiel peut être considéré comme tout ce qui, s'il est détruit, modifié ou autrement dégradé, aurait une incidence sur la confidentialité, l'intégrité ou la disponibilité des services essentiels. Voici une liste de suggestions pour améliorer la compréhension et la protection des biens essentiels d'une organisation.

Cerner et classer les principaux biens et systèmes

Il est essentiel que toute organisation élabore des mesures efficaces et efficientes de protection et de dissuasion pour comprendre l'ampleur, la complexité et la profondeur des biens qui composent ses systèmes et son infrastructure. Les biens essentiels comprennent notamment les installations, les systèmes, l'équipement, la technologie et la propriété intellectuelle. Les organisations devraient inclure l'identification et le classement des biens et des systèmes essentiels comme élément clé de la planification de la continuité des activités.

Il existe un certain nombre de méthodes ou de techniques pour déterminer et classer les biens. Par exemple, une méthode permettant à une organisation de déterminer ses biens essentiels consiste à effectuer une évaluation des risques. Une évaluation des risques aidera à déterminer les biens, les processus des systèmes et les données essentiels d'une organisation et leur profil de risque actuel. Grâce à une évaluation de cette nature, les organisations seront en mesure de classer et de coter avec précision leurs biens essentiels et, par la suite, d'élaborer une stratégie d'atténuation pour les protéger. Lorsqu'elle est intégrée à la planification de la continuité des activités de l'organisation, l'importance des biens peut être évaluée et les mesures de sécurité appropriées peuvent être mises en œuvre.

Sécuriser les principaux biens et systèmes

Les organisations devraient également mettre en œuvre des procédures de sécurité qui les protègent contre l'accès physique et informatique. Ces procédures peuvent comprendre des points de contrôle de sécurité, des authentifications à deux facteurs pour accéder aux réseaux informatiques, des pare-feu, la surveillance des réseaux ou toute autre méthode conçue pour restreindre l'accès aux utilisateurs autorisés. De plus, les organisations devraient élaborer une approche pour surveiller l'utilisation du système par les utilisateurs autorisés et non autorisés ainsi que l'accès physique aux

6 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, CP-2(8), CM-2, CM-8, PM-5, PM-8, et RA-2 et dans la norme ISO 27002 : 7.1.1 Inventaire des actifs.

locaux en dehors des heures de travail. Les documents relatifs à l'architecture doivent également décrire la façon dont les données sont envoyées à des tiers et la nature et le caractère sensible de ces données, car les données jugées essentielles ou sensibles doivent être masquées ou chiffrées. En outre, il est essentiel d'avoir en place des moyens de protection visuellement reconnaissables et intrinsèques pour protéger les biens, le niveau de protection étant associé à l'importance du bien.

Exploiter la signalisation et les moyens de dissuasion visibles pour contrer l'accès

Une approche holistique de la protection des biens doit comprendre des mesures de protection visibles pour les employés afin de réduire les risques d'accès non intentionnel. L'utilisation appropriée de panneaux et d'autres moyens de dissuasion visibles peut fournir des instructions claires visant à réduire l'accès non intentionnel par les employés. Il peut s'agir de mesures d'envergure comme des gardes de sécurité, des clôtures et des points de contrôle de la circulation, ou de tactiques plus subtiles comme les panneaux d'avertissement indiquant un accès restreint, l'étiquetage des documents ou l'affichage des politiques et règlements.

Les zones où l'accès doit être contrôlé par des moyens physiques doivent être établies et indiquées clairement afin de réduire l'accès accidentel et non intentionnel. Les panneaux d'avertissement sont un moyen courant et efficace d'établir les zones réglementées et de gérer la circulation du personnel. En ce qui a trait à la protection de l'information, il est important de catégoriser adéquatement les renseignements afin que le personnel puisse reconnaître immédiatement les données sensibles et appliquer les protocoles de manipulation, de stockage ou de destruction appropriés.

Appliquer le principe de droit d'accès minimal

Le principe du droit d'accès minimal doit être appliqué afin de restreindre les utilisateurs au niveau minimal d'accès requis pour s'acquitter efficacement de leurs fonctions. La restriction de l'accès aux réseaux et à l'infrastructure d'un organisme au moyen de ce principe peut être essentielle afin d'atténuer le risque interne. Par exemple, un utilisateur qui est responsable du traitement des factures pour payer les fournisseurs n'a probablement pas besoin d'avoir accès aux dossiers du personnel. De même, un opérateur de machinerie lourde n'a sans doute pas besoin d'accéder à une salle de commande. L'objectif fondamental de ce principe est d'adopter une approche stratégique du contrôle de l'accès au sein d'un organisme.

