QUESTIONS ESSENTIELLES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION DANS L'ENTREPRISE

Quelles sont les étapes essentielles déterminant le succès de l'entreprise?

De quelles informations avons-nous besoin, aujourd'hui et dans le futur, pour garantir ces étapes?

Quels sont les risques significatifs pour les informations décisives?

Quels objectifs de sécurité voulons-nous atteindre pour les informations vitales de l'entreprise?

Quel est l'état actuel de la sécurité de l'information dans l'entreprise?

Quelles sont les mesures à prendre concernant la sécurité de l'information dans l'entreprise?

Fondation *InfoSurance*

Badenerstrasse 551
8048 Zurich
Téléphone 01 433 39 39
Télécopie 01 433 38 78
E-Mail: mail@infosurance.ch
http://www.infosurance.org

Fondation *InfoSurance*

Guide pour

SÉCURITÉ DE L'INFORMATION

pour les cadres d'une entreprise

AVANT-PROPOS

Sur le plan économique et au niveau de l'entreprise, l'information occupe désormais une place aussi importante que les facteurs de production classiques, tels le travail, le capital et le sol. Leur protection occasionne des frais importants, tant au niveau de la sécurité au travail, des garanties des risques à l'investissement, de la protection des infrastructures que sur le plan des assurances sociales.

En revanche, la protéction de l'information, cette nouvelle ressource vitale, n'est garantie que de manière partielle et peu coordonnée. Pourtant, l'information peut être aisément copiée, détournée ou modifiée.

A cause du progrès technologique, le secteur de la protection de l'information joue désormais un rôle décisif pour le succès d'une entreprise. Mais ce rôle reste largement sous-estimé. Par la présente brochure, la fondation InfoSurance souhaite apporter sa contribution à un travail de sensibilisation et introduire les principes fondamentaux de la sécurité de l'information dans les entreprises et dans les administrations.

La sécurité de l'information est du ressort de la direction stratégique. C'est pourquoi cette brochure s'adresse aux cadres qui doivent pouvoir agir rapidement. La perte, la manipulation ou le vol d'informations peuvent en effet affaiblir considérablement une entreprise et mettre à mal ses perspectives d'avenir.

http://www.infosurance.org

QU'EST-CE QUE LA SÉCURITÉ DE L'INFORMATION?

L'information est la mise en relation de données sous la forme de chiffres, de mots ou de faits en vue de les rendre interprétables. La mise en relation des informations crée le savoir, qui est, dans un premier temps, rattaché à un individu.

La sécurité de l'information comprend tous les efforts pour la protection de ces informations. La sécurité de l'information va donc bien au-delà de la sécurisation de données informatiques (comme l'enregistrement des données de vos clients sur disque). Elle implique également la garantie des activités à long terme de l'entreprise et la protection du savoir des collaborateurs. C'est pourquoi la sécurité de l'information est une question plus stratégique que technique. Cette brochure concerne ainsi toutes les données, informations et autres éléments constituant le savoir.

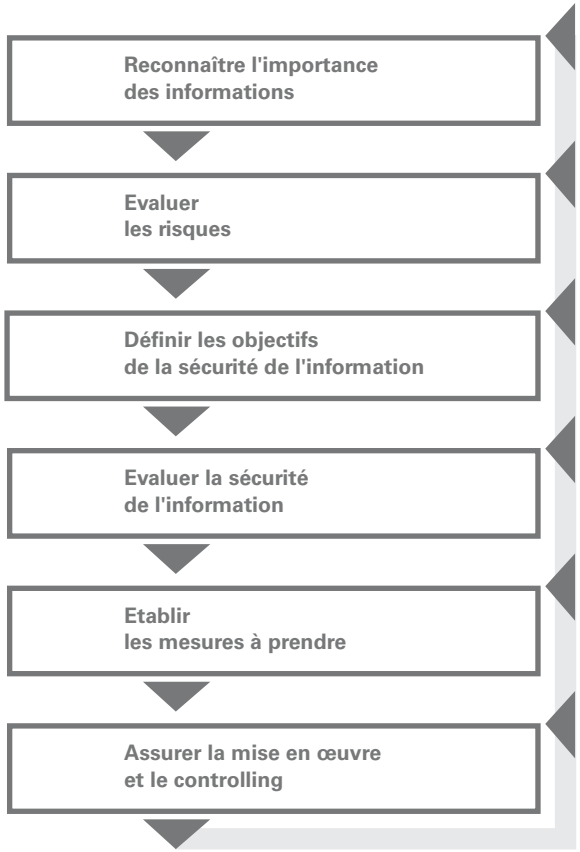
Le progrès des technologies de l'information rend la sécurité de l'information toujours plus essentielle. La sécurité des systèmes informatisés, accessibles par des réseaux, est une question hautement actuelle. Ces systèmes peuvent se retrouver paralysés par des attaques de hackers ou de virus informatiques. Mais n'oublions pas l'éventualité de pannes dans le secteur des transports publics (systèmes de signalisation), qui causent également des dommages économiques importants, ou l'infiltration de systèmes informatiques sensibles (criminalité électronique), qui suscite des préoccupations

