SSi-Conseil
Pilotez la sécurité de vos informations

SSi-Conseil est certifié
Lead Auditor ISO 27001

Janvier 2007

Pilotez la sécurité de vos informations

"parce que la sécurité n'est pas un produit, c'est un processus"

Votre système d'information est-il sécurisé ? A quand remonte votre dernier audit sécurité ?

- Firewalls, anti-virus, IDS, anti-spyware, anti-spam, DMZ, supervision, architecture sécurisée, solutions de cryptage, locaux sous surveillance,.... vous avez beaucoup investi et tout est paré pour combattre l'ennemi extérieur ?
- Loi sur la sécurité financière, CNIL, protection des données personnelles,... où en êtes-vous face à votre responsabilité juridique quant à la protection des données confidentielles ?

Avez-vous un Plan de Continuité d' Activité ? A quand remonte sa dernière évaluation ?

- Tempête ou inondations,
- Incendie complet ou partiel,
- Destruction d'un site critique
- Grèves, incident technique de grande ampleur,
- Attaque terroriste,
- Grippe aviaire...

Avez-vous fait diligence ?

75% des pertes occasionnées par des incidents de sécurité ont une cause interne à l'entreprise.

- Avez-vous fait le point de vos enjeux de sécurité et de vos vulnérabilités ?
- Avez-vous une politique de sécurité ?, une charte sécurité ?
- Votre personnel est-il bien sensibilisé ?
- Disposez-vous d'une gestion globale des identités ou de solutions d'identification unique de vos utilisateurs (SSO) ?
- Êtes vous conforme au plan réglementaire et juridique ?
- L'organisation de la sécurité de vos informations repose-t-elle sur un système de gestion compatible ISO 27001 ?

43% des entreprises frappées par un sinistre n'ont jamais ré-ouvert, 29% d'autres ont disparu dans les 3 ans suivants.

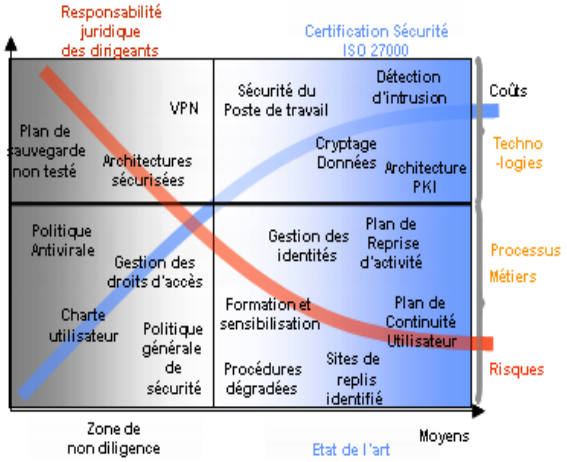
- Votre plan de sauvegarde est-il à la hauteur de vos enjeux ?
- Êtes vous prêts à faire face, même bien assuré ?
- A réagir dans des délais compatibles avec les besoins de vos utilisateurs?
- A mettre en place à la fois coordination, prise de décision et moyens opérationnels appropriés ?
- Avez-vous une solution de repli, pour vos personnels, pour vos moyens informatiques ?
- Combien de temps cela peut-il durer sans mettre en cause la survie de votre entreprise ?

De nombreuses entreprises ont pris conscience des enjeux liés à la valeur des informations qu'elles détiennent et à la nécessité de les protéger. Qu'elles soient liées à leurs activités commerciales (données clients par exemple) ou à leurs activités industrielles (secrets de fabrication par exemple), ces informations constituent un avantage concurrentiel fragile et convoité.

Pouvez-vous échanger en confiance avec un partenaire dont la sécurité du système d'information est douteuse ?

Parce que la sécurité n'est pas un produit mais un processus, SSi-Conseil aide ses clients à construire et piloter leur politique de sécurité.

Après avoir mis en évidence vos enjeux métiers critiques et vos vulnérabilités, la méthodologie SSi-Conseil, basée sur des outils d'analyse de risque éprouvés, permet de positionner la politique de sécurité de votre entreprise sur un optimum économique équilibrant risques acceptables et coûts de la sécurité. Une stratégie originale vous accompagne pour la réalisation et la certification de votre plan de reprise d'activité.



En évitant la zone de non diligence, pénalement risquée pour les dirigeants, SSi-Conseil vous aide à positionner la dynamique sécurité de votre entreprise dans une zone où l'application de l'état de l'art rends votre entreprise conforme ISO27001.
Comme vous l'avez fait pour la qualité avec ISO 9001, cette culture et cette certification deviennent alors un avantage concurrentiel et une valeur pour vos partenaires, clients et actionnaires.

"Si vous pensez que la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris ni aux problèmes ni à la technologie"

Cette citation quelque peu provocatrice de Bruce Schneier(*), résume la situation actuelle de la sécurité des informations et des systèmes d'information et inspire la vision de SSI-Conseil :

La sécurité n'est pas un produit, c'est un processus !