Mesure de sécurité nº 6

1) Cerner et classer les principaux biens et systèmes
2) Sécuriser les principaux biens et systèmes
3) Exploiter la signalisation et les moyens de dissuasion visibles pour contrer l'accès
4) Appliquer le principe de droit d'accès minimal
5) Séparer les fonctions

Séparer les fonctions

Les organisations devraient envisager de répartir les principales fonctions entre plusieurs personnes afin de s'assurer qu'une seule personne ne peut pas utiliser à mauvais escient des renseignements de nature délicate ou saboter des biens essentiels. Le partage mutuel des responsabilités entre des employés de confiance réduit le risque d'activités malveillantes internes contre un organisme. Il permet également d'assurer la continuité si quelqu'un quitte un poste essentiel. Cependant, il y a un coût associé à la formation qui peut être nécessaire au partage des responsabilités, et il incombe à l'organisation de trouver l'équilibre qui convient le mieux à son environnement.

Les organisations doivent :

Mener une évaluation à l'échelle de l'organisation pour cerner les biens et les systèmes essentiels et les classer, ainsi que déterminer les mesures de sécurité pour les protéger.

Surveiller l'utilisation du système par les utilisateurs autorisés et non autorisés, ainsi que l'accès aux installations.

Décrire quelles données sont envoyées à des tiers et de quelle façon la transmission est effectuée, ainsi que la sensibilité des données, afin de protéger les données de façon appropriée.

Examiner le principe du droit d'accès minimal et de la séparation des fonctions concernant les systèmes et les données essentielles.

Tirer parti des moyens de dissuasion visibles pour réduire la probabilité d'un accès non intentionnel aux installations, aux réseaux et aux systèmes.

Mesure de sécurité nº 7
Réagir aux comportements inhabituels, les surveiller et les atténuer[7]

L'établissement d'un programme de sécurité au sein d'une organisation doit comprendre des procédures pour surveiller le comportement physique et le comportement dans le réseau, ainsi qu'un plan d'intervention en cas d'incident. Des contrôles de sécurité physique appropriés associés à un moyen de suivi de l'accès ainsi qu'à une sensibilisation et une vigilance efficaces des employés devraient aider à réduire les risques internes. Voici quelques mesures recommandées visant à réduire les risques organisationnels internes.

Assurer un suivi de l'accès à distance et surveiller les dispositifs d'extrémités

Les organisations doivent connaître les technologies d'accès à distance utilisées par les employés et les risques potentiels pour les systèmes et les données de leur organisation. Les attaquants mal intentionnés accèdent aux organisations à distance pendant qu'ils sont à leur emploi ou après leur cessation d'emploi, en utilisant l'accès légitime fourni par l'organisme. Ce type d'accès peut être bloqué, ou à tout le moins surveillé, au moyen de politiques organisationnelles et de solutions technologiques. Il est recommandé que, dans la mesure du possible, l'accès aux données essentielles ne soit accordé qu'aux employés qui sont présents sur les lieux de travail, et non à ceux qui travaillent à distance.

Les organisations adoptent de plus en plus des politiques qui encouragent le télétravail ou une autre forme de régime de travail mobile. Ainsi, l'accès à distance aux réseaux d'entreprise par téléphone intelligent, ordinateur portatif et tablette est devenu la nouvelle norme. L'accès à distance aux systèmes informatiques d'un organisme est l'occasion idéale pour les acteurs malveillants d'attaquer les systèmes ou d'y accéder. Même s'il peut améliorer la productivité des employés, l'accès à distance aux données, aux processus et aux systèmes d'information essentiels doit être accordé avec prudence et documenté par les organisations.

Ces dernières devraient également envisager de saisir l'intégralité du contenu des paquets ou des données de flux réseau sur le périmètre de leur réseau. Des anomalies comme le fait que de grandes quantités d'information numérique quittent le réseau peuvent indiquer une compromission possible ou un accès non autorisé. Elles doivent également envisager de surveiller l'utilisation

Mesure de sécurité nº 7

1) Assurer un suivi de l'accès à distance et surveiller les dispositifs d'extrémités
2) Établir des mesures efficaces de signalement, de suivi et d'intervention en cas d'incident
3) Sensibiliser aux meilleures pratiques concernant l'utilisation des sites de réseautage social

7 Des ressources supplémentaires sur les risques internes sont disponibles dans la Special Publication 800-53, Revision 4 du NIST, CP-2(8), CM-2, CM-8, PM-5, PM-8, et RA-2 et dans la norme ISO 27002 : 7.1.1 Inventaire des actifs.

d'imprimantes, de numériseurs, de photocopieurs et de télécopieurs afin d'atténuer l'exfiltration des données en cas de copie, de téléchargement et de télécopie d'un grand volume de renseignements.