croissantes. La menace d'espionnage, de sabotage ou de vol de données importantes exige enfin également des dispositifs de sécurité efficace.

Comme nous l'avons évoqué plus haut, la protection d'informations économiquement importantes dans une entreprise ne se limite pas aux données informatiques. Il faut aussi s'attacher à protéger le savoir, documenté ou non (know-how), dans le secteur recherche et développement ou dans les processus de production. Ici, les conditions préalables consistent en des structures organisationnelles adaptées et en une politique du personnel active et moderne. On néglige trop souvent cet aspect, pourtant essentiel à la protection des données. Des collaborateurs motivés et sensibilisés à la sécurité de l'information grâce à un entraînement adéquat, peuvent aussi améliorer la protection du savoir de l'entreprise ou de toute autre organisation.

Les organisations et les entreprises dépendent de plus en plus de données, d'informations et de savoir. Leur compétitivité, leur survie économique, le respect de dispositions légales et leur image dépendent directement de la disponibilité, la fiabilité et la confidentialité des informations.

LE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION



LA SÉCURITÉ DE L'INFORMATION – UNE RESPONSABILITÉ DU MANAGEMENT

Repérer et définir les informations critiques pour une entreprise, choisir les mesures adéquates pour leur sécurité: autant de responsabilités de management difficiles à déléguer. Ainsi, la sécurité de l'information fait partie des tâches importantes de chaque cadre, dans chaque entreprise ou chaque organisation.

Cette brochure répond aux questions les plus importantes. Ces réponses concernent un processus simplifié de gestion des risques, dont les étapes essentielles sont représentées dans le graphique ci-contre.

- Reconnaître l'importance des informations
- Evaluer les risques
- Définir les objectifs de la sécurité de l'information
- Evaluer la sécurité de l'information
- Etablir les mesures à prendre
- Assurer la mise en œuvre et le controlling

Le succès de l'entreprise dépend largement du savoir-faire, des compétences et des informations. Ces trois éléments doivent donc être protégés en conséquence. C'est pourquoi il faut régulièrement vérifier la sécurité des informations, de manière à pouvoir l'adapter en période de changements et la maintenir à un haut niveau.

RECONNAÎTRE L'IMPORTANCE DES INFORMATIONS

En principe, les cadres connaissent leur entreprise. Cependant, ils ne savent que trop rarement à quel point chaque étape du processus commercial dépend, directement ou indirectement, de l'information. Il est donc judicieux de représenter de manière schématique, les activités, processus et compétences spécifiques à chaque secteur de l'entreprise. Cet exercice permettra d'identifier les informations dont l'influence est critique pour la bonne marche de l'entreprise.

Questions essentielles

Quelles sont les étapes essentielles déterminant le succès de l'entreprise?

De quelles informations avons-nous besoin, aujourd'hui et dans le futur, pour garantir ces étapes?

Explication

On peut représenter de différentes manières (p. ex. diagramme de chaînes de production) les étapes critiques des opérations nécessaires à l'accomplissement des objectifs fixés par l'entreprise. La description doit être suffisamment détaillée pour permettre, ultérieurement, l'identification et le classement des informations nécessaires à chacune de ces étapes.

Si l'on veut prendre des mesures utiles et sensées pour la sécurité de l'information, il faut connaître les informations critiques pour l'entreprise.

Pour cela, il est nécessaire d'avoir une vue d'ensemble que l'on obtient en juxtaposant et en comparant les diverses représentations des étapes critiques.

