Innovation & compétitivité
CCI RHÔNE-ALPES

Espace Innovation & Compétitivité

Intelligence économique

« Protéger son patrimoine matériel et immatériel »

Octobre 2013

Le **patrimoine matériel** est l'ensemble des constructions, meubles, objets d'utilisation quotidienne, outils et équipements.

Le **patrimoine immatériel** d'une entreprise est l'ensemble des informations et connaissances qu'elle a emmagasinées. Il regroupe à la fois les **informations formelles**, stockées sur des supports (qu'ils soient numériques ou papier) et les **informations informelles**, détenues par les membres de l'entreprise.

Il est donc nécessaire pour toute organisation de le protéger afin de prévenir les pertes, les fuites ou les vols.

Comment mettre en place une protection efficace dans l'entreprise ?

52% des grandes entreprises pensent que le manque d'attention et de vigilance de leurs employés constitue une menace sérieuse pour la sécurité de leurs données sensibles. *(Enquête Kaspersky, juin 2013)*

En interne / avec le personnel

Sensibiliser et former le personnel a la discretion et a la vigilance

- Dans les lieux publics et transports en communs (avions, trains, restaurants…), éviter de travailler sur des supports qui peuvent être lus par un tiers, ou s'équiper (filtre de confidentialité pour ordinateur portables). Avec des collègues, ne pas évoquer de sujets comportant des informations stratégiques (nouveaux projets, innovations, partenariats…).
- Au téléphone : Eviter de trop en dire (nouveaux projets, stratégie, parts de marché, etc.) avant d'être assuré de l'identité de l'interlocuteur, d'avoir décelé la finalité réelle de son appel et de la prise en compte de la confidentialité des échanges. Au besoin, demander l'envoi d'un écrit de confirmation (courrier ou fax avec en-tête de l'entreprise, mail d'entreprise).
- Alerter les collaborateurs sur l'utilisation possible à leur encontre de techniques d'interview intrusives.

Gerer la presence de stagiaires et personnels interimaires

- Vérifier le CV
- Ajouter au contrat des clauses de confidentialité si nécessaire
- Définir et contrôler les accès (zones de l'entreprise, réseau informatique, documents…)
- Veiller à contrôler la diffusion du rapport de stage

Anticiper le depart d'un salarie

- Prévoir une clause de non-concurrence, si besoin
- Gérer les dossiers stratégiques
- Prévoir la transmission des informations informelles du salarié : formation du ou des salariés qui prendront la suite.

Guides utiles :

Passeport de conseils aux voyageurs : http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

Veiller futé à l'international : http://www.cnccef.org/PAR_TPL_IDENTIFIANT/10/TPL_CODE/TPL_PUBLICATION_INTERNET/46-publications.htm

Fiche « Sécuriser et optimiser sa participation à un salon » : http://www.rhone-alpes.cci.fr/competences/IntelligenceEconomique/Salon.pdf

Guide pour réaliser un plan de continuité d'activité : http://www.sgdsn.gouv.fr/IMG/pdf/Guide_PCA_SGDSN_120613_web.pdf

Innovation & compétitivité
CCI RHÔNE-ALPES

« Protéger son patrimoine matériel et immatériel »

Le système d'information (SI)

Les cyberattaques ont augmenté de 42% en 2012, pour atteindre un coût global de 110 milliards de dollars. (Centre d'Analyse Stratégique – Note d'Analyse n°324 Mars 2013 / Etude Internet Security Threat Report 2013, Symantec)

PROTEGER SON SI A L'INTERIEUR DE L'ENTREPRISE

- Sécuriser le matériel : mots de passe complexes (8 caractères minimum avec majuscules, minuscules, chiffres et caractères spéciaux) à garder confidentiels, ou autre solution d'identification (reconnaissance digitale…) ; sauvegardes régulières des données sur un périphérique externe ensuite mis en sécurité.
- Former les collaborateurs à adopter un comportement prudent : ne pas brancher de périphérique externe (clé USB) ou télécharger de pièces jointes sans être certain de leur provenance, ne pas fournir d'informations personnelles ou sur l'entreprise via internet sauf motif légitime et destinataire fiable, verrouiller sa session avant de s'absenter.

PROTEGER SON SI CONTRE LES INTRUSIONS

- Sécuriser les réseaux : Installer des antivirus et les mettre à jour régulièrement, utiliser des pare-feu pour se protéger des attaques externes.
- Se méfier des réseaux sans fil, particulièrement dans les lieux publics, qui permettent l'accès aux données par un appareil extérieur.
- Protéger les communications : utiliser des solutions de cryptographie ; pour les informations très sensibles, utiliser le courrier papier.
- Emporter les données confidentielles sur des supports sécurisés et garder une surveillance constante sur le matériel.

Les locaux

Les entreprises de la région Rhône-Alpes sont statistiquement 4 fois plus souvent victimes d'atteintes que les résidences privées. *(Chiffres de la Gendarmerie Nationale)*

- Sécuriser les locaux et les abords extérieurs : clôtures, éclairages extérieurs automatiques, rideaux métalliques, barreaux aux petites ouvertures, portes verrouillées.
- Restreindre l'accès à l'entreprise : système d'identification pour les salariés (badge, digicode), contrôle d'identité pour les personnes extérieures.
- Ne pas laisser les documents stratégiques à portée de tous : broyer les documents sensibles avant de les jeter, effacer le tableau de la salle de réunion, garder les documents confidentiels dans un coffre, ne pas laisser le registre des visites à la disposition de tous.
- Organiser les locaux de l'entreprise de manière à limiter les risques de diffusion d'informations sensibles : éloigner le standard de la salle d'attente pour éviter que les visiteurs puissent entendre les conversations…

Guides utiles :

Guide d'hygiène informatique : http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

Guide Sécurité des Systèmes d'Information : http://fr.calameo.com/read/0002213411d409acbe3ff

Guide escroquerie sur internet : http://www.cher.gouv.fr/document/escroqueries-web_depliant.pdf

Info escroqueries : 0811 02 02 17 (coût d'un appel local)

Pour signaler un courriel ou un site internet d'escroquerie : www.internet-signalement.gouv.fr

Contact Intelligence Economique:

Franck GUIGARD : 04 75 75 87 24

www.innovation.rhone-alpes.cci.fr
www.netvibes.com/ie-rhonealpes-cci