Établir des mesures efficaces de signalement, de suivi et d'intervention en cas d'incident

Les organisations doivent établir un processus permettant de signaler et de suivre de façon confidentielle les comportements inhabituels ou les incidents potentiels. La direction devrait envisager les mesures les plus appropriées à prendre lorsqu'un incident est signalé, y compris la responsabilité de la haute direction d'atténuer tout risque interne possible. Il peut s'agir d'une entrevue personnelle avec un employé, d'une surveillance régulière du réseau et d'un congédiement ou d'une intervention policière selon la gravité de l'événement.

Sensibiliser aux meilleures pratiques concernant l'utilisation des sites de réseautage social

Les organisations doivent élaborer des politiques et des procédures transparentes sur l'utilisation appropriée des sites de réseautage social (SRS) en milieu de travail afin de s'assurer que les employés n'affichent pas de renseignements qui pourraient les rendre vulnérables à la divulgation involontaire ou délibérée de renseignements. L'utilisation de SRS en milieu de travail a des répercussions sur la vie privée des employés et des employeurs et augmente le risque global pour les menaces internes opportunistes. Les employés doivent savoir que les renseignements ou les communications publiés sur leurs SRS peuvent être accessibles de tous, notamment de l'organisme lui-même. Il convient également de noter que les SRS peuvent également servir d'alerte précoce pour les personnes qui pourraient être devenues des menaces internes.

Les organisations doivent :

Établir un moyen de surveiller l'accès physique et réseau à partir de tous les points d'extrémité et des dispositifs à distance.

Développer une culture qui sensibilise davantage les employés à la sécurité et signale les activités inhabituelles ou les comportements anormaux.

Accroître la sensibilisation aux risques potentiels associés aux sites de médias sociaux.

Limiter l'accès à distance aux biens et aux systèmes non essentiels autant que possible.

Établir des protocoles pour signaler les incidents inhabituels, en assurer le suivi et intervenir.

Envisager de mobiliser les milieux de la sécurité et du renseignement, y compris la GRC ou le SCRS.

Mesure de sécurité nº 8
Protéger vos données[8]

La prévention est une première ligne de défense contre les menaces internes. Les organisations doivent veiller à ce que leurs systèmes et leurs données essentielles soient non seulement protégées, mais également sauvegardés avec un plan de rétablissement en place afin de réduire au minimum les interruptions en cas de compromission. La mise en place de mécanismes de secours et de rétablissement efficaces peut réduire considérablement le temps nécessaire pour rétablir un système après un incident. Les procédures de sauvegarde, de récupération et de surveillance des données et des systèmes doivent comprendre les éléments suivants :

Établir et mettre à l'essai des plans et des procédures de continuité des activités.

Dans la mesure du possible, les organisations doivent disposer de plusieurs copies de sauvegarde de données, stockées dans un endroit sûr et hors site. Cela comprend le contrôle de l'accès à la documentation et aux données de sauvegarde physique, visant à assurer que personne ne puisse y accéder. De plus, elles doivent exiger la divulgation complète de tout fournisseur tiers

8 Des ressources supplémentaires pour les risques internes se trouvent dans la publication spéciale 800-53 du NIST, révision 4, CP-2, CP-3, CP-4, CP-6, CP-9 et CP-10, et dans la norme ISO 27002 : 10.5.1

sous-traitant offrant des services de sauvegarde, y compris le stockage hors site. Elles doivent également mettre à l'essai leurs processus de sauvegarde et de reprise régulièrement dans le cadre de leur planification de la reprise après sinistre et de la continuité.

Mettre en œuvre des procédures pour limiter les points de sortie de l'information

L'un des défis pour les organisations est de s'assurer qu'elles savent non seulement où se trouvent leurs données, mais aussi par quelles voies et par quelles méthodes elles peuvent sortir de leurs réseaux et de leurs systèmes. Des politiques doivent être établies au sein d'une organisation afin de définir des règles et des lignes directrices acceptables pour le téléchargement et le stockage de grandes quantités de données ou de fichiers sensibles. Des politiques sur l'utilisation des dispositifs de stockage portatifs (clés USB, disques durs et appareils mobiles) devraient également être mises en œuvre, en particulier s'ils sont connectés ou ont accès au réseau informatique de l'organisation. Outre le fait de limiter les sources de points d'exfiltration potentiels de l'information, les organisations peuvent regrouper les points d'accès à Internet de manière à assurer une surveillance et une détection maximales aux points d'entrée et de sortie limités. Enfin, ces dernières peuvent mettre en œuvre des systèmes distincts qui préviennent la perte de données au moyen d'appareils isolés dont la connectivité au réseau est limitée ou inexistante. Par exemple, une organisation peut fournir aux employés un accès à Internet au moyen d'un ordinateur distinct qui n'est pas connecté au réseau corporatif de quelque façon que ce soit.