- Comment décrire et classer sous forme de typologie les informations ainsi obtenues?
- Dans quelle mesure ces informations sont-elles accessibles par des réseaux?
- Qui se sert de ces informations?
- Quand, à quel rythme, combien de temps et à quelle fréquence ces informations sont-elles utilisées?
- Quelles conséquences peut-on prévoir pour l'entreprise et la chaîne de production si ces informations ne sont plus disponibles?
- Quelle est la part de ces informations à la création de valeur? Connaît-on les informations susceptibles d'influencer ou non les bilans?

Solutions

- Rassembler les informations nécessaires aux étapes décisives de production.
- Définir la part de ces informations qui s'avèrent déterminantes pour l'entreprise.
- Classer les informations selon qu'elles sont des facteurs de compétitivité ou des informations nécessaires sur le plan opérationnel.

ÉVALUER LES RISQUES

Cette étape doit permettre de déterminer les différents risques et leurs conséquences possibles pour l'entreprise.

Question essentielle

Quels sont les risques significatifs pour les informations décisives?

Explication

La mise en danger d'informations se présente sous différents aspects. Cela va des données confidentielles qui tombent en de mauvaises mains, aux données qui ne sont pas disponibles au lieu et au moment voulu, en passant par celles qui sont erronnées ou manipulées. Inadéquations techniques, lacunes organisationnelles, personnes mal intentionnées ou attaques violentes représentent encore d'autres facteurs de risques. Les causes et les responsables de ces risques peuvent se trouver aussi bien à l'intérieur qu'à l'extérieur de l'entreprise.

Cette étape permet d'identifier différents risques qui, lorsqu'ils surviennent, peuvent avoir diverses influences sur les informations dans l'entreprise. Ils peuvent ne toucher que des données isolées, ou alors détruire des informations vitales, ou encore affaiblir la compétitivité de l'entreprise. L'attention doit se focaliser sur les risques pouvant influencer les informations vitales pour l'entreprise, afin de cerner les mesures susceptibles de minimiser ces risques, voire de les supprimer. Il faut en

outre relever que l'engagement croissant des technologies de l'information crée une dépendance économique et technique énorme, elle-même source de nouveaux risques.

Solutions

- Etablir l'analyse des risques pour les différentes informations.
- Recourir à un avis externe pour cerner la palette de risques possibles pour les informations de l'entreprise.

DÉFINIR LES OBJECTIFS DE LA SÉCURITÉ DE L'INFORMATION

Cette étape consiste à fixer les objectifs en matière de protection des informations vitales pour l'entreprise.

Question essentielle

Quels objectifs de sécurité voulons-nous atteindre pour les informations vitales de notre entreprise?

Explication

D'une entreprise à l'autre, les informations peuvent avoir une importance très différente, ce qui conduit également à des exigences différentes en matière de sécurité. Certaines informations doivent être accessibles à tout moment et en tout lieu, d'autres sont significatives à long terme, d'autres enfin seulement à court terme. Dans la plupart des cas, l'information doit être intacte, fiable et rester inaccessible à des tiers non autorisés. Les secrets d'entreprise, les données comptables, les informations concernant les relations avec les clients ou les fournisseurs en sont des exemples typiques.

Outre les exigences de sécurité des informations, il faut aussi définir le niveau de protection nécessaire. Toutes les informations n'exigent pas forcément une protection absolue. La direction stratégique de l'entreprise détermine quelles informations doivent être protégées et à quel point. Cette tâche ne peut être que partiellement déléguée. De plus, elle suppose une prise de décision sur

les coûts humains et financiers de la protection, ainsi que sur le matériel mis à la disposition de cette sécurité.

Solutions

- Formuler des objectifs concrets pour la sécurité des informations vitales.
- Etablir un catalogue d'objectifs.

ÉVALUER LA SÉCURITÉ DE L'INFORMATION

Cette étape consiste à faire l'état des lieux en matière de sécurité de l'information dans l'entreprise. Elle permet de déceler les éventuelles lacunes ou les faiblesses du dispositif de protection.

Question essentielle

Quel est l'état actuel de la sécurité de l'information dans l'entreprise?

