



ÉTUDE TECHNIQUE

Gestion de la sécurité de l'information par la haute direction



...la force de l'engagement^{MC}

TABLE DES MATIÈRES

POURQUOI LA SÉCURITÉ DOIT ÊTRE GÉRÉE PAR LA HAUTE DIRECTION?	3
MESURES REQUISES DE LA PART DE LA HAUTE DIRECTION POUR ASSURER LA SÉCURITÉ	4
- DÉFINIR LES RÔLES ET LES RESPONSABILITÉS	4
- DÉVELOPPER DES POLITIQUES ET DES PROCÉDURES	5
- SENSIBILISER ET FACILITER LA COORDINATION	6
- ASSURER LA SURVEILLANCE ET LA FORMATION	6
CONCLUSION	7
À PROPOS DE CGI	7

POURQUOI LA SÉCURITÉ DOIT ÊTRE GÉRÉE PAR LA HAUTE DIRECTION?

Dans le monde contemporain des affaires, où les technologies jouent un rôle plus important que jamais, il est essentiel pour les entreprises de protéger leurs actifs, leurs systèmes et leurs réseaux d'information. La révolution technologique leur a permis de réaliser d'immenses bénéfices, mais les a aussi exposées à de nouveaux risques et de nouveaux domaines de responsabilité. La transition des systèmes informatiques centralisés aux environnements répartis a rendu les actifs en technologies de l'information (TI) et les données commerciales plus vulnérables aux attaques internes et externes. Le nombre croissant de personnes détenant des connaissances poussées en informatique et la grande disponibilité d'outils de piratage ont également contribué à accroître les risques d'attaques. Les virus informatiques, le vandalisme de sites Web, l'utilisation illicite de renseignements confidentiels, les vols et les autres formes de violations de la sécurité informatique sont monnaie courante et se soldent par des pertes financières, des poursuites judiciaires, des dommages à la réputation des entreprises et l'effritement de la confiance des actionnaires.

Les dernières années ont été marquées par une hausse sans précédent de la criminalité informatique et des activités connexes. Les résultats de l'édition 2009 du sondage sur la criminalité et la sécurité informatiques (Computer Crime and Security Survey), réalisé par le Computer Security Institute (gocsi.com), montrent que cette forme de criminalité est plus répandue que jamais. Des 443 répondants qui ont participé au sondage, le tiers d'entre eux ont indiqué que leur entreprise a été frauduleusement identifiée comme expéditeur d'un courriel hameçon et ont rapporté une hausse importante du taux d'incidents liés au reniflage de mots de passe, à la fraude financière et aux infections dues à des programmes malveillants. Lorsqu'interrogés à propos des solutions de sécurité qui figuraient en tête de leurs listes, plusieurs répondants ont nommé des outils qui leur permettraient d'accroître leur visibilité : une gestion améliorée de l'ouverture de session, la gestion des événements et de l'information liée à la sécurité, la visualisation des données de sécurité, des tableaux de bords de sécurité, et ainsi de suite.

L'exposition à des risques de violation de la sécurité de l'information et aux dommages pouvant en résulter a entraîné l'adoption ou la préparation de nouvelles lois et réglementations aux niveaux national et international, qui rendent les entreprises et les membres de leur haute direction responsables des violations de la sécurité et de la confidentialité de l'information. Certaines de ces réglementations formulent des exigences très strictes et vérifiables que les entreprises sont dans l'obligation de satisfaire dont la Loi Sarbanes-Oxley (SOX), la norme de sécurité des données du Payment Card Industry (PCI DSS) et la Loi sur la protection des renseignements personnels et les documents électroniques (HIPAA aux États-Unis/LPRPDE au Canada). Les experts juridiques anticipent également une vague de poursuites civiles engagées par des parties contre des entreprises leur ayant causé des torts découlant de mécanismes de sécurité inadéquats.

Pour toutes ces raisons, les entreprises accordent maintenant une priorité plus élevée à la sécurité de l'information. Les membres de la haute direction des organisations ne perçoivent plus les enjeux relatifs à la sécurité comme des questions touchant exclusivement les TI, mais comme une composante vitale à la survie des entreprises. Celles-ci font appel de plus en plus fréquemment à des experts externes pour les aider à accroître le niveau de sécurité de leurs systèmes d'information, entraînant du même coup une croissance rapide du marché des services de sécurité. « La sécurité accapare une part plus importante du budget alloué aux TI, souligne Jonathan Penn, analyste de Forrester, dans une étude effectuée par l'entreprise en 2009. Les entreprises ont consacré 11,7 % de leur budget d'entreprise en TI à la sécurité en 2008, contrairement à 7,2 % en 2007, et prévoient augmenter leur budget de sécurité en TI à 12,6 % en 2009 ». Les nouvelles initiatives représenteront aussi un pourcentage plus élevé des affectations budgétaires dédiées à la sécurité cette année, passant de 17,7 % en 2008 à 18,5 % en 2009, précise le rapport. Des augmentations similaires sont prévues dans des entreprises de plus petite taille, indique Penn dans le rapport des PME. « Les petites et moyennes entreprises ont consacré 9,1 % de leur budget de fonctionnement des TI à la sécurité des TI en 2008 - une diminution par rapport aux 9,4 % accordés en 2007 – mais ces entreprises prévoient rehausser les budgets affectés à la sécurité des TI à 10,1 % en 2009, indique le rapport. Des affectations budgétaires pour les nouvelles initiatives reflètent cette tendance, avec une part du budget prévu pour la sécurité qui passe de 14,9 % en 2008 à 15,9 % en 2009. Peu de coupes budgétaires sont prévues ici. »