Mesure de sécurité nº 8

1) Établir et mettre à l'essai des plans et des procédures de continuité des activités
2) Mettre en œuvre des procédures pour limiter les points de sortie de l'information

Les organisations doivent :

Sauvegarder et protéger régulièrement toutes les données et tous les systèmes essentiels de l'organisme.

Élaborer des politiques relatives au téléchargement de grandes quantités de données ou de fichiers sensibles.

Regrouper les points d'accès à Internet.

Mettre en œuvre des systèmes distincts pour prévenir la perte de données.

Limiter ou restreindre les dispositifs de stockage portatifs.

Conclusion

La menace venant de l'intérieur peut provenir de n'importe qui et survenir à n'importe quel moment, et il n'y a pas de solution unique pour détecter ou prévenir ce type d'activité. Toutefois, le risque interne est un type de risque organisationnel fondamentalement différent qui peut être adéquatement atténué grâce à une approche holistique des mesures et des tactiques visant à limiter l'exposition et à réduire le risque. Une approche organisationnelle visant à réduire les risques internes devrait commencer au début du processus d'embauche et se poursuivre tout au long du cycle de vie de l'emploi. Les organisations doivent aussi être proactives et s'occuper immédiatement des employés qui affichent des comportements inhabituels. Elles doivent procéder aux vérifications des antécédents criminels et du crédit, ainsi que discuter avec les employeurs précédents au sujet d'un candidat à l'embauche. Elles doivent également mettre en place des politiques et des procédures permettant aux employés de signaler les comportements perturbateurs ou préoccupants de leurs collègues, ainsi qu'un solide programme d'aide aux employés pour aider les personnes en période de difficultés ou de stress.

La technologie joue également un rôle important dans la détection et l'atténuation des risques internes. Une surveillance adéquate de tous les biens numériques de l'organisation est essentielle, y compris de ses données essentielles et de l'information stockée sur son réseau. L'accès à l'information et aux systèmes corporatifs doit être géré en fonction de la sensibilité des données consultées. De plus, le mouvement des renseignements de nature délicate, des fichiers de données volumineux et l'activité du réseau doivent être surveillés, et toutes les données pertinentes doivent être sauvegardées et vérifiées régulièrement.

Le personnel d'une organisation peut être sa plus grande force, ou sa plus grande vulnérabilité , et les menaces internes mal intentionnées ou accidentelles peuvent causer des effets potentiellement dévastateurs pour toute organisation. Les organisations doivent donc être vigilantes et résilientes; surveiller continuellement le paysage de la menace; planifier méticuleusement les activités d'intervention et de rétablissement et mettre en œuvre des mesures de protection contre les incidents. Un risque interne peut menacer toutes les organisations, peu importe l'industrie, la géographie et le type de cible. En suivant les huit mesures de sécurité recommandées dans le présent guide, les organisations peuvent élaborer ou améliorer leurs propres programmes en matière de risque interne.

Même s'il est recommandé de prendre toutes ces mesures, il est reconnu que, compte tenu des ressources limitées, cela peut ne pas être possible pour une organisation donnée. Toutefois, l'une ou l'autre des mesures de sécurité mentionnées dans le présent document aurait une incidence en ce qui a trait à la sécurité d'une organisation face aux risques internes.

ANNEXE A

Scénarios de risque interne

Les deux scénarios de risque interne suivants sont hypothétiques et intègrent des éléments des huit mesures de sécurité décrites précédemment dans le présent guide. Les deux scénarios démontrent l'importance de mettre en œuvre des mesures de sécurité appropriées et peuvent être utilisés comme occasion d'apprentissage visant à atténuer le risque interne.

Scénario nº 1
Risque interne lié à un employé mal intentionné

Dans de nombreuses organisations, il y a des gens qui ont accès à des renseignements délicats et qui en ont le contrôle. La question qu'il faut se poser est la suivante : « Qu'arrive-t-il si l'une de ces personnes ressent le besoin de nuire à cette organisation, et quelles seraient les répercussions sur une organisation? » Par exemple, imaginez un employé du service informatique qui a des privilèges d'administrateur au sein d'une organisation et qui est sur le point d'être mis à pied. Un tel événement pourrait motiver l'employé à accéder aux systèmes directement ou à distance et à causer un préjudice injustifié aux utilisateurs en supprimant leurs privilèges d'utilisateur ou leurs renseignements d'ouverture de session. Si la personne veut causer des dommages plus importants, elle pourrait avoir une incidence sur les systèmes essentiels ou retirer des renseignements exclusifs qui sont essentiels aux activités de l'organisation. Pour compliquer la situation, elle pourrait également prendre des mesures pour empêcher le rétablissement, comme supprimer ou empêcher l'accès aux sauvegardes. Cette combinaison d'actions pourrait paralyser toute organisation qui fait l'objet d'une telle attaque. Il s'agit d'une situation de risque interne typique et d'une démonstration de six des mesures de sécurité présentées ci-dessus, à savoir :

