

Sécurisation de l'information vitale : dossier commercial en faveur de la gestion déléguée de la sécurité



_la force de l'engagement



Les technologies de l'information appliquées aux solutions d'affaires

TABLE DES MATIÈRES

INTRODUCTION	3
FACTEURS INFLUENÇANT LA SÉCURITÉ DE L'INFORMATION	3
AVANTAGES DE L'APPROCHE DE GESTION DÉLÉGUÉE DE LA SÉCURITÉ	4
CHOIX D'UN FOURNISSEUR GDS	6
CONCLUSION	7
À PROPOS DE CGI	7

Introduction

L'information et les technologies permettant d'y accéder, de l'utiliser, de la stocker et de la transférer sont devenues les principaux facteurs de création de richesse et de valeur dans l'économie numérique mondiale contemporaine. Les entreprises de tous les secteurs d'activité traitent chaque jour des volumes colossaux de données qui doivent être protégées contre les accès illicites, le vandalisme, la destruction et le vol. Dans le même ordre d'idées, les systèmes et réseaux informatiques complexes utilisés pour le traitement de ces données doivent également faire l'objet d'une protection adéquate. Une protection insuffisante de ces actifs en information peut entraîner des conséquences désastreuses, y compris d'importantes pertes financières et des poursuites judiciaires, pour les entreprises touchées.

Au cours des dernières années, la sécurité de l'information a acquis une importance significative, en raison surtout de la prolifération des délits informatiques et de l'adoption de lois concernant la sécurité de l'information par plusieurs pays à l'échelle mondiale. Autrefois une fonction reléguée au service des TI, la sécurité de l'information est maintenant un sujet fréquemment discuté par les conseils d'administration de nombreuses entreprises, qui la perçoivent comme une fonction méritant une attention sérieuse et des investissements en conséquence.

Avec l'augmentation du coût et de la complexité des technologies de l'information, les entreprises éprouvent toutefois des difficultés croissantes à gérer à l'interne les tâches liées à la sécurité de l'information. C'est pourquoi nombre d'entreprises font appel à des fournisseurs de services de gestion déléguée de la sécurité (GDS) pour obtenir de l'aide. Cette étude technique présente les avantages de la GDS et examine les facteurs dont les entreprises doivent tenir compte lors de la sélection d'un fournisseur de services de gestion déléguée de la sécurité.

Facteurs influençant la sécurité de l'information

Délits informatiques

Confrontées aux risques et aux coûts croissants liés aux attaques informatiques, les entreprises n'ont d'autre choix que d'adopter une attitude plus énergique en matière de sécurité de l'information. Les délits informatiques connaissent une croissance vertigineuse, et visent aussi bien les individus et les gouvernements que les entreprises à l'échelle mondiale. L'avènement du réseau Internet a révolutionné les communications et le commerce, mais sa nature ouverte et universelle a rendu les systèmes informatiques et les réseaux de télécommunications plus vulnérables aux attaques internes et externes. La portée mondiale d'Internet permet à un seul criminel informatique de faire des ravages partout dans le monde à l'aide d'un banal ordinateur personnel relié à un modem.

Les reportages sur les dommages colossaux provoqués par les virus les plus récents et les derniers actes de piraterie informatique sont devenus monnaie courante dans tous les médias. Alors que le niveau d'adoption des ordinateurs et des nouvelles technologies augmente constamment dans l'ensemble de la société, le nombre de criminels informatiques et le type d'attaques qu'ils mettent au point continuent de se multiplier rapidement.

Bien qu'il soit difficile de chiffrer avec précision le coût des délits informatiques pour l'économie mondiale, on estime qu'il atteint plusieurs milliards par année. Les délits informatiques engendrent des frais directs et indirects pour les entreprises. Les coûts directs comprennent les sommes consacrées à l'acquisition de systèmes et de logiciels de sécurité, à l'embauche d'experts en sécurité et aux pertes de productivité encourues à la suite de violations de la sécurité. Les coûts indirects des délits informatiques comprennent les ventes perdues, les dommages à la réputation des entreprises, la dégradation des relations avec la clientèle, la perte de la confiance des actionnaires et les frais liés aux poursuites judiciaires. L'évaluation des coûts indirects des délits informatiques est un exercice complexe, mais certains chercheurs estiment que leur valeur excède largement celle des coûts directs de ce type de délits.

