Lettre d'information économique

L'activité créatrice et commerciale de l'entreprise est dépendante de son environnement. L'internationalisation des sociétés et l'accession à de nouveaux marchés aussi variés que lointains ont depuis quelques décennies effacé la frontière entre géopolitique, enjeux économiques et jeux d'influence.

Depuis un mois, le déclenchement puis l'évolution du conflit entre la Russie et l'Ukraine ont vu coexister économie de guerre et guerre économique. **Les sociétés qui composent *la base industrielle et technologique de la défense***, par leur activité sectorielle directement liée aux armées pour les unes, par leur savoir-faire contributif, ciblé ou dual, pour d'autres, **sont *de facto* positionnées sur un front parallèle à celui des effets politiques et diplomatiques.** Cette autre ligne de confrontation est composée d'effets directement induits (bouleversement des tarifs et des marchés) ou résultant des actions contraignantes des différentes parties (sanctions et contre-sanctions).

Vous êtes concernés, cette lettre vous est donc adressée.

Ces effets sont susceptibles de porter atteinte subitement et durablement à la stabilité de votre activité générale, notamment celle liée à la sphère défense et par extension à votre écosystème (partenaires, industriels, fournisseurs, sous-traitants, collaborateurs, etc.). Alors que, les effets de la pandémie ne sont pas encore résorbés, ce risque fort rehausse le **besoin de vision et de dispositifs de sûreté et sécurité** globaux, adaptés et éprouvés régulièrement, afin de maintenir l'activité.

Pour faire face, rester dynamiques, innovants et opérationnels, il est essentiel de savoir, comprendre et réagir « à temps ». A ce titre, les risques nécessitent d'être distingués, mesurés et anticipés.

Dans le contexte du conflit russo-ukrainien, les points de vigilance et de diligence que nous souhaitons partager avec vous, sont les suivants :

1 - Identifier les tentatives d'ingérences commerciales.

En temps de guerre, la course à l'autonomie technologique s'accélère. Il s'agit, de détecter les risques de captation directe ou détournée de savoir-faire déficitaires en Russie.

Pour cela, nous vous conseillons d'être particulièrement vigilant, à l'égard de toute proposition qui pourrait s'apparenter *in fine* à un contournement des sanctions.

La DRSD constate une augmentation des approches des entreprises et des demandes d'acquisition, en urgence, de différents matériels de guerre par des individus se présentant comme des intermédiaires des autorités ukrainiennes.

2 - Identifier et prévenir les ingérences numériques.

Le risque d'attaques cyber visant les entreprises, notamment en réponse aux sanctions économiques européennes, est majeur. Ce risque est encore renforcé pour les entreprises françaises hébergeant leurs données sur des serveurs à l'étranger, notamment en Europe centrale.
Les objectifs poursuivis par les auteurs de ces atteintes sont principalement l'altération des données (recours massifs aux *wipers* visant à effacer vos données), l'influence, ainsi que l'espionnage économique.

3 - Mesurer et décrire les risques indirects et induits.

Il importe d'alerter sur les déséquilibres et déficits liés aux impacts des sanctions qui vous concernent (risques de ruptures d'approvisionnement, difficultés financières liées à la perte de contrats/ partenariats, et autres effets).

En miroir des premiers effets, il est nécessaire de mesurer et d'anticiper les risques liés aux contre-sanctions qui pourraient vous concerner (confiscation de biens et d'avoirs en Russie, risque pour le personnel français resté sur place, risques liés aux audits de conformité envisagés par des acteurs étrangers tiers au mépris de la législation nationale).

Dans ce contexte, vos interlocuteurs habituels de la DRSD restent pleinement mobilisés et disponibles pour **accompagner les entreprises, sensibiliser les équipes dirigeantes et collaborateurs**, recueillir les sollicitations et remonter auprès du ministère des armées les difficultés qu'elles pourraient rencontrer.

Les DISSE sont également des points d'entrée pour vous aiguiller dans vos actions. Afin d'appuyer et de protéger au mieux les intérêts qu'elles partagent avec la Défense, les entreprises de la BITD sont invitées à **remonter auprès de leur référent DRSD toute information** sur les effets actuels ou pressentis de ce conflit.

4 - Identifier les vulnérabilités

- Inventorier les implantations géographiques de votre chaîne de valeur, en particulier les sites les plus vulnérables détenant un savoir-faire essentiel.
- Cartographier vos sous-traitants stratégiques et évaluer leurs liens avec la Russie, ainsi que les risques potentiels en cas de rupture d'approvisionnement ou de savoir-faire.
- Evaluer les répercussions financières directes et indirectes (banques, investissement, actionnariat, etc. ex. réseau SWIFT).
- Identifier les données stockées sur des serveurs à l'étranger, en particulier ceux situés en Europe de l'Est et caractériser leur sensibilité en vue d'un éventuel rapatriement.
- Identifier toute approche d'entreprise au but d'information ou de demande d'acquisition par des individus, français ou étrangers, se présentant comme intermédiaires de sociétés ukrainiennes, voire de l'Etat ukrainien.

