Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

SECO
LA LETTRE DE LA SÉCURITÉ ÉCONOMIQUE

N°4 - 1er trimestre 2013

L'éditorial

Olivier BUQUEN,
Délégué Interministériel à l'Intelligence Economique

Qu'on parle de « sécurité économique » ou de « sûreté », la protection du personnel et du patrimoine informationnel est une préoccupation quotidienne pour tout acteur économique. Tous les membres de l'entreprise, quelles que soient leurs fonctions, doivent être mobilisés car ils sont tous, tels les maillons d'une chaîne dont on mesurerait la résistance à l'aune du plus fragile, impliqués et responsables. Certes, la fonction sûreté n'étant pas une activité « productive », il n'est pas toujours aisé d'évaluer une telle politique interne ou de transcrire en chiffres ses retombées. Ce manque de visibilité du retour sur investissement conduit malheureusement encore trop souvent les dirigeants à ne pas prendre en compte sérieusement les menaces et à sous-estimer le coût des attaques. Pourtant, une telle négligence peut, à terme, coûter cher à l'entreprise (perte de marchés, impact sur la réputation, procédure judiciaire, etc.). Aujourd'hui, aucune structure ne peut donc s'affranchir de cette composante. Il en va potentiellement de sa survie et donc des emplois qu'elle crée ou qu'elle maintient. Et pour tordre le cou aux idées reçues, la sécurité économique n'est pas forcément onéreuse. Une bonne politique de sûreté ne repose pas uniquement sur des investissements techniques coûteux, elle repose avant tout sur une communication interne efficace, visant à faire adhérer l'ensemble des salariés afin qu'ils adoptent, au quotidien, un comportement adéquat. Nous avons donc choisi de vous présenter, dans ce quatrième numéro de **SECO**, l'approche d'un grand groupe sur ce sujet et la campagne de communication interne qu'il a mis en œuvre. Vous retrouverez sur notre site des exemples de films de sensibilisation réalisés par de grands groupes dans le cadre de leurs campagnes internes de sécurité économique.

© Crédit : MINEFI / P.Ricard

Olivier BUQUEN

Et dans votre entreprise ?

Michel PAGES,
Directeur Sûreté du Groupe SAFRAN, témoigne.

SAFRAN
AEROSPACE · DEFENCE · SECURITY

D2IE : ***Quelle place est donnée à la sûreté par un groupe comme SAFRAN ?***

Michel PAGES : La sûreté des personnes travaillant pour le Groupe est une préoccupation constante de la Direction générale du Groupe, du fait notamment de la présence de salariés en mission et d'expatriés de Safran dans un grand nombre de pays, y compris dans des zones sensibles. L'autre priorité de la sûreté est d'accompagner le plus efficacement possible les capacités d'innovation du Groupe SAFRAN en protégeant le patrimoine informationnel dans ses composantes les plus sensibles.

En effet, l'innovation fait partie de l'ADN de l'entreprise ; le Groupe SAFRAN est le deuxième déposant français de brevets et a dépensé 1,7 milliard d'euros en recherche et développement en 2012.

D2IE : ***Quels outils permettent cette protection ?***

Michel PAGES : Cette innovation peut être protégée par des enceintes sécurisées et des coffres-forts, mais les meilleurs garants de cette protection sont les personnels du Groupe eux-mêmes, dans leur quotidien, lorsqu'ils adoptent quelques comportements simples et de bon sens.

En effet, nous savons que la plupart des atteintes à la sûreté de notre information sensible relèvent d'erreurs d'appréciation ou d'une méconnaissance des réelles menaces.

(suite en page 4)

D2iE

Délégation interministérielle à l'intelligence économique
5 place des Vins-de-France
75573 Paris CEDEX 12
01.53.44.26.22
www.intelligence-economique.gouv.fr

Abonnement à SECO

En ligne sur **www.intelligence-economique.gouv.fr/inscription-la-newsletter**
Par e-mail avec ABONNEMENT en objet à **contact@ie.gouv.fr**

Désabonnement : avec DESABONNEMENT en objet à ***contact@ie.gouv.fr***

Toute ressemblance avec un fait réel ...

A chaque numéro, la D2IE présente des cas récents d'ingérence économique, afin de vous aider à anticiper et à vous protéger. Récits d'événements réellement survenus au cours des derniers mois, les cas présentés constituent une illustration de la diversité des atteintes susceptibles de viser les entreprises françaises.

