

Ébauche de livre blanc

Sécurité orientée données

SÉCURITÉ ORIENTÉE DONNÉES

ÉBAUCHE DE LIVRE BLANC — AVRIL 2009

Auteur

Gerald D. Trites, FCA, CA•TI, CA•CISA

Directeur de projet

Malik Datardina, CA, CISA

Comité consultatif sur les technologies de l'information

Président

Ray Henrickson, CA•TI, CA•CISA, Banque Scotia, Toronto

Membres

Efrim Boritz, FCA, CA•TI/CISA, Ph.D., Université de Waterloo, Toronto

Nancy Y. Cheng, FCA, Bureau du vérificateur général du Canada, Ottawa

Malik Datardina, CA, CISA, Data Sync Consulting Inc., Mississauga
(conseiller du Comité)

Mario Durigon, CA, KPMG LLP, Toronto

Henry Grunberg, CA•TI, Ernst & Young LLP, Toronto

Andrew Kwong, CA, Deloitte & Touche LLP, Toronto

Carole Le Néal, CISA, CISSP, CIA, Mouvement des caisses Desjardins, Montréal

James R. Murray, CA•CISA, CA•CIA, Grant Thornton LLP, Halifax

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•TI, CA•CISA, CISM, PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA, Bureau du vérificateur général du Canada, Ottawa

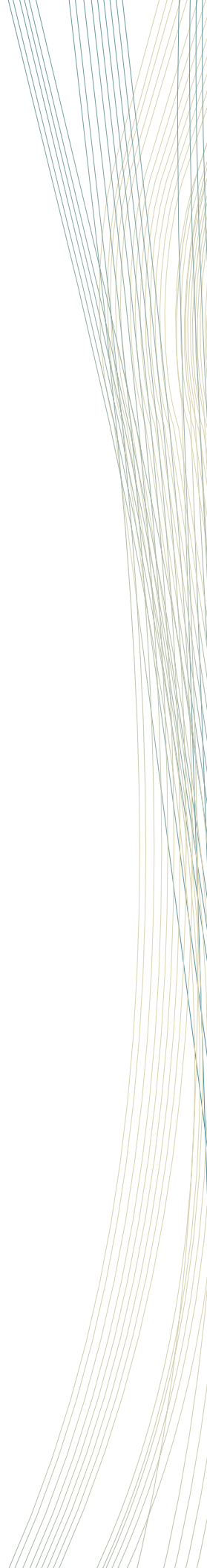
Gerald D. Trites, FCA, CA•TI, CA•CISA, Zorba Research Inc., Heatherton
(conseiller du Comité)

Bryan C. Walker, CA, L'Institut Canadien des Comptable Agés, Toronto

Permanent de l'ICCA

Dave Pollard, CA, vice-président, Développement des connaissances

Le Comité consultatif sur les technologies de l'information (CCTI) relève de la division Développement des connaissances de l'ICCA. Il joue un rôle de soutien et de conseil sur les questions de TI qui ont une incidence sur la profession de CA et sur le milieu des affaires.



INTRODUCTION

Dans la plupart des organisations, les données naguère statiques et stockées toutes au même endroit circulent à présent d'une plateforme à l'autre à travers toute l'entreprise, voire à l'extérieur de celle-ci. Puisque de nos jours ces données sont souvent générées et modifiées par les utilisateurs et qu'elles résident simultanément sous différentes formes et différentes versions à différents endroits, il devient de plus en plus difficile d'en assurer la sécurité.

Le présent livre blanc suggère que la direction, les auditeurs et les autres intervenants concernés par la sécurité des données dans ce nouvel environnement mobile mettent en place une politique orientée données. Dans le présent document, le terme «sécurité» s'entend au sens le plus large et comprend la confidentialité, l'intégrité (exactitude, exhaustivité et validité) ainsi que la disponibilité.

La prolifération de petits dispositifs portatifs ayant une grande capacité de traitement des données est la principale raison pour laquelle les données sont devenues à ce point mobiles. Les ordinateurs portables en sont un exemple évident, mais il en existe bien d'autres. Les assistants numériques personnels (PDA — *Personal Digital Assistants*), comme le Blackberry, offrent une capacité considérable de stockage et de transmission de données. Le courrier électronique et la messagerie instantanée (IM — *Instant Messaging*) sont devenus des moyens courants de transmission des données. Les téléphones cellulaires intelligents, comme le iPhone, sont de plus en plus performants et omniprésents; le iPod, naguère associé au seul stockage de musique, accueille maintenant d'autres formes de données. Enfin, de nombreuses organisations se servent de dispositifs de poche spécialisés pour saisir et mettre à jour les données sur les clients, prendre des commandes, traiter des paiements sur le terrain et conserver des registres de stocks.

Les données sensibles ayant trait aux clients, aux employés, aux contrats, aux listes de prix, à la recherche, etc., peuvent maintenant résider à tout moment sur des unités de ce type. De plus, ces données peuvent transiter d'un appareil à un autre ou d'une unité à une autre, et ce, sans fil. Par conséquent, les notions de «données au repos» et de «données en mouvement» sont des notions clés qui doivent être prises en compte dans l'élaboration d'une politique efficace de sécurité orientée données.

Puisque ces unités sont portatives et donc susceptibles d'être perdues ou volées, la première étape de l'élaboration d'une politique de sécurité orientée données doit prévoir la conception d'un processus permettant de connaître en tout temps l'emplacement des données et de suivre leurs mouvements d'une unité à une autre.