5 - Maîtriser les impacts

- Pour les sites points d'importance vitaux (PIV), s'assurer que le plan de continuité de l'activité (PCA) est actualisé et fonctionnel.
- Pour les sites non PIV, formaliser un plan sur le modèle des PCA.
- Renforcer les contrôles de sécurité et sûreté sur vos sites, notamment en cas de visite de délégations étrangères.
- Renforcer la sensibilisation des personnes internes et externes ayant accès aux zones protégées et ZRR.
- Contrôler vos processus SSI, les amender si nécessaire (ex. segmentation de vos SI, contrôle des accès individualisé, processus de sauvegarde physique hors réseau, etc.).

6 - Alerter pour réagir

Vous constatez :

- une vulnérabilité critique de votre chaîne de valeur (ex : rupture d'approvisionnement ou risque financier) ;
- une dépendance logicielle ou technique aux matériels russes ou ukrainiens ;
- un comportement SSI anormal (connexions inconnues, changement de mot de passe non sollicité, comportement anormal dans les logs) ou une tentative de cyberattaque ;
- un contact cyber suspect (email, approche sur les réseaux sociaux, etc.) ;
- un incident de sécurité (intrusion physique, survol de drone).

Gardons contact

N’hésitez pas à contacter votre agent référent afin de faire remonter toute ingérence ou atteinte (physique, économique, juridique, cybernétique, etc.) dont vous penseriez être victimes.

Soyez assurés que la DRSD et les agents présents à votre contact se tiennent à vos côtés dans ce contexte aussi singulier que versatile.

SUIVRE L'ACTUALITÉ

Bercy met en place un dispositif exceptionnel pour accompagner les entreprises affectées par les conséquences de la guerre en Ukraine

https://www.entreprises.gouv.fr/fr/actualites/crise-ukrainienne-impact-sur-les-activites-economiques

CONSEIL DU MINISTERE DE L'EUROPE ET DES AFFAIRES ETRANGERES :
Numéro de la cellule de crise H24/J7 du Centre de crise et de soutien : 01.53.59.11.00

SANCTIONS ÉCONOMIQUES ET FINANCIÈRES, RESTRICTION DES EXPORTATIONS :
Site de la Direction générale du Trésor :
https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/russie
Sur les sanctions mises en place : sanctions-russie@dgtresor.gouv.fr
Sur leur impact sur les biens à double usages : doublusage-sanctions.russie@finances.gouv.fr
DISSE : Délégués à l'information Stratégique et à la Sécurité économiques :
Coordonnateur régional de la politique de sécurité économique
https://sisse.entreprises.gouv.fr/sisse-region/sisse-region

TENSIONS SUR LES APPROVISIONNEMENTS :
tensions-approvisionnements.russie@finances.gouv.fr
Risque de tentative de contournement de l'embargo russe :
En cas de doute nous vous invitons vivement à vous s'adresser à l'autorité nationale de classement, la DGA/DI : dga-di.classement.fct@intradef.gouv.fr

RENFORCEMENT DE LA VIGILANCE CYBER
ANSSI (Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Point de contact (disponible H24, 7/7) en cas d'incident :
+33 (0)1 71 75 84 68 ou cert-fr.cossi@ssi.gouv.fr
ACYMA : Assistance et prévention en sécurité numérique : *www.cybermalveillance.gouv.fr*

FOCUS PME/ETI
Contacter le Commissaire aux Restructurations et à la Prévention :
https://www.entreprises.gouv.fr/fr/industriepolitique-industrielle/commissaires-aux-restructurations-et-prevention-des-difficultes

PRIX DE L'ÉNERGIE ET RELATIONS AVEC SON FOURNISSEUR ÉNERGÉTIQUE
Les prix du gaz et de l'électricité, notamment pour les entreprises, connaissent depuis plusieurs mois des évolutions à la hausse, qui pourraient être maintenues ou augmentées en fonction de l'évolution de la situation en Ukraine. Le site rappelle les modalités de changements de fournisseurs, propose un comparateur des offres des différents fournisseurs, rappelle les droits du client par rapport à son fournisseur.
https://www.energie-info.fr/pro/
En cas de défaillance d'un fournisseur, le Gouvernement a désigné un fournisseur de secours pour assurer à titre transitoire la continuité d'approvisionnement des consommateurs.
https://www.ecologie.gouv.fr/fourniture-dernergie-ministere-designe-des-fournisseurs-secours-en-electricite-assurer-titre