- **Mesure de sécurité nº 1 : Instaurer une culture de sécurité :** La sécurité est un élément fondamental et essentiel de la gestion des risques opérationnels, comme les menaces internes liées à un employé mal intentionné ou qui cause du tort de façon non intentionnelle. Les politiques de sécurité organisationnelle doivent intégrer tous les secteurs d'une organisation et décrire les responsabilités de tous les employés.
- **Mesure de sécurité nº 5 : Offrir de la formation, accroître la sensibilisation et mener des exercices :** Il aurait fallu accorder une attention plus importante à la personne et la surveiller plus étroitement à l'approche de sa date de cessation d'emploi.
- **Mesure de sécurité nº 6 : Déterminer les biens essentiels et les protéger :** Cette situation aurait pu être évitée si les principales fonctions clés au sein de l'organisation avaient été réparties de façon à ce qu'une personne ne puisse voler ou modifier des données.
- **Mesure de sécurité nº 7 Intervenir face aux comportements inhabituels, les surveiller et les atténuer :** En accordant l'accès à distance uniquement aux courriels et aux données non essentielles, l'organisation aurait empêché l'exfiltration des données.
- **Mesure de sécurité nº 8 Protéger vos données :** Le fait de saisir le contenu complet des paquets au périmètre ou au minimum, de saisir le flux des données qui transit sur le réseau et d'envoyer une alerte à la

haute direction au sujet des anomalies à ces points de sortie aurait pu empêcher l'atteinte.

- **Mesure de sécurité nº 8 Protéger vos données :** Cela aurait pu être évité en contrôlant l'accès au support physique, ce qui signifie qu'aucune personne ne devrait avoir accès aux données en ligne et au support de sauvegarde physique. La règle des deux personnes pourrait également s'appliquer lorsque personne n'a un accès complet, mais exige le code d'accès ou l'approbation d'un deuxième administrateur.

Scénario nº 2

Risque interne lié à un employé qui n'était pas mal intentionné (involontaire)

La société A entretient une relation de travail continue avec la société B. La nature de cette relation exige un accès partagé aux réseaux communs. Dans le cadre des activités commerciales normales, un employé de la société A reçoit un courriel non sollicité contenant une pièce jointe malveillante. Considérant que le courriel est légitime, l'utilisateur ouvre la pièce jointe du courriel infecté et infecte involontairement son ordinateur. Le logiciel malveillant installe divers programmes conçus pour compromettre l'ordinateur de l'utilisateur et recueillir l'information disponible, comme l'identification de l'utilisateur et l'accessibilité du réseau. L'utilisateur ayant accès aux deux réseaux de l'entreprise, transmet bientôt cette infection à d'autres réseaux connectés, permettant ainsi au logiciel et à la personne responsable d'accéder sans autorisation à toute information qui peut être trouvée sur les réseaux associés. Il peut s'agir de renseignements exclusifs essentiels provenant des deux entreprises, comme les dossiers financiers, les données personnelles sur les employés de l'entreprise, ainsi que les noms d'utilisateur et les mots de passe des cadres de l'entreprise. Une fois que l'accès à un système est acquis, un attaquant n'est limité que par ses propres capacités et l'efficacité du système de se défendre et de se protéger. Il n'est pas rare que ce genre de présence non autorisée subsiste pendant des semaines, des mois et même des années. Les 5 mesures de sécurité suivantes doivent être notées dans ce scénario :