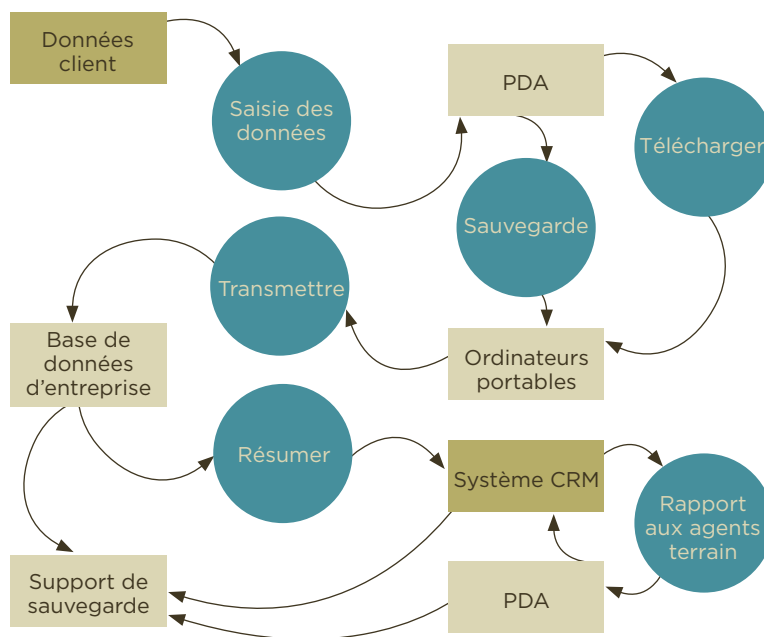


ÉLABORATION D'UNE POLITIQUE DE SÉCURITÉ ORIENTÉE DONNÉES

Phase 1 : Suivre les données

Les outils les plus utiles pour consigner le stockage et le déplacement des données sont des diagrammes de flux de données suffisamment détaillés pour localiser les données en tout temps au cours de leur déplacement.

La Figure A : Exemple de diagramme de flux de données



La Figure A illustre un exemple de flux de données dans une entreprise. Les données résident tout d'abord dans les fichiers clients, puis sont ensuite saisies par un représentant de l'entreprise et stockées sur un assistant numérique personnel (PDA – *Personal Digital Assistant*). Durant la soirée, le représentant télécharge les données du PDA dans un ordinateur portable et les transmet dans la base de données de l'entreprise. Les données sont résumées dans un système de gestion des relations avec la clientèle (CRM – *Client Relationship Management*) et mises à la disposition des agents sur le terrain, qui les saisissent dans leur PDA. D'autres modes de gestion des données sont également possibles; par exemple, les données pourraient être saisies directement dans l'ordinateur portable ou transmises directement du PDA dans la base de données de l'entreprise.

Chaque cercle du diagramme représente des données en mouvement et chaque carré représente des données au repos. Les données sont en mouvement lorsqu'elles sont saisies, téléchargées, transmises, résumées et consultées par les agents sur le terrain. Dans ce diagramme, les données sont au repos dans un PDA deux fois, ainsi que dans un ordinateur portable et dans les bases de données de l'entreprise. Les supports magnétiques de sauvegarde contiennent des données au repos, mais ils doivent se trouver hors site et donc être transportés ailleurs.

Poursuivons avec cet exemple et voyons les différents risques qui se présentent à chaque étape :

- *Saisie des données* : Cette étape pourrait comprendre une saisie manuelle, et donc comporter un risque inhérent d'erreur humaine, ou s'effectuer au moyen de courtes fréquences, comme Bluetooth, lesquelles ne sont pas sans risque de détection par d'autres unités électroniques à proximité.
- *Téléchargement* : Un téléchargement par connexion filaire ne présente à peu près aucun risque, sauf la possibilité d'une erreur humaine. Un téléchargement sans fil risque d'être détecté par une autre unité électronique à proximité.
- *Transmission* : Les données sont probablement transmises par Internet. Le degré de sécurité de telles transmissions varie selon les entreprises. Certaines recourent à un réseau privé virtuel (VPN — *Virtual Private Network*), alors que d'autres permettent l'utilisation du courriel standard. En l'absence d'un système de sécurité très efficace, le risque que les données soient lues par des personnes non autorisées est relativement élevé.
- *Résumé* : Pour être résumées, les données doivent passer par une application quelconque. La sécurité dépend alors des contrôles mis en place pour cette application et pour l'environnement dans lequel elle s'exécute.
- *Consultation par le personnel de terrain* : Le personnel de terrain consulte les données selon une méthode quelconque fondée sur Internet, peut-être similaire à celle qui a servi à transmettre les données au départ. Les risques sont donc semblables. De plus, le risque que des personnes non autorisées accèdent aux transmissions de données effectuées par le personnel de terrain dépend de la puissance des fonctions de transmission de données.

La puissance des appareils utilisés pour copier ou modifier les données saisies pose des problèmes supplémentaires de contrôle relatifs à la possibilité pour les utilisateurs d'effectuer de telles actions, à la sécurité et à l'intégrité des nouvelles copies ou versions et au lieu où elles sont stockées.