Explication

Pour définir l'état actuel de la sécurité de l'information dans l'entreprise ou dans une organisation et pour déceler les faiblesses, il est indispensable de répondre de manière concrète aux questions suivantes:

- La sécurité de l'information fait-elle partie intégrante de la politique de sécurité de l'entreprise considérée dans son ensemble?
- La sécurité de l'information dans l'entreprise est-elle coordonnée et les responsabilités sont-elles clairement définies?
- La direction stratégique de l'entreprise est-elle unanime quant à l'importance de la sécurité de l'information et quant aux moyens nécessaires?
- Les collaborateurs sont-ils sensibilisés et formés à la gestion d'informations sensibles?
- La sécurité de l'information lors de collaboration avec des tiers (partenaires, autres entreprises, four-

nisseurs, clients, autorités, etc.) est-elle définie?
- Les dispositions légales concernant la sécurité de l'information dans l'entreprise sont-elles connues et appliquées?
- Comment l'entreprise communique-t-elle, de manière interne ou externe quant à l'importance et la gestion des informations?
- Au sein d'une association professionnelle, ou alors avec d'autres entreprises, a-t-on déjà procédé à un partage d'expériences?
- Les informations sont elles toutes suffisamment protégées, en fonction des risques qu'elles représentent, tant sur les plans technique, physique et du management?

Solutions

- Etablir l'état des lieux de la sécurité de l'information.
- Analyser les lacunes et les faiblesses.

ÉTABLIR LES MESURES A PRENDRE

Cette étape vise à comparer les faiblesses repérées avec les objectifs de sécurité, afin de définir les mesures à prendre. En établissant ces mesures, il faut bien sûr veiller au rapport coût/opportunité, sans perdre de vue la stratégie de l'entreprise et son orientation future.

Question essentielle

Quelles sont les mesures à prendre concernant la sécurité de l'information dans l'entreprise?

Explication

Les lacunes importantes doivent être contrées avec des moyens adaptés. Les conditions cadre suivantes peuvent jouer un rôle déterminant:

- Stratégie de l'entreprise et directives internes sur la sécurité
- Réflexions sur le rapport coût/opportunité
- Ressources disponibles (en personnel, en finances et en temps)
- Exigences légales
- L'entreprise est-elle plutôt offensive ou défensive en matière de risques?

Questions principales:

- Les coûts des mesures sont-ils transparents et maîtrisés?
- Les mesures sont-elles soumises à un contrôle régulier?

- Comment prend-on en considération les évolutions futures?

Solutions

- Développer un catalogue de mesures.
- Evaluer l'efficacité des mesures.
- Fixer les priorités entre les mesures.

ASSURER LA MISE EN ŒUVRE ET LE CONTROLLING

Les étapes précédentes ont permis de connaître les mesures nécessaires. Il s'agit maintenant de les mettre en œuvre en fonction d'objectifs clairs et précis. Les étapes suivantes sont du ressort de la direction stratégique et contribuent de manière déterminante au succès des mesures:

- Formuler les mandats internes pour la concrétisation, la planification et la mise en œuvre des mesures, et les confier à des spécialistes.
- Informer et sensibiliser l'ensemble des collaborateurs sur le thème de la sécurité de l'information.

L'ensemble du processus peut être réalisé sous la forme de groupes de travail. Les cadres doivent constituer le noyau de ces groupes et assumer la tâche importante de les animer. Au besoin, ne pas hésiter à faire appel à des spécialistes internes pour répondre à des interrogations détaillées.

Les mesures sont vérifiées sur la base de leur efficacité. En outre, il faut régulièrement vérifier la sécurité de l'information, afin de pouvoir réagir rapidement aux changements.

Solutions

- Organiser des groupes de travail internes.
- Etablir le contact avec des forums d'entreprise ou des cercles expérimentés.

- Assurer le contrôle des mesures sur le plan de leur efficacité.
- Vérifier régulièrement l'état de la sécurité de l'information.

INFORMATIONS SUPPLÉMENTAIRES ET APERÇU BIBLIOGRAPHIQUE

Les informations et leur gestion font l'objet d'un flot impressionnant de documentation. Ci-après, la fondation InfoSurance vous donne une sélection de sources vous permettant d'approfondir vos connaissances sur le sujet:

- The Business Manager's Guide to Information Security, éd. Department of Trade and Industry, United Kindom, 1996.
- Guidelines for the Security of Information Systems, éd. Organization for Economic Cooperation and Development, 1992.
- Wissen managen. Wie Unternehmen ihre wertvollste Ressource optimal nutzen. Gilbert Probst, Steffen Straub, Kai Romhardt, Frankfurt a. M./Wiesbaden,1999.
- Code of Practice (CoP), éd. British Standards Institution, London, 1999.
- http://www.infosurance.org

NOTES

NOTES