# SECTEUR MANUFACTURIER CRITIQUE : Sécurité de la chaîne d'approvisionnement et marché gris

Cette fiche d'information renseigne les lecteurs sur la progression continue du marché gris et sur la manière dont ses composants peuvent affecter les chaînes d'approvisionnement nationales. Ce document présente également plusieurs types de marchés (gris et noir) et explique pourquoi ceux-ci posent problème.

## POURQUOI LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT EST-ELLE IMPORTANTE POUR LE SECTEUR MANUFACTURIER CRITIQUE ?

Le Secteur manufacturier critique s'appuie fortement sur des chaînes d'approvisionnement complexes (à la fois nationales et internationales) pour la livraison de matières premières, de pièces fabriquées et de composants finaux. Les chaînes d'approvisionnement des fabricants sont de plus en plus vastes, complexes et interdépendantes, comprenant parfois des centaines d'installations, de fournisseurs et de prestataires répartis dans différentes régions. L'approche d'une entreprise en matière de sécurité de la chaîne d'approvisionnement est essentielle et doit être adaptée aux caractéristiques et besoins spécifiques de la chaîne d'approvisionnement.

## MARCHÉS BLANC, GRIS ET NOIR

Les entreprises se doivent de faire la distinction entre les marchés blanc, gris et noir afin de s'assurer que leurs produits importés proviennent de distributeurs autorisés, liés à la marque ou aux fabricants de composants d'origine (OCM).

- Le marché blanc est le marché légal, officiel ou autorisé de biens et de services, qui utilise des circuits, des fabricants et des distributeurs autorisés.
- Le marché gris est un marché controversé qui donne accès aux vendeurs et aux acheteurs par le biais de circuits non autorisés, qui ne sont pas affiliés à la marque ou aux fabricants de composants d'origine.
- Le marché noir évite les sanctions gouvernementales en échangeant des biens et en effectuant des transactions par des circuits illégaux.

## QUE SE PASSE-T-IL SI UN MATÉRIAU DU MARCHÉ GRIS PÉNÈTRE DANS LA CHAÎNE D'APPROVISIONNEMENT ?

Les matériaux du marché gris ou noir peuvent entrer dans la chaîne d'approvisionnement par de nombreux points, rendant ainsi difficile la traçabilité de leur origine et de leur fournisseur initial. À long terme, les produits et composants du marché gris ont un impact négatif sur la réputation de la marque, les coûts, la responsabilité et le chiffre d'affaires tout au long de la chaîne d'approvisionnement. Même si des mesures de prévention sont prises, des matériaux provenant du marché gris peuvent s'immiscer dans la chaîne d'approvisionnement d'une entreprise. La prise en compte des risques et la mise en œuvre des meilleures pratiques peuvent atténuer les intrusions du marché gris.

### Éléments à prendre en compte pour les risques de la chaîne d'approvisionnement

- Nombre et emplacements des fournisseurs.
- Origine des expéditions.
- Conditions contractuelles définissant les obligations de sécurité pour les expéditions des fournisseurs ou des prestataires.
- Fournisseurs de logistique tiers ou partenaires impliqués dans la chaîne d'approvisionnement (par exemple, sociétés d'emballage, d'entreposage, de transport routier, transitaires et transporteurs aériens ou maritimes) qui s'occupent des expéditions.

### Meilleures pratiques pour l'analyse de la chaîne d'approvisionnement

- Établir une politique d'entreprise concernant la gestion des risques liés aux fournisseurs. Toute politique de gestion des risques liés aux fournisseurs doit commencer par la définition de critères de sélection spécifiques, de procédures de contrôle et du nombre de fournisseurs possibles pour chaque type de produit ou de composant. Le recours à plusieurs fournisseurs agréés peut atténuer les perturbations de la chaîne d'approvisionnement.
- Utiliser une matrice de gestion des risques et de contrôle des fournisseurs pour évaluer ces derniers. Une matrice de gestion et de contrôle des risques liés aux fournisseurs permet de calculer une estimation des risques et de la probabilité de survenue d'un incident afin de déterminer les mesures à prendre pour atténuer les risques inacceptables liés aux fournisseurs.
- Élaborer et mettre en œuvre un accord de niveau de service (ANS) avec les prestataires ou fournisseurs sélectionnés. Un accord de niveau de service définit le niveau de service attendu d'un prestataire, d'un fournisseur ou d'un distributeur en précisant des indicateurs de service, ainsi que des solutions ou des pénalités si les indicateurs et les conditions de service ne sont pas respectés.
- Effectuer une vérification continue des fournisseurs. Examiner en permanence les risques commerciaux des fournisseurs tout au long de la durée de leur collaboration.

## GESTION DU RISQUE FOURNISSEUR

Généralement mise en œuvre avant et après l'achat ou l'externalisation auprès de distributeurs et de fournisseurs tiers, la compréhension et la mise en œuvre de la gestion du risque fournisseur (également connue sous le nom de gestion du risque fournisseur) aide les entreprises à éviter les risques et à protéger leur réputation.