Comme nous l'avons mentionné, les données sont au repos en divers points dans cet exemple :

- *Assistants numériques personnels (PDA — Personal Digital Assistants)* : Ces petites unités à main sont évidemment très vulnérables à la perte et au vol. Même si elles sont habituellement dotées de fonctions de sécurité telles que des mots de passe, ces fonctions peuvent être sans effet, surtout en cas de vol de l'unité. Certaines versions récentes offrent également la connectivité WI-FI, ce qui accroît le risque de transmettre des données sur des réseaux non protégés.
- *Ordinateurs portables* : Comme en témoigne l'Annexe B, on a constaté de nombreux incidents où la confidentialité de renseignements personnels sensibles a été compromise par suite de la perte ou du vol d'un ordinateur portable. De nombreux ordinateurs portables offrent de très bonnes fonctions de sécurité, particulièrement celles qui reposent sur le chiffrement. Cependant, un sondage a révélé que 46 % des entreprises n'utilisent pas le chiffrement¹.
- *Base de données d'entreprise/ERP/CRM* : Les données qui résident à l'intérieur du pare-feu d'un système d'entreprise devraient être plus faciles à contrôler puisqu'elles font l'objet des procédures de sécurité du système central. Bien entendu, tous les éléments traditionnels des bons systèmes de sécurité doivent être en place, soit la séparation des fonctions, le contrôle d'accès, le contrôle physique et la surveillance.

Phase 2 : Évaluation du risque de perte de données

Il est nécessaire de procéder à une évaluation du risque de perte de données sur chaque système pour déterminer les contrôles appropriés à chacun relativement au risque de divulgation ou de corruption de données, et le niveau de risque que l'entreprise est prête à assumer. Il serait déraisonnable de supposer que toutes les données de l'entreprise nécessitent un contrôle maximal. Une telle démarche serait coûteuse et engendrerait des contrôles superflus. Par exemple, certains renseignements sur les clients, collectés par le personnel de terrain, pourraient être considérés publics et donc ne nécessiter aucun contrôle, alors que d'autres données sont privées et sensibles et doivent être contrôlées.

Des documents contiennent des lignes directrices utiles pour effectuer des évaluations de risques, notamment le cadre de contrôle COBIT 4.1, *Risk and Control Objectives*, et les publications de l'ICCA² *Lignes directrices sur l'intégrité des données et Infrastructure TI sécurisée pour le commerce électronique*.

L'évaluation du risque de perte de données doit tenir compte de la sensibilité des données et de leur emplacement dans l'entreprise, qu'elles soient au repos ou en mouvement.

Classement des données

L'évaluation commence par le classement des données selon les facteurs de risque, par exemple :

- *Données publiques* : Données dont la diffusion aurait peu ou n'aurait pas d'effet négatif pour l'entreprise.
- *Données d'exploitation internes* : Données nécessaires aux employés de l'entreprise dans l'exécution de leur travail et qui ne sont pas destinées à une diffusion publique.
- *Données confidentielles* : Données régies par la législation relative à la protection de la vie privée (ou réputées confidentielles dans le cadre d'obligations contractuelles) et dont la diffusion pourrait causer des difficultés juridiques à l'entreprise ou la mettre dans l'embarras.

La direction doit également tenir compte de la perte de réputation, de la perte d'avantages concurrentiels, de sanctions réglementaires ou juridiques ou de rupture de contrat qui pourraient survenir si les données tombaient en de mauvaises mains.

Une fois les risques inhérents identifiés, restent les risques résiduels. Après avoir établi les contrôles d'atténuation pour les risques inhérents, des contrôles compensatoires supplémentaires peuvent réduire les risques résiduels à un niveau acceptable.

Phase 3 : Application des contrôles dans une politique orientée données

Des contrôles doivent être appliqués sur les parties du système où les données sont le plus exposées à un accès non autorisé, qu'elles résident sur un appareil ou qu'elles transitent d'un appareil à un autre.

Chiffrement : contrôle essentiel de sécurité orientée données

Le chiffrement est un contrôle essentiel dans un système orienté données, car les données passent par différents systèmes et sont souvent vulnérables à des attaques de sources diverses tout au long de leur parcours. Le chiffrement est l'un des moyens les plus efficaces pour protéger les données en mouvement. Cela ne signifie pas qu'il faille l'appliquer dans tous les cas, mais bien qu'il est normalement approprié d'élaborer une stratégie de chiffrement dans le cadre de la stratégie globale de contrôles. C'est donc dire que le résultat direct de l'analyse des risques est l'identification des données qu'il est nécessaire de chiffrer. Parfois, il n'est tout simplement pas possible de chiffrer les données (par exemple, bon nombre des dispositifs mobiles sur le marché n'offrent pas de fonction de sécurité efficace), auquel cas il faut envisager d'autres contrôles.

Dans les situations récentes où des renseignements personnels ont été exposés à des risques en raison de la perte de disques durs d'ordinateur ou de supports magnétiques de sauvegarde, le chiffrement des données aurait considérablement atténué les risques.

Rôle du chiffrement

Le chiffrement comme moyen de protection des données, qu'elles soient au repos ou en mouvement, est l'un des contrôles les plus puissants qui soient et doit donc être envisagé chaque fois qu'une forte protection est nécessaire. Chaque fois que c'est possible, il est préférable d'opter pour une seule méthodologie de chiffrement, comme celle qui se fonde sur la norme PGP (*Pretty Good Privacy*), et de s'en servir partout dans l'entreprise, afin que les données puissent être facilement récupérées en cas de perte ou de corruption des clés de chiffrement. Normalement, il ne suffit pas d'utiliser les technologies de chiffrement qui existent dans les divers référentiels d'information, comme les ordinateurs portables, les assistants numériques personnels (PDA), les téléphones cellulaires ou des technologies comme Wi-Fi ou Bluetooth.