Législation concernant la sécurité

Les menaces présentées par la violation de la sécurité et de la confidentialité dans le cyberspace ont incité de nombreux gouvernements à adopter des lois et des règlements relatifs à la sécurité informatique partout dans le monde. La conformité à ces exigences représente toutefois un défi colossal pour les entreprises, compte tenu de la multiplication et de la complexité des lois et règlements. Pire encore, les risques associés à la non-conformité, y compris les amendes, les pénalités et la publicité négative dans les médias, peuvent s'avérer très coûteux.

Aux États-Unis, les entreprises sont assujetties à une foule de lois et de règlements concernant la sécurité de l'information. Parmi les lois sur la sécurité adoptées récemment, mentionnons :

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** – Cette loi exige que les fournisseurs de soins de santé prennent des mesures pour protéger la confidentialité des renseignements sur la santé transmis ou sauvegardés sous forme électronique.
- **Gramm-Leach-Bliley Act of 1999 (GLBA)** – Cette loi traite de la sécurité des dossiers des clients dans les institutions financières.
- **Sarbanes-Oxley Act of 2002** – Cette loi impose aux sociétés ouvertes des exigences de contrôle interne et de divulgation des résultats financiers
- **USA Patriot Act of 2001, et la Homeland Security Act of 2002** – Ces lois, adoptées à la suite des événements du 11 septembre 2001, établissent des exigences en matière de sécurité de l'information dans le but de lutter contre les crimes terroristes.

Plusieurs autres pays ont adopté de semblables lois et règlements sur la sécurité, que les entreprises doivent connaître et auxquels elles doivent se conformer, s'il y a lieu. Au Canada, par exemple, la Loi sur la protection des renseignements personnels et les documents électroniques protège la confidentialité des renseignements personnels utilisés à des fins commerciales. L'Union européenne a mis en œuvre de nombreuses directives touchant la confidentialité, y compris les Directives de protection des données de l'UE de 1998, qui exigent que tous les États membres appliquent une réglementation exhaustive pour la protection de la confidentialité des données personnelles.

Des normes de sécurité internationales ont été développées pour aider les organisations à rehausser leur niveau de sécurité et à se conformer aux obligations imposées par la loi. À l'heure actuelle, la norme de sécurité la plus reconnue dans le monde est la norme ISO 17799, qui découle de la norme britannique British Standard 7799. Mise au point par l'Organisation internationale de normalisation (ISO), la norme ISO 17799 propose un ensemble complet de pratiques en matière de sécurité pour guider les hauts dirigeants dans le développement de programmes de sécurité de l'information. Pour en savoir plus sur les normes ISO 17799 et BS 7799, visitez les sites Web <http://www.iso.org> ou <http://www.bsi-global.com>.

Avantages de l'approche de gestion déléguée de la sécurité

Les entreprises qui veulent accroître le niveau de sécurité de l'information au sein de leur organisation doivent accomplir une tâche ardue. Les menaces à la sécurité continuent de changer et de se multiplier en parallèle aux technologies créées pour les mettre en échec. La conception, la mise en œuvre et la gestion d'un programme de sécurité efficace constituent un projet vaste, complexe et coûteux pour la plupart des entreprises. Comme aucun programme de sécurité n'est sûr à 100 %, les entreprises les évaluent en fonction de leur efficacité à gérer les risques. Dans le but de limiter la portée de ces risques, les entreprises en partagent la responsabilité avec des fournisseurs de gestion déléguée de la sécurité (GDS) et profitent des nombreux avantages découlant de cette approche.

Coûts

Les entreprises qui optent pour la gestion déléguée de la sécurité profitent de nombreux avantages dont, au premier chef, une réduction considérable des frais d'exploitation. En général, il est moins coûteux de confier les fonctions de sécurité en impartition, plutôt que de maintenir à l'interne un groupe spécialisé à plein temps. Les fournisseurs GDS permettent à leurs clients de profiter d'économies d'échelle en répartissant le coût de leurs experts en sécurité, de leurs installations, du matériel et des logiciels sur plusieurs clients. De plus, les compétences, l'expérience et les technologies évoluées des fournisseurs GDS réduisent considérablement les risques d'attaques informatiques, et évitent aux entreprises les pertes qui y sont associées.