Alors que 80% des incidents de sécurité ont une origine organisationnelle et humaine interne, l'écart entre les investissements technologiques en sécurité (83%) et ceux liés à l'organisation et à la sensibilisation du personnel (16%)** est révélateur.

La Mission de SSI-Conseil est d'accompagner les dirigeants et responsables dans l'organisation, la mise en oeuvre opérationnelle et la valorisation de leur politique de sécurité de l'information : A partir d'une analyse rigoureuse des enjeux métier spécifique de votre entreprise, SSI-Conseil, vous apportera son assistance dans les domaines suivants :

- **Management de la sécurité,**
- **Gestion des risques,**
- **Schéma directeur de la Sécurité des Informations,**
- **Gestion de la Sécurité ,**
- **Gestion de crise, et plans de secours**
- **Communication et valorisation de la sécurité.**

Management de la sécurité :

SSI-Conseil vous aide à piloter la politique de sécurité de votre entreprise :

Notre démarche permet de vous assurer que votre stratégie éécurité des systèmes d'information est:

- en ligne avec vos objectifs business,
- en accord avec les contraintes juridiques et réglementaires,
- capable de sauvegarder l'image, la réputation et la survie de votre entreprise en cas de sinistre,
- Conforme à l'état de l'art et aux obligations réglementaires et juridiques.

Les domaines abordés comprennent notamment la politique sécurité, l'organisation sécurité, la définition des rôles et responsabilités : Qui préconise ?, Qui réalise ?, Qui contrôle ?, Comment la Direction Générale est informée des enjeux et des mesures prises par la fonction sécurité.

Notre valeur ajoutée :

l'optimisation économique et la démarche de certification de votre politique de sécurité,

Conformité du Système de Gestion de la Sécurité aux standards notamment ISO 27001 et ISO 17799,

Méthodologie Méhari™ et outil RISICARE™ pour la gestion des risques,

Méthodologie BCI pour des Plans de Continuité d'Activité (PCA) fiables et éprouvés.

SSi-Conseil est certifié Lead Auditor ISO27001 par le BSI.

Gestion des risques : Analyse des enjeux de vos métiers et évaluation des besoins de sécurité.

SSi-Conseil, sur la base d' une méthodologie éprouvée, s'adapte aux enjeux de vos métiers pour identifier et gérer les risques relatifs à la sécurité des systèmes d'information afin d'atteindre vos objectifs business sans risques ni coûts excessifs.

Les domaines abordés comprennent notamment le développement d'un processus d'analyse des enjeux et des vulnérabilités, l' analyse d'impacts, le traitement des risques, le choix des stratégies de sécurité et l 'élaboration de plan d'actions permettant de gérer et réduire ces risques.

Schéma directeur de la sécurité des informations :

Concevoir, développer et piloter un système de management de la sécurité de vos informations pour réussir la mise en œuvre des principes établis par la gestion des risques. Les domaines abordés comprennent notamment la conduite de projet, les cycles de développement applicatifs, l'architecture de sécurité, les plans de reprise d'activité en cas de sinistre.

Gestion de la Sécurité :

SSi-Conseil vous assiste dans la mise en œuvre les orientations contenues dans le schéma directeur de la sécurité. Les domaines abordés comprennent notamment les tableaux de bord, le budget sécurité, l'audit et contrôle, la formation et la sensibilisation des acteurs en relation avec l'entreprise : collaborateurs, fournisseurs, partenaires...

Gestion de crise :
Toutes les procédures de votre plan de continuité d'activité et leurs enchaînements disponibles sur une seule clé USB.

Votre Plan de Continuité d'Activité Clé-USB en main®

SSi-Conseil vous accompagne dans une démarche d'organisation et de préparation de vos plans de continuité d'activité. Vos équipes et vos utilisateurs seront en mesure de répondre efficacement à des incidents de sécurité ou à des situations de sinistres. Il leur sera possible de redémarrer leurs activités dans des délais compatibles avec vos impératifs de production.

Les domaines abordés comprennent notamment la mesure des risques, la gestion d'incidents, les plans de secours, le plan de continuité d' activités, le plan de retour à la situation normale, la communication de crise.

Communication et valorisation de la politique sécurité

Mettre en place une politique de communication dynamique tournée à la fois :

- Vers l'intérieur : c'est la mise en place d'une culture sécurité
  - pour dynamiser en permanence la contribution de tous les acteurs à une bonne compréhension des enjeux et des procédures de sécurité,
- Vers l'extérieur : c'est la valorisation de votre état de l'art en matière de sécurité
  - pour transmettre le message aux acteurs en relation avec l'entreprise, mais aussi transformer et valoriser la politique de sécurité en avantage concurrentiel.

(*)Bruce Schneier, est un expert technique renommé en sécurité:
Secrets et Mensonges traduit aux éditions Vuibert Informatique.
(**)Ernst and Young " la sécurité des systèmes d'information dans les entreprises françaises en 2003.