Une seule méthodologie de chiffrement doit être appliquée partout dans l'entreprise pour les raisons suivantes :

- les fichiers qui ont été chiffrés doivent demeurer accessibles dans les années à venir à des fins commerciales, d'audit, de fiscalité ou à d'autres fins réglementaires; l'entreprise doit donc avoir la maîtrise de la technologie de déchiffrement utilisée, notamment la maintenance des clés cryptographiques;
- puisque les données peuvent circuler dans des systèmes de taille variable, le processus de chiffrement doit être évolutif pour fonctionner aussi efficacement dans un seul petit ordinateur que dans plusieurs grands systèmes;
- du fait que les données passent d'une plateforme à l'autre, la solution de chiffrement doit fonctionner sur toutes les plateformes importantes du système;
- en l'absence d'une seule et unique technologie de chiffrement, toutes les données devront être déchiffrées avant utilisation et chiffrées de nouveau après utilisation.

Norme de chiffrement

Il existe divers niveaux de chiffrement, et chacun requiert l'utilisation de clés de chiffrement de différentes longueurs. Les plus courantes sont les clés de 64 et 128 bits, bien qu'il existe des niveaux de chiffrement plus faibles et plus élevés. En général, le chiffrement à 64 bits n'est pas adéquat pour protéger les données de l'entreprise. L'algorithme DES à 64 bits a souvent été neutralisé dans le passé et l'est maintenant régulièrement. La politique de chiffrement doit donc exiger le chiffrement à 128 bits, qui devrait être adéquat dans la plupart des cas.

Gestion des clés

La gestion des clés publiques et privées est une partie importante de n'importe quelle politique de chiffrement. Comme l'indique la norme ISO/IEC 17799:2005, la gestion des clés comprend :

- la production des clés;
- l'obtention de certificats de clé publique;
- la distribution des clés;
- le stockage des clés;
- la mise à jour ou la modification des clés;
- les procédures de gestion des clés compromises;
- les procédures de révocation des clés;
- le recouvrement des clés perdues ou corrompues;
- la gestion des clés qui déchiffrent les sauvegardes;
- les pistes de vérification associées aux processus et procédures de gestion des clés³.

Si les clés sont insuffisamment protégées ou mal gérées, le risque de violation du chiffrement s'accroît.

Bien que toutes les entreprises aient besoin de contrôles élémentaires de gestion des clés, la rigueur et le coût de ceux-ci varient d'une entreprise à l'autre. Par exemple, il convient habituellement que la gestion des clés soit entièrement automatisée et que les clés privées demeurent confidentielles; toutes les clés, cependant, doivent être chiffrées. Les clés utilisées pour chiffrer d'autres clés doivent être distinctes des clés de déchiffrement des données. Les clés de courte durée doivent, si possible, comporter des dates d'activation et de désactivation. Il est important que les clés soient choisies de façon aléatoire. VISA a publié un document contenant une liste détaillée des procédures de gestion des clés sous le titre *Payment Card Industry PIN Security Requirements*⁴.

Contrôle des points d'extraction des données

Le contrôle des points d'extraction des données, tels que les ports USB et les unités de CD/DVD inscriptibles, est une autre technique qui contribue au contrôle des risques liés aux données. À partir de ces points, il est possible d'extraire les données et de les utiliser sans autorisation. Le contrôle des points d'extraction peut s'effectuer comme suit :

- *Solutions de gestion des points d'extrémité* : Des contrôles activés par la technologie permettent de gérer la connexion et l'utilisation des appareils. Ces technologies, par exemple, permettent de surveiller les fichiers transférés par le port USB ou l'unité de disque et limitent l'utilisation du copier-coller. Ces outils peuvent être achetés dans le cadre d'une solution complète de prévention des pertes de données.
- *Désactivation des ports USB et des unités CD/DVD* : Si les ports et les unités ne sont pas nécessaires à l'exploitation du système, comme dans le cas des sauvegardes, des contrôles peuvent les désactiver. Par exemple, les ports USB des ordinateurs d'un centre d'appel pourraient être désactivés pour empêcher toute utilisation non autorisée par un employé.

Contrôles des dispositifs électroniques portatifs

Les vols et les pertes d'ordinateurs portables sont courants. Par conséquent, les contrôles du matériel sont particulièrement pertinents dans une politique de sécurité orientée données, car la portabilité et d'autres caractéristiques de ce type de matériel constituent des risques inhérents. Les données peuvent aussi être exposées à d'autres risques que le vol ou la perte; par exemple, les ordinateurs portables peuvent faire l'objet de fouilles et de saisies aux frontières internationales. Ces risques peuvent être atténués comme suit :