MESURES REQUISES DE LA PART DE LA HAUTE DIRECTION POUR ASSURER LA SÉCURITÉ

En mettant l'accent sur la sécurité, les conseils d'administration des entreprises ont entériné la mise sur pied d'infrastructures de sécurité de l'information au sein des organisations qu'ils dirigent. C'est aux membres de la haute direction, et non aux services des TI, que les administrateurs confient le mandat de développer et de mettre en œuvre ces infrastructures pour protéger les entreprises contre les violations de la sécurité et les risques de poursuites judiciaires. Ce domaine est entièrement nouveau pour plusieurs hauts dirigeants et le manque de directives adéquates peut les mener au désastre.

Définir les rôles et les responsabilités

Pour être couronné de succès, un programme de gestion des infrastructures doit être clairement défini. La mise sur pied et la maintenance d'une infrastructure de sécurité n'échappent pas à cette règle. Dans la plupart des cas, l'un des plus importants défis consiste à déterminer qui doit être responsable de la gestion des questions de sécurité. Idéalement, la responsabilité globale de ces enjeux doit être confiée à un chef de la sécurité. Si cette fonction n'est pas confiée à un titulaire spécifique, elle doit à tout le moins être intégrée aux responsabilités du chef des technologies ou du chef de l'information.

La combinaison de ces rôles ne doit être envisagée que dans les cas où une personne peut raisonnablement assumer l'ensemble de ces tâches, sans conflits d'intérêts. Pour le conseil d'administration, le chef de la sécurité est principalement responsable de la gestion et de la réduction efficaces des risques. La combinaison du rôle de chef de l'information à d'autres fonctions peut entraîner des conflits d'intérêts qui mettent en péril la réalisation de la mission de sécurité. Dans les cas où les responsabilités du chef de la sécurité sont intégrées à celles d'un autre poste, l'entreprise doit mettre sur pied des mécanismes de contrôle et assurer une surveillance adéquate pour éviter l'émergence de conflits d'intérêts.

L'embauche de professionnels de la sécurité compétents et expérimentés est un autre élément essentiel au succès d'une initiative en sécurité. La sécurisation de l'ensemble d'une organisation est un processus dynamique complexe exigeant une expertise poussée. Plusieurs programmes de certification professionnelle en sécurité reconnus à l'échelle internationale sont offerts aux spécialistes du domaine et attestent l'acquisition des compétences nécessaires en sécurité de l'information. Les plus importants sont présentés dans le tableau ci-dessous.

Organismes de certification		
Organisme	Certification	Commentaire
ISC ²	CISSP	http://www.isc2.org
ISACA	CISA CISM	http://www.isaca.org
SANS	GIAC	http://www.sans.org , http://www.giac.org
DRI	GIAC	http://www.dri.ca

Développer des politiques et des procédures

Ce n'est qu'après avoir défini clairement les rôles et les responsabilités qu'une organisation peut s'attaquer au défi consistant à mettre sur pied et à gérer une infrastructure de sécurité de l'information. L'organisation doit développer une compréhension approfondie du concept de sécurité de l'information en tant que discipline en expansion et en évolution constantes, et doit intégrer ce concept à son mode de fonctionnement pour garantir l'efficacité maximale des mesures de sécurité. De plus, toutes les composantes de l'infrastructure de sécurité doivent être entièrement intégrées les unes aux autres, ainsi qu'aux activités quotidiennes de l'organisation.

Les politiques et les procédures de l'organisation constituent la clé de l'intégration. L'adoption de politiques et de procédures appropriées témoigne sans équivoque de l'engagement de la haute direction envers l'application d'un ensemble de normes et envers les méthodologies permettant de les mettre en œuvre. Combinées à des règles claires de répartition des responsabilités, ces politiques et procédures forment une base solide sur laquelle les mesures de sécurité peuvent être établies et mises en application.

Le Centre d'information ISO/CEI, géré conjointement par l'Organisation internationale de normalisation (ISO) et la Commission Électrotechnique Internationale (CEI), constitue l'une des meilleures ressources pour les membres de la haute direction d'une entreprise à la recherche de repères et de directives pour le développement de politiques et de procédures. Ensemble, ces organismes ont mis au point la norme ISO/IEC 27000, un ensemble complet des meilleures pratiques en matière de gestion de la sécurité de l'information. Adaptée de règlements antérieurs dont les normes British Standard 7799 et ISO 17799, la norme 27000 est l'ensemble de règles de sécurité le plus largement reconnu à l'échelle mondiale à l'heure actuelle. Elle divise la fonction globale de sécurité de l'information en plusieurs niveaux et désigne les secteurs pour lesquels l'adoption de politiques et de procédures est essentielle. Des renseignements supplémentaires sur ISO/IEC 27000:2009 (exposé général) et sur les normes clés ISO/IEC 27001:2005 (Exigences des systèmes de management de la sécurité de l'information) et ISO/IEC 27002:2005 (Code de bonne pratique pour le management de la sécurité de l'information) sont disponibles sur le site suivant : <http://www.iso.org>.