Les faits **: Absence de protection d'un ordinateur contenant des données sensibles**

Une PME, spécialisée dans la création de logiciels d'aide à la décision pour la gestion et la maîtrise des risques industriels, a dépêché un de ses ingénieurs pour la représenter lors d'un séminaire international organisé dans l'ouest de la France. Celui-ci a présenté les activités de son entreprise, dont il a notamment évoqué l'expertise dans le domaine très sensible de la gestion des risques industriels et environnementaux. Oubliant toute règle élémentaire de sécurité lors de la pause déjeuner, il a laissé dans la salle de conférence son ordinateur portable.
Pendant ce laps de temps, l'ordinateur du géophysicien a été dérobé. La salle de conférence contenait pourtant de multiples supports informatiques nomades à la valeur marchande bien plus élevée, mais seul le sien a disparu.
L'appareil dérobé contenait des informations stratégiques pour l'entreprise : fichier clients, certains contrats commerciaux confidentiels, les bilans carbone et les rapports d'audits de plusieurs sociétés clientes, des informations très confidentielles concernant la gestion des risques industriels dans le domaine énergétique et des transports, etc.

Commentaire **: Un risque permanent, même en milieu supposé de confiance**

Ce spécialiste du risque industriel n'a pas assimilé d'autres types de risques, notamment liés à la sensibilité des informations en sa possession et donc à la nécessité de les protéger. Si l'ordinateur lui avait appartenu, il y aurait sûrement prêté plus d'attention, ne serait-ce qu'en raison de sa valeur marchande.
Une grande partie des cas d'ingérence économique par atteintes aux systèmes d'information est encore constituée de vols d'ordinateurs à contenus très sensibles non cryptés. Sachant ce qu'il contenait, l'ingénieur n'aurait dû se séparer de son ordinateur à aucun moment. S'il souhaitait être libre pendant la pause, il aurait dû prévoir une présentation à partir d'un support amovible, type clé USB.

Les faits **: Divulgation d'informations confidentielles sur internet de la part d'un employé loquace**

Un ingénieur d'une grande entreprise française travaillant sur un projet innovant non commercialisé a communiqué sous un pseudonyme des informations confidentielles sur un forum lié à son secteur d'activité. Il a notamment évoqué le projet sur lequel il travaillait, en divulguant des photographies prises par ses soins dans un atelier de fabrication en dehors de toute autorisation. Le projet porté par l'entreprise était encore dans sa phase de développement et faisait l'objet d'un partenariat avec un client européen auquel le produit devait être livré ultérieurement. Le contrat avec le partenaire possédait une clause de confidentialité et précisait que ce dernier disposait d'une exclusivité du droit à l'image avant le lancement officiel. La direction sûreté de l'entreprise a pu identifier l'auteur des faits et établir que ce salarié avait agi par naïveté, sans réelle intention de nuire. L'employé indélicat a néanmoins fait l'objet d'une sévère mise en garde et la direction sûreté a mis en place une nouvelle campagne interne de communication.

Commentaire **: Une naïveté qui aurait pu coûter cher...**

La problématique de la protection de l'information ne porte pas exclusivement sur la divulgation d'informations techniques. Dans le cas présent, il s'agit de la communication non maîtrisée par l'entreprise de données commercialement sensibles pour lesquelles elle avait un accord de confidentialité. Cette diffusion est donc susceptible d'entacher le calendrier de communication du client, titulaire du droit à l'image du futur produit, de générer un contentieux entre le fabricant et son client, et de nuire à l'image du fabriquant en raison de son incapacité à protéger correctement son information stratégique. La sensibilisation des employés aux dangers d'une communication non maîtrisée, notamment sur Internet, doit donc faire partie intégrante de la politique de sûreté de l'entreprise.

A chaque numéro, la D2IE vous propose une fiche synthétique. Elle présente succinctement les risques potentiels sur un sujet précis et suggère des mesures de prévention et des parades simples à mettre en place.

Fiche n°4 : Une politique interne de sûreté : des messages simples, l'implication de tous

Pourquoi *chacun est responsable de tous**?

** Antoine de Saint-Exupery*

Que l'information stratégique soit diffusée à l'extérieur par accès indu à l'entreprise (piratage informatique, visiteurs indiscrets, stagiaires indélicats, etc.), ou par le détenteur lui même, involontairement ou non (perte de supports numériques mobiles, indiscrétions sur les réseaux sociaux, etc.), ce sont bien souvent des comportements humains qui facilitent cette diffusion ou les ingérences des acteurs malveillants. Une politique de sûreté efficace repose donc sur une **communication positive** visant à faire adhérer **l'ensemble du personnel** et à le **responsabiliser**. L'implication de tous les salariés et l'application au quotidien de ces petits gestes contribuent en effet grandement à diminuer les risques et, in fine, à préserver les emplois.