- *Authentification multifactorielle* : Le chiffrement des ordinateurs portables pouvant être contourné par les utilisateurs avertis, les entreprises devraient envisager le recours à l'authentification multifactorielle, comme la combinaison de mots de passe et de caractéristiques biométriques ou la combinaison de mots de passe et de dispositifs d'accès à jeton USB.
- *Installation d'un logiciel de suivi* : Un logiciel de suivi permet à l'ordinateur portable d'émettre un signal lorsqu'il est relié à Internet. Ce logiciel peut également désactiver l'ordinateur portable et (ou) supprimer toutes les données. Une étiquette devrait être apposée sur les ordinateurs utilisant ce logiciel pour avertir les voleurs potentiels que l'appareil fera l'objet d'un suivi en cas de vol.
- *Utilisation de l'ordinateur portable comme terminal et non comme unité de stockage* : Un ordinateur portable utilisé comme terminal nécessite de centraliser le stockage des données et d'utiliser des services de terminal, des connexions sécurisées (par exemple un réseau privé virtuel, ou VPN) et des contrôles permettant de s'assurer que les utilisateurs ne stockent pas de données sur leur ordinateur portable, que ce soit intentionnellement ou par inadvertance. De plus en plus d'entreprises stockent leurs données sur Internet ou sur leurs propres serveurs et n'autorisent aucun stockage sur les ordinateurs portables. Certaines entreprises commencent à utiliser des miniportatifs pour stocker leurs données sur Internet.

Outils de surveillance en prévention des pertes de données (DLP)

Certaines entreprises ont commencé à utiliser des outils de surveillance en prévention des pertes de données (DLP — *Data Loss Prevention*), relativement nouveaux, pour déceler les fuites de données. Pour en savoir plus sur la prévention des pertes de données, consultez les sites des divers fournisseurs.

Procédures de diffusion de l'information

Pour aider à contrôler les fuites de données, la direction doit également examiner de quelle façon l'information est transmise aux parties externes. Il faut établir des normes strictes d'authentification avant de transmettre de l'information privée à des parties externes. Par exemple, il doit exister une procédure obligeant les employés à vérifier l'identité des messagers.

Les contrats avec des tiers ou d'autres entités indépendantes doivent contenir des clauses prévoyant des pénalités afin de protéger les données partagées. La direction doit être autorisée à auditer les contrôles de sécurité orientés données ou avoir droit à un rapport de vérification conforme au chapitre 5970 du *Manuel de l'ICCA*, un rapport en vertu de la SAS 70, ou une mission de services Trust attestant l'efficacité opérationnelle des contrôles de sécurité orientés données. La direction doit également exiger des tiers que ceux-ci l'informent de tout manquement.

Phase 4 : Officialisation de la politique de sécurité orientée données

Une fois terminées les phases 1 à 3, la direction peut officialiser et approuver la politique de sécurité orientée données et la diffuser aux utilisateurs. La politique doit servir de référence pour la gestion des données partout dans l'entreprise. L'Annexe A contient les éléments d'une politique de sécurité orientée données.

CONCLUSIONS

L'utilisation de différents appareils de communication et de stockage de données par les employés et les tiers extérieurs requiert des entreprises modernes qu'elles élaborent des politiques de sécurité orientées données permettant le suivi des données à travers tout le système, car la plupart des systèmes sont reliés par l'intermédiaire de différents types de matériel. Cet environnement d'exploitation expose l'entreprise à la perte de données en raison de la perte d'unités portatives contenant des données et (ou) de la violation de la sécurité offerte par des unités spécifiques et (ou) de la perte de données résidant dans un endroit anormal ou transmises sur des supports non protégés.

Seule une politique de sécurité coordonnée, permettant de localiser les données en tout temps et d'identifier et de contrer le risque d'accès non autorisé, sera efficace. Toutefois, une politique bien conçue qui répond à ces critères ne pourra produire de résultats que si elle est diffusée auprès des employés et que ceux-ci croient en son bien-fondé et reçoivent la formation nécessaire à son utilisation.



ANNEXE A : ÉLÉMENTS D'UNE POLITIQUE DE SÉCURITÉ ORIENTÉE DONNÉES

[**Remarque :** Ces exemples peuvent être personnalisés selon les besoins de chaque entreprise.]

Les données sont un élément vital de l'entreprise et doivent être protégées. Pourtant, toujours en déplacement entre divers appareils et unités à l'intérieur et à l'extérieur de l'entreprise, elles sont soumises à un risque d'accès non autorisé. Le chiffrement est le moyen de protection le plus efficace. La présente politique définit les principes à respecter pour concevoir une politique de sécurité orientée données basée sur un chiffrement à 128 bits. Une analyse de risque doit être effectuée chaque année pour comprendre le flux des données de l'entreprise et pour évaluer le caractère adéquat des contrôles.

Les données au repos et les données en mouvement présentent deux problèmes de contrôle différents. Les données au repos sont habituellement contenues dans des systèmes protégés (ou qui devraient l'être) par les systèmes de sécurité en place. Les données en mouvement passent dans divers autres systèmes dont certains peuvent exiger des précautions supplémentaires parce qu'ils échappent au contrôle du propriétaire des données.

DONNÉES AU REPOS

Supports fixes

- Protégez les données d'entreprise au repos dans des supports fixes tels que des serveurs d'entreprise situés dans des zones sécurisées par un pare-feu assurant de stricts contrôles d'accès.
- Reliez ces contrôles à un réseau privé virtuel (VPN — *Virtual Private Network*) pour que toutes les données qui circulent d'un serveur à un autre soient chiffrées.
- Sécurisez les systèmes qui contiennent ou transmettent des données à l'aide d'un logiciel antivirus ou d'une protection similaire. Désactivez les services et les ports non utilisés et faites en sorte que les applications soient correctement configurées.