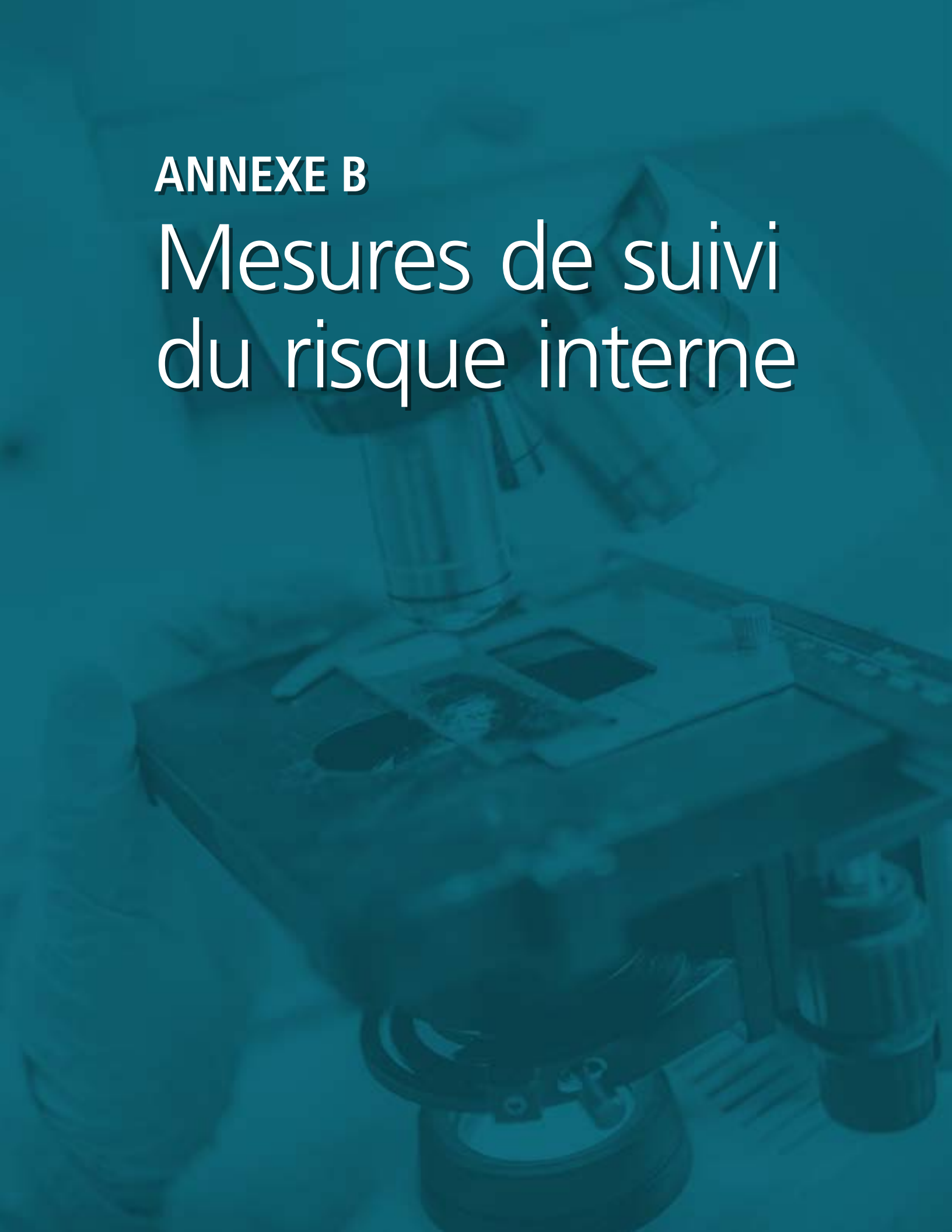
- **Mesure de sécurité nº 2 Élaborer des politiques et procédures de sécurité claires :** Une politique d'utilisation d'Internet consistant à ne pas lire ou ouvrir les pièces jointes suspectes aurait pu prévenir cette situation. La responsabilité n'incombe pas seulement à la personne, mais aussi à ceux qui sont chargés de veiller à ce que des systèmes adéquats de protection des courriels soient en place, appliqués et régulièrement mis à jour.
- **Mesure de sécurité nº 3 Réduire les risques associés aux partenaires et aux tiers fournisseurs :** La société B aurait dû tenir compte du fait

que la surface d'attaque d'un réseau d'entreprise de l'organisation est considérablement accrue, les tiers fournisseurs et partenaires ayant accès aux données sensibles et aux processus de réseau. Dans cette situation, les évaluations des risques effectuées par les deux entreprises auraient pu repérer cette dépendance ainsi que le risque connexe pour les réseaux connectés, et mettre en place des procédures, des politiques et des technologies pour atténuer le risque.

- **Mesure de sécurité nº 3 : Réduire les risques associés aux partenaires et aux tiers fournisseurs :** Les deux sociétés auraient pu rédiger une entente officielle régissant des domaines comme la propriété des données, la confidentialité, la propriété intellectuelle, l'utilisation du réseau et la non-divulgation avant de permettre à la société A d'avoir accès au réseau de la société B.
- **Mesure de sécurité nº 5 : Offrir de la formation, accroître la sensibilisation et mener des exercices :** Les employés doivent être sensibilisés aux bonnes pratiques relatives aux courriels et à Internet, ainsi qu'aux dangers auxquels une organisation pourrait être confrontée si elle était compromise par ces voies de communication. Une formation officielle sur la sensibilisation à la sécurité à l'intention de tous les employés devrait être obligatoire et appliquée régulièrement au moyen de communiqués, de bulletins, de courriels et des réseaux de médias sociaux ministériels.
- **Mesure de sécurité nº 6 Déterminer les biens essentiels et les protéger :** L'actif essentiel dans ce cas était l'information confidentielle stockée dans les systèmes de la société B. Si cette information avait été correctement recensée, segmentée et protégée, il est possible que l'intrus n'ait pas été en mesure d'accéder aux données. Chaque organisation doit déterminer ce qui est essentiel à sa mission et prendre les mesures nécessaires pour protéger ces biens contre toute compromission.