Expertise

En raison de la pénurie de professionnels spécialisés en sécurité de l'information, le recrutement et la rétention d'employés qualifiés représentent des défis de taille pour les entreprises. L'impartition permet aux entreprises de déléguer ces responsabilités aux fournisseurs GDS, tout en leur donnant la possibilité de bénéficier des compétences d'experts hautement qualifiés et expérimentés. Un fournisseur GDS peut recruter les professionnels les plus qualifiés du secteur – des spécialistes qui ont consacré l'ensemble de leur carrière à la sécurité de l'information – en leur offrant des programmes de formation, des défis professionnels et des occasions de progression professionnelle. Les entreprises bénéficient des services d'experts détenant des certifications professionnelles, un savoir-faire technologique poussé et une vaste expérience de traitement d'incidents touchant la sécurité, acquise au cours de centaines ou même de milliers d'interventions quotidiennes auprès d'une clientèle diversifiée.

Installations

Les installations offertes par les fournisseurs GDS constituent un autre argument de poids en faveur de l'impartition. De nombreux fournisseurs exploitent des centres opérationnels de sécurité (COS) spécialisés dans plusieurs emplacements. Ces centres, qui sont généralement à la fine pointe de la technologie, sont gérés par un personnel hautement qualifié et offrent les meilleures solutions matérielles et logicielles de leur catégorie, conçues pour assurer la sécurité des clients.

Rendement des services

Les entreprises bénéficient d'un niveau de rendement plus élevé en confiant leurs fonctions de sécurité à un fournisseur GDS. À partir de leurs centres opérationnels de sécurité, les fournisseurs GDS peuvent offrir des fonctions de gestion, de surveillance et de soutien 24 heures par jour, sept jours par semaine. En comparaison, les employés du groupe de sécurité informatique interne d'une entreprise peuvent n'être disponibles que durant les heures normales de bureau. Les procédures d'exploitation des fournisseurs GDS garantissent une disponibilité ininterrompue des services, et des réactions rapides en cas d'incident. De plus, l'application des meilleures pratiques et de méthodologies exclusives leur permet de déterminer la pertinence des menaces et d'éliminer les pertes de temps associées aux fausses alarmes. Les fournisseurs GDS sont également imputables de la qualité de leurs services. Les niveaux de service sont garantis afin de minimiser les risques encourus par les clients.

Conformité

La conformité avec la multitude de lois et de règlements sur la sécurité aujourd'hui dans la plupart des pays constitue une tâche colossale pour les entreprises. Non seulement les responsables de la sécurité des entreprises doivent-ils comprendre dans le moindre détail ces exigences légales complexes, mais ils doivent aussi élaborer des solutions grâce auxquelles les programmes de sécurité de l'entreprise pourront s'y conformer. En faisant appel à des fournisseurs de services de gestion déléguée de la sécurité, les entreprises

accèdent directement à une expertise et à des solutions de conformité. Les fournisseurs permettent à leurs clients de profiter de leur connaissance approfondie des exigences réglementaires et des normes de l'industrie, ainsi que de leur expérience en développement et en mise en œuvre des meilleures pratiques de sécurité. Ils fournissent aussi des services de vérification en continu afin de s'assurer que les installations des clients demeurent conformes aux exigences.

Choix d'un fournisseur GDS

Le choix d'un fournisseur de gestion déléguée de la sécurité exige une planification rigoureuse et une réflexion approfondie. Le marché des services GDS regorge de fournisseurs dont les services, les compétences et l'expérience varient considérablement. Plusieurs fournisseurs n'offrent pas les services et les solutions dont votre entreprise a besoin, ou n'offrent que des produits et des services génériques. Précisez vos exigences dès le début des négociations, et demandez aux fournisseurs potentiels de vous démontrer clairement leur capacité de répondre à ces exigences. D'autres critères de sélection doivent être pris en considération, notamment :