Supports amovibles

Les supports amovibles comprennent les CD-ROM, les disquettes, les bandes de sauvegarde, les clés USB et tout autre dispositif portatif pouvant contenir des données.

- Chiffrez tous les supports amovibles contenant des données d'entreprise et stockez-les dans un endroit sûr et verrouillé; n'utilisez pas de mot de passe.

DONNÉES EN MOUVEMENT

Sécurité des transmissions

- Chiffrez tous les messages de courrier électronique contenant des données d'entreprise.
- Chiffrez toutes les données d'entreprise transmises sur un réseau public comme Internet ou passez par un tunnel chiffré.

- Chiffrez les tunnels selon le chiffrement à clé publique de 128 bits, comme dans le réseau privé virtuel (VPN) de l'entreprise ou dans les protocoles PPTP (Point-to-point Tunnel Protocol) comme SSH (Secure Shells) et SSL (Secure Socket Layer).
- Chiffrez les transmissions sans fil (Wi-Fi) à l'aide de WPA ou d'un chiffrement supérieur.

Supports amovibles

- Avant de transporter des supports amovibles, identifiez le destinataire, vérifiez son authenticité et assurez-vous qu'il peut recevoir les supports en toute légitimité.
- Transportez les supports de manière sécurisée, c'est-à-dire avec une compagnie de transport, une méthode d'emballage, des moyens de transport et une possibilité de suivi dûment approuvés et documentés.

Dispositifs portatifs

- Chiffrez les données d'entreprise stockées sur des dispositifs portatifs tels que des ordinateurs portables et des assistants numériques personnels (PDA — *Personal Digital Assistants*).
- N'utilisez pas d'appareils portatifs pour le stockage à long terme de données d'entreprise.
- Installez un logiciel antivirus, un logiciel pare-feu et un mécanisme de chiffrement sur tous les appareils portatifs utilisés pour stocker ou transmettre des données d'entreprise.
- Désactivez tous les services et les ports non utilisés.

GESTION DES CLÉS

- Dans la mesure du possible, utilisez l'infrastructure de clé publique (PKI — *Public Key Infrastructure*) de l'entreprise. Il doit être expressément interdit aux utilisateurs de se servir de normes ou d'outils de chiffrement non reconnus par l'entreprise.
- Automatisez la gestion des clés.
- Chiffrez toutes les clés et assurez la confidentialité des clés privées.
- Séparez et distinguez les clés de chiffrement des clés de déchiffrement des données.
- Dans la mesure du possible, utilisez des clés de courte durée pourvues de dates d'activation et de désactivation.
- Choisissez les clés de façon aléatoire.
- Partagez le chargement des clés entre deux personnes⁵.
- Répartissez la connaissance des clés entre deux personnes. Nul ne doit connaître à lui seul tous les renseignements relatifs à une clé⁶.

ANNEXE B : EXEMPLES DE FUITES DE DONNÉES

Les fuites de données liées à la perte ou au vol d'un ordinateur portable, d'un téléphone mobile ou d'un assistant numérique personnel sont devenues monnaie courante. Par exemple, le 19 septembre 2008, le ComputerWeekly.com rapportait ce qui suit : «Un sondage mené par Credant Technologies auprès des chauffeurs de taxi de Londres a révélé que 55 843 téléphones mobiles et 6 193 autres dispositifs tels que des ordinateurs portables ont été oubliés sur la banquette arrière des taxis noirs au cours des six derniers mois. Ce résultat correspond à celui d'un sondage effectué quelques années auparavant par Pointsec, qui montrait que durant le dernier semestre de 2004, 63 135 téléphones mobiles, 5 838 assistants numériques personnels et 4 973 ordinateurs portables ont été oubliés dans des taxis londoniens.»

D'après un sondage effectué en 2007 par PricewaterhouseCoopers auprès des entreprises du Royaume-Uni, 72 % des grandes entreprises ont fait l'objet d'une effraction qui les a exposées à la «perte de données confidentielles⁷». Dans un autre sondage, le Poneman Institute a révélé que 85 % des «cadres supérieurs d'échelon C» interrogés avaient indiqué qu'on avait déjà atteint à la sécurité de leurs données⁸. Les risques les plus courants à l'origine de ces atteintes étaient liés à un contrôle inapproprié des éléments suivants :

- dispositifs électroniques portatifs;
- dispositifs de stockage de données;
- processus d'élimination des dossiers et des dispositifs de stockage de données;
- accès à l'information sensible stratégique;
- procédure de diffusion de l'information.

Voici des exemples d'incidents spécifiques dans chacune de ces catégories.

Dispositifs électroniques portatifs

Une étude a montré qu'aux États-Unis, 1 000 ordinateurs portables disparaissent chaque jour et que seulement 3 % d'entre eux sont retrouvés⁹. Les assistants numériques personnels (Blackberry, etc.) sont exposés à des risques similaires. Voici des exemples de tels incidents :

- Février 2008 : Vol d'un ordinateur portable des National Institutes of Health contenant les données chiffrées d'environ 2 500 patients participant à un projet de recherche¹⁰.
- Mai 2006 : Le département américain des Anciens combattants (VA) s'est fait voler un ordinateur portable contenant 26,5 millions d'enregistrements contenant des dates de naissance et des numéros d'assurance sociale¹¹.
- Février 2006 : Un ordinateur portable appartenant à Hotel.com et contenant les dossiers de 243 000 clients, où figuraient leurs «noms, adresses et renseignements de carte de crédit ou de débit» a été volé dans la voiture d'un vérificateur de Ernst & Young¹².
- Mai 2005 : Vol d'un ordinateur portable contenant les renseignements de carte de crédit de 80 000 employés du département américain de la Justice¹³.