ANNEXE B

Mesures de suivi du risque interne



La résilience aux risques internes
8 mesures de sécurité recommandées

Établir une culture de sécurité
- ☐ Établir l'engagement et la responsabilisation de la haute direction
- ☐ Désigner un cadre supérieur responsable de la gestion des risques internes
- ☐ Établir un engagement de l'ensemble de l'organisation à l'égard de la sécurité et mettre l'accent sur le leadership à tous les niveaux

Élaborer des politiques et des procédures de sécurité claires
- ☐ Définir des attentes et des résultats clairs
- ☐ Déterminer les niveaux de risques des postes au sein de l'organisation
- ☐ Harmoniser l'accès des employés avec les niveaux de risque des postes

Réduire les risques des partenaires et des tiers fournisseurs
- ☐ Comprendre les principaux biens et systèmes
- ☐ Connaître vos partenaires
- ☐ Connaître vos risques

Mettre en œuvre un cycle de vie de filtrage de sécurité du personnel
- ☐ Effectuer les vérifications préalables à l'emploi
- ☐ Mettre en place un filtrage de sécurité continu des employés
- ☐ Incorporer les procédures de départ et de roulement interne
- ☐ Établir des politiques de sécurité transparentes

Offrir de la formation, accroître la sensibilisation et mener des exercices
- ☐ Offrir une formation régulière pour réduire les risques d'infractions non intentionnelles à la sécurité
- ☐ Accroître la sensibilisation aux signes avant-coureurs
- ☐ Favoriser une culture de vigilance et responsabiliser les employés

Déterminer les biens essentiels et les protéger
- ☐ Cerner et classer les principaux biens et systèmes
- ☐ Sécuriser les principaux biens et systèmes
- ☐ Exploiter la signalisation et les moyens de dissuasion visibles pour contrer l'accès
- ☐ Appliquer le principe de droit d'accès minimal
- ☐ Séparer les fonctions

Réagir aux comportements inhabituels, les surveiller et les atténuer
- ☐ Assurer un suivi de l'accès à distance et surveiller les dispositifs d'extrémités
- ☐ Établir des mesures efficaces de signalement, de suivi et d'intervention en cas d'incident
- ☐ Sensibiliser aux meilleures pratiques concernant l'utilisation des sites de réseautage social

Protéger vos données
- ☐ Établir et mettre à l'essai des plans et des procédures de continuité des activités
- ☐ Mettre en œuvre des procédures pour limiter les points de sortie de l'information

Sécurité publique Canada | Public Safety Canada

Canada

Mesure de sécurité nº 1
Instaurer une culture de sécurité

- ✓ Désigner un champion au sein de l'organisation pour la gestion des risques internes avec pleine responsabilité;
- ✓ désigner un cadre supérieur responsable de l'élaboration d'une politique et d'un programme de sécurité à l'échelle de l'entreprise;
- ✓ élaborer une structure de gouvernance, y compris un groupe de travail sur le risque interne, pour élaborer, exécuter et gérer un programme de risque interne;
- ✓ établir un « engagement » organisationnel pour reconnaître l'importance de la sécurité dans la réalisation d'une entreprise rentable et durable;
- ✓ concevoir des politiques et des procédures exhaustives de sécurité des réseaux physiques et cybernétiques englobant tous les départements;
- ✓ promouvoir une culture de sécurité à tous les niveaux en établissant un lien entre le rendement des employés et de la direction et les paramètres de sécurité.

Mesure de sécurité nº 2 :
Élaborer des politiques et des procédures de sécurité claires

- ✓ Définir clairement les politiques de sécurité corporative, les afficher et en faire part aux employés;
- ✓ effectuer la présélection des employés en fonction des exigences du poste;
- ✓ Attribuer des niveaux de risque appropriés aux employés en fonction de la criticité et de l'importance de l'information, des systèmes et du secteur auxquels ils ont accès.

Mesure de sécurité nº 3 :
Réduire les risques associés aux partenaires et aux tiers fournisseurs

- ✓ Procéder à une évaluation des risques à l'échelle de l'organisation pour déterminer tous les principaux biens et systèmes essentiels; cerner toutes les préoccupations en matière de sécurité liées à l'accès de tiers à ses réseaux, données et systèmes;
- ✓ vérifier de façon indépendante la posture de sécurité des tiers fournisseurs de services, y compris la vérification des antécédents des employés ayant accès aux installations ou aux réseaux essentiels d'une organisation;

- ✓ veiller à ce que des ententes de sécurité exhaustives conclues avec de tierces parties, dont le libellé d'assurance est inclus dans les ententes, réduisent les risques liés à la chaîne d'approvisionnement;
- ✓ établir des relations de confiance à long terme avec les principaux fournisseurs de services.