Comment se protéger : des gestes simples, appliqués au quotidien

Au bureau

- Identifier ses interlocuteurs et les visiteurs
- Ne pas mettre de documents sensibles à la corbeille, les détruire au broyeur
- Ne pas laisser traîner de documents sensibles sur son bureau
- Si l'imprimante et la photocopieuse sont partagées, récupérer immédiatement ses documents
- Utiliser un mot de passe robuste sur son ordinateur
- Chiffrer les données sensibles envoyées par e-mail
- Utiliser un logiciel de chiffrement pour protéger les dossiers sensibles sur son disque dur
- Verrouiller son ordinateur en quittant le bureau (il existe des raccourcis clavier très pratiques)
- S'assurer que les logiciels sont régulièrement mis à jour, ainsi que les anti-virus et les pare-feu
- Utiliser les clés USB de manière sécurisée (éviter les prêts, bien séparer les usages personnel et professionnel)

Après une réunion, surtout lorsque que celle-ci se tient dans un lieu partagé type « *business center* » n'appartenant pas à l'entreprise :

- Effacer le tableau
- Retirer les feuilles du *paper-board*, les emporter ou les broyer

A l'extérieur

- Ne jamais se séparer de ses supports numériques nomades (ordinateur portable, téléphone, tablette, clé USB, etc.)
- Dans les zones et les transports publics, habiller son écran d'ordinateur d'un filtre de confidentialité
- Rester discret dans les lieux publics ou les transports en commun
- Ne pas évoquer d'informations sensibles au téléphone
- Adopter une conduite sûre sur les réseaux sociaux, en restant discret sur son activité professionnelle
- Faire un usage réfléchi de ses outils numériques professionnels (navigation internet, etc.)

Vous souhaitez en savoir plus : retrouvez des exemples en vidéos de campagnes de communication internes sur **http://www.intelligence-economique.gouv.fr/actualites/sensibiliser-ses-salaries-la-securite-economique**

Et dans votre entreprise ? (suite)

Vous avez mis en place des bonnes pratiques en matière de sécurité ? Vous avez fait face avec succès à une menace ou à une agression économique ? Si vous souhaitez partager votre expérience, cette rubrique est la vôtre.
Ecrivez-nous à ***contact@ie.gouv.fr***

(suite de la page 1)

D2IE : ***Partant de ce constat, comment procédez-vous pour faire évoluer ces comportements au quotidien ?***

Michel PAGES : Il faut bien entendu obtenir l'adhésion de l'ensemble des salariés à cet enjeu, en énonçant clairement que, sur le long terme, leur emploi est potentiellement lié à l'innovation et à sa protection. Pour cela, nous avons lancé, conjointement avec la direction de la Communication, une campagne didactique interne (films, affiches) et mondiale de sensibilisation, traduite en six langues et diffusée dans plus de 200 établissements du Groupe.

D2IE : ***Les salariés ne perçoivent-ils pas cela comme une contrainte supplémentaire ?***

Michel PAGES : Effectivement, pour de nombreuses personnes, la sûreté peut apparaître presque comme une contrainte, comme l'est le fait de mettre sa ceinture de sécurité en voiture ou de porter un casque sur un chantier. C'est une question d'image et de formation à développer pour changer cette fausse appréciation. Nous avons fait le choix de faire une campagne volontairement décalée et non anxiogène, en utilisant l'humour plutôt que la crainte ou le message dogmatique. Cette campagne de sensibilisation repose sur des conseils de bon sens, de bonnes pratiques à adopter au quotidien, en un mot sur une « hygiène comportementale » simple : parler avec discrétion au téléphone ou dans des lieux publics, surveiller ses outils de communication nomades lors de ces déplacements, etc.

D2IE : ***Actuellement, quel retour avez-vous sur cette approche de la sûreté ?***

Michel PAGES : Il est trop tôt pour tirer un bilan, d'autant plus que la modification des comportements ne pourra se faire sans communiquer et sensibiliser de manière régulière les salariés du Groupe. Toutefois, cette campagne a donné à la sûreté une plus grande visibilité dans le Groupe. Elle a contribue à faire évoluer positivement l'image de notre mission auprès des salariés, qui comprennent que cette dernière ne repose pas exclusivement sur le nombre de caméras et la hauteur des « clôtures », mais avant tout sur le comportement au quotidien de chacun.

L'actualité de la D2IE

www.intelligence-economique.gouv.fr

La D2IE a lancé son nouveau site internet ! Il vous aidera à mieux comprendre les enjeux liés à l'intelligence économique, tant pour l'Etat que pour les entreprises et les établissements de recherche. Vous y retrouverez notamment une présentation de l'ensemble des actions menées par la Délégation, non seulement en matière de sécurité économique mais aussi de veille, d'influence, ou encore de formation à l'IE. Vous pourrez aussi y trouver des informations pratiques, des conseils et des recommandations utiles à la mise en œuvre d'une démarche d'IE, les publications de la D2IE, et les anciens numéros de **SECO**.

Bonne navigation !

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

INFORMATION SIGNALEMENT

A votre service…

Vous avez des questions sur la sécurité économique.
Vous faites face à une situation atypique et vous ne savez pas avec qui l'évoquer.
Vous souhaitez signaler un fait, une atteinte que vous avez subie.

Sans entrer dans le détail, laissez-nous vos coordonnées.
Vous serez rapidement recontactés par le service de l'Etat compétent.

securite-economique@interieur.gouv.fr