Supports et dispositifs de stockage

Les bandes de sauvegarde, les disques et les autres dispositifs de stockage sont également susceptibles d'être volés ou perdus. Par exemple :

- Avril 2008 : HSBC a perdu un disque contenant 370 000 dossiers, où figuraient des noms, des dates de naissance et d'autres renseignements personnels¹⁴.
- Novembre 2007 : Le ministère du Revenu et des Douanes du Royaume-Uni a perdu des disques contenant des renseignements sur les demandeurs de prestations pour enfant, ce qui a touché 25 millions de personnes¹⁵.
- Mai 2007 : Alcatel-Lucent a perdu la trace d'un disque contenant les renseignements personnels de ses employés, incluant «le nom, l'adresse, la date de naissance, le numéro de sécurité sociale et la date de versement du salaire¹⁶» de plus de 200 000 employés, retraités et leurs personnes à charge¹⁷.
- Février 2007 : La filiale de fonds communs de placement de la Banque Canadienne Impériale de Commerce, Talvest, a perdu un disque de sauvegarde contenant les renseignements personnels de 470 000 clients¹⁸.

Élimination des fichiers et des dispositifs de stockage

L'élimination non protégée des données constitue un autre sujet de préoccupation. Par exemple, la Banque de Montréal a vendu accidentellement des serveurs contenant «les noms, adresses et numéros de téléphone de plusieurs centaines de clients de la Banque, ainsi que les renseignements sur leurs comptes bancaires comme le type et le numéro de compte, les soldes et, dans certains cas, les soldes des CPG, REER, marges de crédit, cartes de crédit et assurances¹⁹». Dans le cadre d'un autre incident, la clinique Select Physical Therapy a été accusée par le procureur général du Texas de «viol de la loi sur la protection contre le vol d'identité²⁰» pour avoir mis au rebut dans un conteneur à ordures 4 000 documents contenant des renseignements sensibles sur ses clients²¹.

Information sensible stratégique. Même si le vol de données par des concurrents ne fait pas les manchettes²², il s'agit néanmoins d'un risque qui doit être géré. Par exemple, le cofondateur de Bureau en gros, Thomas Stemberg, a ouvertement reconnu avoir envoyé son épouse se faire embaucher par Office Depot afin de savoir comment fonctionnait leur nouveau système de livraison²³. Dans une perspective de sécurité orientée données, des utilisateurs malveillants peuvent brancher les unités de stockage de masse sur des ports USB non contrôlés afin d'obtenir de façon illicite des secrets commerciaux ou d'autres données sensibles²⁴. Les employés peuvent également se servir de systèmes de courriel Web (comme Gmail, Hotmail, etc.) pour transmettre par courriel des fichiers sensibles à l'extérieur de l'entreprise. Par exemple, Shin-Guo Tsai s'est servi de son compte personnel de courrier électronique pour obtenir des renseignements stratégiques sur les produits vendus par Volterra, son employeur. Après avoir été interrogé par la police, il aurait admis avoir obtenu ces renseignements afin de les donner à une nouvelle entreprise de Taiwan qui voulait le recruter^{25, 26}. Dans le cadre d'un autre incident, un dirigeant d'une entreprise de sécurité TI s'est fait voler sous la menace d'une arme son ordinateur portable contenant les plans directeurs non chiffrés des principaux produits de son entreprise^{27, 28}.

Diffusion des données à des parties non autorisées

Une autre cause de fuite de données réside dans les processus mal conçus qui donnent par inadvertance accès aux données à des personnes non autorisées. L'étendue de ce problème a été démontrée dans le cadre d'un concours dans lequel les participants ont trouvé des renseignements sensibles (noms, numéros de carte de crédit, etc.) sur environ 25 millions de personnes — uniquement en utilisant le moteur de recherche Google²⁹. En décembre 2007, le Bureau des passeports du Canada a signalé une brèche de sécurité par laquelle les demandeurs de passeport pouvaient avoir accès aux dossiers d'autres demandeurs en modifiant l'adresse Internet dans leur navigateur Web³⁰. En 2004, Choicepoint Inc. a été victime d'une brèche de sécurité largement publicisée qui a entraîné la divulgation par l'entreprise des renseignements personnels (en l'occurrence, l'historique de crédit) de quelque 163 000 clients à des fraudeurs parce qu'elle n'avait pas suffisamment contrôlé les entreprises destinataires de ces renseignements³¹. La FTC (Federal Trade Commission) a imposé une amende de 10 millions \$ à ChoicePoint et l'a obligée à verser 5 millions \$ en dédommagement aux 800 personnes affectées par cette brèche, pour n'avoir pas respecté les lois fédérales sur les droits et la vie privée des consommateurs³².

Courrier électronique, messagerie instantanée et autres canaux de communication électroniques

Selon un sondage effectué en 2007, les participants considéraient en moyenne que 20 % de leur courrier électronique sortant constituait «un risque juridique, réglementaire ou financier pour leur entreprise³³». Le sondage a également montré que près de 40 % des entreprises (comptant plus de 20 000 employés) embauchent du personnel pour analyser le contenu du courrier électronique sortant³⁴.