- **Stabilité financière** – Le fournisseur présente-t-il un bilan solide? Possède-t-il un historique de rendement financier élevé et une clientèle diversifiée?
- **Services en sécurité** – Le fournisseur offre-t-il une vaste gamme de services en sécurité pour répondre à vos exigences de bout en bout? Est-il disposé à regrouper ses services en forfaits correspondant spécifiquement à vos besoins d'affaires? L'ampleur de ses services peut-elle être modulée pour s'adapter à la croissance future de votre entreprise?
- **Expertise** – Combien d'experts en sécurité le fournisseur compte-t-il au sein de son personnel? Le fournisseur offre-t-il des programmes de formation? Ses employés détiennent-ils des certifications professionnelles? Combien d'années d'expérience les experts en sécurité du fournisseur possèdent-ils en moyenne?
- **Centres opérationnels de sécurité (COS)** – Combien de COS le fournisseur exploite-t-il, et où sont-ils situés? Quels types de technologies y sont mises en œuvre? Les procédures d'exploitation des centres sont-elles adéquatement documentées? Quelles méthodologies de sécurité y applique-t-on? À quelle fréquence les systèmes des COS sont-ils vérifiés, et par qui?
- **Normes de l'industrie et d'assurance de la qualité** – Le fournisseur respecte-t-il les normes de sécurité internationales et nationales reconnues dans l'industrie? Quelles normes d'assurance de la qualité applique-t-il? Le fournisseur est-il membre d'organismes de normalisation? Si oui, desquels?
- **Soutien aux clients** – Combien de clients le fournisseur soutient-il à l'heure actuelle? Combien d'incidents liés à la sécurité traite-t-il chaque jour? Le fournisseur peut-il fournir des exemples d'incidents récents, et expliquer comment il les a résolus? Le fournisseur est-il en mesure de présenter des références provenant de clients actuels et antérieurs?
- **Ententes sur les niveaux de service** – Le fournisseur offre-t-il des ententes sur les niveaux de service clairement définies? Ces ententes comportent-elles une souplesse inhérente? Des pénalités sont-elles spécifiées pour les manquements à la conformité? Les ententes comprennent-elles des clauses de confidentialité?

En choisissant un fournisseur, une entreprise doit s'efforcer de développer une relation de travail satisfaisante fondée sur la confiance et le respect mutuels. Ce type de relations ne peut s'épanouir que dans un climat ouvert favorisant des communications efficaces. Certaines entreprises tendent à confier entièrement les questions de sécurité à leur fournisseur SGS, et adoptent l'attitude « loin des yeux, loin du cœur ». Une approche plus responsable consiste à affecter un ou plusieurs employés au traitement des questions de sécurité les plus urgentes et à la supervision de la relation d'impartition, pour s'assurer que le fournisseur minimise efficacement les risques et s'acquitte de ses obligations contractuelles.

Conclusion

Un programme de sécurité « convenable » n'offre pas une protection suffisante dans l'environnement imprévisible avec lequel les entreprises doivent composer de nos jours. La mise en œuvre d'un programme de sécurité médiocre peut non seulement entraîner des pertes importantes, mais aussi l'échec de l'entreprise. La complexité croissante des questions de sécurité incite un nombre de plus en plus important d'entreprises à examiner la possibilité de confier ces aspects en impartition à un fournisseur de services de gestion déléguée de la sécurité. Les entreprises peuvent ainsi profiter d'une foule d'avantages en confiant la résolution des questions de sécurité à des experts, afin de se concentrer sur leurs activités de base. CGI compte le plus important groupe-conseil en sécurité au Canada et est à l'avant-garde du secteur de la gestion déléguée de la sécurité. À partir de ses centres d'expertise en sécurité, CGI offre une gamme complète de services conçus pour combler les besoins de sécurité de bout en bout de ses clients. Pour en savoir plus sur les offres GDS de CGI, visitez le site Web www.cgi.com.

À propos de CGI

Depuis 1976, CGI aide des clients provenant d'un vaste éventail de secteurs économiques à tabler sur les technologies de l'information pour maximiser leur performance et la valeur ajoutée qu'ils produisent. Nous offrons également une gamme complète de services d'impartition des processus d'affaires nous permettant de gérer et d'améliorer les processus d'affaires quotidiens de nos clients afin qu'ils puissent se concentrer sur leurs décisions stratégiques. Nous offrons des services de consultation, d'intégration de systèmes et d'impartition répondant à l'ensemble des besoins technologiques et d'affaires de nos clients. CGI aborde chaque mandat avec un même objectif en tête – contribuer à la croissance et au succès de ses clients. Elle fournit des services à des clients dans le monde entier, à partir de ses bureaux du Canada, des États-Unis et d'Europe, et également de ses centres d'excellence en Inde et au Canada.

Pour explorer ces aspects et découvrir comment nous pouvons vous aider, communiquez avec votre directeur de compte CGI ou visitez la page www.cgi.com/web/fr/siege_social.htm pour connaître l'emplacement des bureaux de CGI les plus près des vôtres. D'autres renseignements sont affichés sur le site www.cgi.com.

.