Sensibiliser et faciliter la coordination

Une fois les politiques et procédures documentées et approuvées par les membres du conseil d'administration et de la haute direction, il est nécessaire de les faire connaître à l'ensemble de l'organisation. Les utilisateurs doivent comprendre comment ces politiques et procédures les affectent et être conscients des attentes de la direction en ce qui a trait à leur application.

L'une des plus importantes responsabilités du chef de la sécurité consiste à assurer la liaison avec les divers services de l'organisation afin de promouvoir la connaissance des mesures de sécurité à l'échelle des services et d'en coordonner l'application. Plusieurs services, dont les ressources humaines, la gestion des installations, les TI et la vérification interne, jouent un rôle clé à ce chapitre. Ces services s'en remettent au chef de la sécurité pour veiller à ce qu'ils collaborent le plus efficacement possible les uns avec les autres dans le but de traiter les questions relatives à la sécurité.

Dans le cadre de son rôle de réduction des risques, le chef de la sécurité doit aussi harmoniser étroitement les mesures de sécurité de l'information aux directives d'entreprise, y compris les lignes directrices concernant la continuité des activités commerciales et les plans antisinistres. Ceci amène généralement le chef de la sécurité à participer à la gestion et à la coordination des plans de continuité des activités commerciales et de reprise après sinistre.

Assurer la surveillance et la formation

Une gestion méthodique de la sécurité exige aussi une surveillance continue et la formation du personnel en ce qui a trait aux règles de sécurité de l'information. Les erreurs et les omissions représentent encore la principale cause de violation des règles de sécurité. La surveillance de leur application assure la conformité aux politiques, aux procédures et aux lois en matière de sécurité de l'information.

Elle favorise aussi la responsabilisation du personnel et facilite les activités de vérification. De plus, la surveillance fournit une base assurant la mise en application des politiques et des procédures, car elle identifie le moment, le lieu et la façon dont se produisent les violations à la sécurité, de même que les individus qui en sont les auteurs.

Rafraîchie sur une base régulière, la formation visant la sensibilisation aux mesures de sécurité permet de réaliser deux objectifs essentiels. En premier lieu, elle transmet des renseignements essentiels aux membres de l'organisation qui en ont le plus besoin, soit le personnel général de l'entreprise. Deuxièmement, elle constitue un rappel constant de l'importance de la sécurité de l'information dans les activités quotidiennes.

En principe, la supervision globale de la surveillance et de la mise en application des règles de sécurité devrait relever du chef de l'information. En pratique, ce cumul de tâches pourrait être une source de conflits d'intérêts. Il en va de même pour le personnel du service des TI. Les membres du service des TI peuvent être mandatés pour la mise sur pied des outils de surveillance et d'application des mesures de sécurité. Par principe, ils ne doivent cependant pas être responsables de l'examen des données de conformité aux politiques et procédures de sécurité, afin d'assurer une séparation des tâches en guise de moyen supplémentaire de contrôle.

CONCLUSION

La gestion de la sécurité de l'information est une entreprise très vaste, qui englobe l'ensemble des divisions et des services d'une organisation. Toute entreprise dont les activités reposent sur l'utilisation de technologies a le devoir de mettre en œuvre des mesures efficaces de protection dans le cadre d'un programme global de gestion de la sécurité de l'information. La responsabilité de l'encadrement du développement des initiatives de sécurité incombe à la haute direction de chaque organisation. Afin de minimiser les violations de la sécurité et d'éviter les poursuites judiciaires, les membres de la haute direction doivent prendre les mesures nécessaires pour développer une infrastructure efficace de sécurité de l'information. Les hauts dirigeants doivent prendre le temps nécessaire pour bien comprendre les enjeux relatifs à la sécurité affectant leur organisation, et veiller au développement de politiques et de procédures assurant le niveau de sécurité le plus élevé possible, afin de permettre à l'organisation de réaliser ses objectifs.

À PROPOS DE CGI

La raison d'être de CGI est de satisfaire ses clients et de contribuer à leur croissance et à leur succès. Depuis plus de 30 ans, nous appuyons nos clients en leur rendant des services de grande qualité et en les aidant à relever les défis auxquels ils font face.

Figurant parmi les chefs de file du secteur des services en TI et en gestion des processus d'affaires, CGI regroupe 26 000 professionnels répartis dans plus de 100 bureaux dans le monde. Nous fournissons à nos clients la combinaison de valeur et de savoir-faire qui répond le mieux à leurs besoins en alliant judicieusement les partenariats à l'échelle locale et des options de prestation de services à l'échelle mondiale.

Pour nous, réussir signifie aider nos clients à améliorer leur position concurrentielle et à se distinguer par leurs résultats.