Selon Gartner, les applications de messagerie instantanée (IM — *Instant Messaging*) présentent des risques pour l'entreprise, car il n'existe aucun mécanisme standard de chiffrement pour protéger les messages envoyés. L'absence de «conventions d'appellation universelles» empêche la résolution des litiges relatifs au contenu des communications et aux expéditeurs, et le manque de surveillance de tels canaux de communication permet aux employés de contourner les politiques d'utilisation acceptable³⁵.



Notes

- 1 Denise Dubie, «Data breaches plague U.S. companies», *Network World*, Southborough, vol. 24, n° 20 (15 mai 2007), p. 25. Voir www.networkworld.com/news/2007/051507-data-breaches.html [consulté le 15 août 2008].
- 2 Disponibles sur le site www.icca.ca.
- 3 Organisation internationale de normalisation, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information* (ISO/IEC 17799:2005), Genève, Suisse, 2^e édition, 15 juin 2005.
- 4 Visa International, *Payment Card Industry PIN Security Requirements* (Visa Public 40026-02), 2004. Voir https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrieveId=95 [consulté le 6 août 2008].
- 5 *Ibid.*
- 6 *Ibid.*
- 7 On entend par «grande entreprise» une entreprise employant plus de 250 personnes; Kieran Poynter, «Good data security is not just a matter of technology», *Financial Times*, Londres, R.-U., 16 juillet 2008, p. 13.
- 8 Denise Dubie, «Data breaches plague U.S. companies», *Network World*, Southborough, vol. 24, n° 20 (15 mai 2007), p. 25. Voir www.networkworld.com/news/2007/051507-data-breaches.html [consulté le 15 août 2008].
- 9 Andy Dornan, «It's audit time — Do you know where your private data is?», *IT Architect*, Manhasset, vol. 20, n° 9 (septembre 2005), p. 35 à 41.
- 10 Mary Mosquera, «Stolen laptop reveals security gap», *Federal Computer Week*, Falls Church, vol. 22, n° 7 (31 mars 2008), p. 9.
- 11 Larry Greenemeier, «No more excuses», *InformationWeek*, Manhasset, n° 1091 (29 mai 2006), p. 23 à 25.
- 12 Reuters News Service, «Hotels.com: Credit-card data is lost in stolen laptop computer», *Wall Street Journal*, New York (N.Y.), édition de l'est, 6 juin 2006.
- 13 Gary Fields, «Stolen PC had credit-card data for 80,000 government workers», *Wall Street Journal*, New York (N.Y.), édition de l'est, 31 mai 2005, p. A.4.
- 14 Jane Croft, «HSBC apologizes for loss of customer data», *Financial Times*, Londres, R.-U., 8 avril 2008, p. 4.
- 15 *Ibid.*
- 16 «Alcatel-Lucent unable to locate disk containing personal employee information», *Telecomworldwire*, Coventry, 18 mai 2007, p. 1.
- 17 Nikki Swartz, «Losses highlight need for physical data security», *Information Management Journal*, Lenexa, vol. 41, n° 4 (juillet-août 2007), p. 17.
- 18 Darren Charters, «Addressing privacy breaches», *CMA Management*, Hamilton, vol. 81, n° 9 (février 2008), p. 34.
- 19 «BMO computer hard drives with sensitive info were on EBay auction site», *La Presse canadienne*, 15 septembre 2003.
- 20 «Texas AG accuses rehab center of dumping sensitive customer info», *Associated Press*, 10 janvier 2008. Voir www.kxan.com/global/story.asp?s=7606095 [consulté le 4 août 2008].
- 21 *Ibid.*
- 22 Shane W. Robinson, «Corporate espionage 201», *Information Security Reading Room*, SANS Institute, 2007 [consulté le 31 juillet 2008].
- 23 Richard B. Elsberry, «The spying game: How safe are your secrets?», *Office Systems*, Mt. Airy, vol. 16, n° 9 (septembre 1999), p. 42 à 46.
- 24 *Ibid.*
- 25 *Ibid.*

- 26 Birgitta Forsberg, «The spies in the next cube», *The San Francisco Chronicle*, 25 avril 2005. Voir <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/25/BUGGLCDPUJ1.DTL> [consulté le 4 août 2008].
- 27 Andy Dornan, «It's audit time — Do you know where your private data is?», *IT Architect*, Manhasset, vol. 20, n° 9 (septembre 2005), p. 35 à 41.
- 28 *Ibid.*
- 29 Raymond J. Elson et Rey LeClerc, «Customer information: Protecting the organization's most critical asset from misappropriation and identity theft», *Journal of Information Privacy & Security*, Marietta, vol. 2, n° 1 (2006), p. 3.
- 30 Kenyon Wallace, «Passport applicant finds massive privacy breach», *The Globe and Mail*, 4 décembre 2007, p. A1.
- 31 Christopher Conkey et Ann Carrns, «ChoicePoint to pay \$15 Million to settle consumer-privacy case», *Wall Street Journal*, New York (N.Y.), édition de l'est, 27 janvier 2006, p. A.3.
- 32 *Ibid.*
- 33 Ben Murray, «E-mail "source of risk" to companies», *Strategic Communication Management*, Chicago, vol. 11, n° 5 (août-septembre 2007), p. 9.
- 34 *Ibid.*
- 35 John Ginovsky, «An emerging corporate threat: Instant Messaging», *ABA Bankers News*, Washington, vol. 14, n° 14 (4 juillet 2006), p. 8.