Mesure de sécurité nº 4 :
Mettre en œuvre un cycle de vie de la vérification de sécurité du personnel

- ✓ Effectuer une présélection approfondie et continue de tout le personnel en utilisant toutes les ressources disponibles, y compris les médias sociaux;
- ✓ mettre à jour l'accès et les autorisations de sécurité pour les employés en fonction des rôles et responsabilités de leur poste;
- ✓ modifier les privilèges d'accès pour les employés qui ont été mutés à de nouveaux postes au sein de l'organisation;
- ✓ promouvoir un programme de sécurité transparent auprès de tous les employés pour gérer les attentes en matière de sécurité physique et de sécurité du réseau.

Mesure de sécurité nº 5 :
Offrir de la formation, accroître la sensibilisation et mener des exercices

- ✓ Élaborer un programme de formation en sécurité pour tous les employés;
- ✓ accroître la sensibilisation aux indicateurs de préoccupations potentielles en matière de sécurité;
- ✓ donner accès aux programmes d'aide aux employés pour les aider à éviter que les employés ne courent un risque de compromission;
- ✓ développer et promouvoir une culture de vigilance en matière de sécurité en encourageant les employés à signaler ce qu'ils voient, le cas échéant;
- ✓ effectuer des exercices périodiques pour vérifier la position en matière de sécurité au sein d'une organisation.

Mesure de sécurité nº 6 :
Cerner les biens essentiels et les protéger

- ✓ Mener une évaluation à l'échelle de l'organisation pour cerner les biens et les systèmes essentiels et les classer, ainsi que déterminer les

mesures de sécurité pour les protéger;
- ✓ surveiller l'utilisation du système par les utilisateurs autorisés et non autorisés, ainsi que l'accès aux installations;
- ✓ décrire quelles données sont envoyées à des tiers et de quelle façon la transmission est effectuée, ainsi que la sensibilité des données, afin de protéger les données de façon appropriée;
- ✓ examiner le principe du droit d'accès minimal et de la séparation des fonctions concernant les systèmes et les données essentielles;
- ✓ tirer parti des moyens de dissuasion visibles pour réduire la probabilité d'un accès non intentionnel aux installations, aux réseaux et aux systèmes.

Mesure de sécurité nº 7 : **Surveiller les comportements inhabituels, y réagir et les atténuer**

- ✓ Établir un moyen de surveiller l'accès physique et réseau à partir de tous les points d'extrémité et des dispositifs à distance;
- ✓ développer une culture qui sensibilise davantage les employés à la sécurité et signale les activités suspectes ou les comportements anormaux;
- ✓ accroître la sensibilisation aux risques potentiels associés aux sites de médias sociaux;
- ✓ limiter l'accès à distance aux biens et aux systèmes non essentiels autant que possible;
- ✓ établir des protocoles pour signaler les incidents inhabituels, en assurer le suivi et intervenir;
- ✓ envisager de mobiliser les milieux de la sécurité et du renseignement, y compris la GRC ou le SCRS.

Mesure de sécurité nº 8 : **Protéger vos données**

- ✓ Sauvegarder et protéger régulièrement toutes les données et tous les systèmes essentiels de l'organisme;
- ✓ élaborer des politiques relatives au téléchargement de grandes quantités de données ou de fichiers sensibles;
- ✓ regrouper les points d'accès à Internet;
- ✓ mettre en œuvre des systèmes distincts pour prévenir la perte de données;
- ✓ limiter ou restreindre les dispositifs de stockage portatifs.

Annexe C: Bibliographie

Bowen, P., Hash, J., & Wilson, M. (2006). Information Security – A Guide for Managers. Gaithersburg: National Institute of Standards and Technology.

Caralli, R., Allen, J. H., White, D. W., Young, L. R., Mehravari, N., & Curtis, P. D. (2016). CERT Resilience Management Model, Version 1.2. Pittsburgh: Carnegie Mellon University.

CERT Inside Threat Center. (2016 – Décembre) Common Sense Guide to Mitigating Insider Threats. 5th Ed. Pittsburgh, PA, USA. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Gouvernement du Canada. (2009). Plan d'action sur les infrastructures essentielles. Ottawa : Sa Majesté du chef du Canada.

Joint Task Force Transformation Initiative. (2013). Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 (Revision 4). Bethesda, MD, États-Unis National Institute of Standards and Technology.

Nieles, M., Dempsey, K., & Yan Pillitteri, V. (2017). An Introduction to Information Security. Gaithersburg: National Instute of Standards and Technology.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Gaithersberg: National Institute of Standards and Technology.