### Pourquoi la gestion du risque fournisseur est-elle importante ?

La dépendance à l'égard de fournisseurs peu recommandables a des répercussions importantes sur les activités de l'entreprise, la sécurité des données et des informations, les résultats financiers et la réputation de l'entreprise. Il est impératif de s'assurer que les prestataires et fournisseurs respectent les exigences réglementaires.[1] Ce type de gestion réduit le risque d'une sécurité insuffisante des données et de défaillances de cybersécurité, de violations de la réglementation et d'une interruption des activités due à la défaillance d'un fournisseur ou à des retards importants de livraison de la chaîne d'approvisionnement.

### Exemples de gestion du risque fournisseur

- L'absence de contrats adéquats ou de bons de commande approuvés avant l'obtention de produits auprès d'un prestataire ou d'un fournisseur.
- Une violation de données en matière de cybersécurité remonte jusqu'au prestataire ou au fournisseur tiers.
- Prestataires ou fournisseurs frauduleux.
- Fermetures imprévues de fournisseurs ou retards dus à une mauvaise gestion budgétaire, qui peuvent avoir une incidence sur la continuité des activités.

### Le processus de décision en matière d'approvisionnement

Il est essentiel d'adopter une approche diligente des pratiques d'achat, d'inspection et de test afin de minimiser l'impact du marché gris. L'achat d'articles auprès du fabricant de composants d'origine (OCM), c'est-à-dire des entreprises qui conçoivent ou fabriquent une pièce et qui détiennent les droits de propriété intellectuelle sur l'article, garantit un risque minimal de contrefaçon et, par conséquent, une confiance maximale dans l'authenticité de l'article. Les distributeurs agréés/franchisés et les fabricants sous contrat sont également probablement fiables et ont conclu un accord contractuel avec le fabricant de composants d'origine pour acheter, stocker, reconditionner, vendre et distribuer ses gammes de produits. Lors de l'ouverture des sources d'approvisionnement, les distributeurs indépendants et les courtiers ne sont pas toujours contractuellement liés ou obligés de respecter les conditions du fabricant de composants d'origine, mais ils achètent des pièces pour les vendre et les redistribuer sur un marché ouvert. Les sources inconnues présentent la confiance la plus faible en matière d'authenticité et constituent un risque élevé de contrefaçon.

## COMMENT SIGNALER UNE VIOLATION DE LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

En raison de leur taille et de la complexité des relations, il peut être difficile de retracer les atteintes à la sécurité de la chaîne d'approvisionnement. Le groupe de travail sur la Gestion des risques liés à la chaîne d'approvisionnement des technologies de l'information et de la communication (ICT SCRM) a formulé des conseils pour gérer ces risques. Pour plus d'informations sur le signalement des violations, veuillez consulter les ICT SCRM Essentials (Principes essentiels de gestion des risques liés à la chaîne d'approvisionnement des technologies de l'information et de la communication) sur la page ICT SCRM de la CISA.

## EXEMPLE D'ÉTUDE DE CAS PERTINENTE

La Commission des forces armées du Sénat américain (SASC) a lancé une enquête sur des pièces électroniques contrefaites dans la chaîne d'approvisionnement du Département de la défense entre 2009 et 2011, dont beaucoup provenaient de divers points de revente aux États-Unis, au Royaume-Uni et au Canada. Les enquêteurs ont désigné la Chine comme source de produits électroniques contrefaits et ont découvert des pièces soupçonnées d'être des contrefaçons sur des ordinateurs de mission de missiles de l'Agence des États-Unis pour la défense antimissile (MDA) et sur des viseurs d'armes thermiques. Cette enquête a permis d'identifier 1 800 cas de contrefaçon. En conséquence, l'accès à la Chine a été interdit au personnel de la SASC. Tous les matériaux, composants et pièces électroniques doivent être validés pour s'assurer qu'ils proviennent de distributeurs et de fournisseurs autorisés/franchisés de la chaîne d'approvisionnement. Ce processus de validation et d'authentification procure la plus grande confiance dans l'authenticité et le risque le plus faible de se procurer des matériaux du marché gris et des contrefaçons.[2]

## POUR EN SAVOIR PLUS SUR LE SECTEUR MANUFACTURIER CRITIQUE

Contactez l'équipe de gestion du secteur manufacturier critique à CriticalManufacturingSector@cisa.dhs.gov ou consultez le site cisa.gov/critical-manufacturing-sector.

[1] Les exigences réglementaires concernant la chaîne d'approvisionnement comprennent, notamment, les règles du commerce international, les normes environnementales, sociales et de gouvernance (ESG), les règles de sécurité et de qualité des produits, les règles de confidentialité et de sécurité des données, ainsi que les règles de lutte contre la corruption et les pots-de-vin.

[2] Abesamis, C. et Leblanc, M. (2015) NASA Counterfeit Parts Awareness and Inspection [Diapositives PowerPoint 23 et 24]. Extrait de la version PDF du document NASA Counterfeits Parts Awareness and Inspection.