ANDERS AVOCATS

La Supply Chain : maillon faible… juridiquement aussi ?

Renforcer la maîtrise du risque cyber des tiers par le droit et le contrat

OSSIR | 30 MINUTES

Cécile Vernudachi - Avocat Associé - Anders Avocats

Département droit du numérique - Anders Avocats

Nos domaines d'expertise

- Contrats & Projets IT
- Contentieux informatique
- Données personnelles (RGPD)
- Propriété intellectuelle
- Conformité numérique
- Cybersécurité
- E-commerce
- Intelligence artificielle

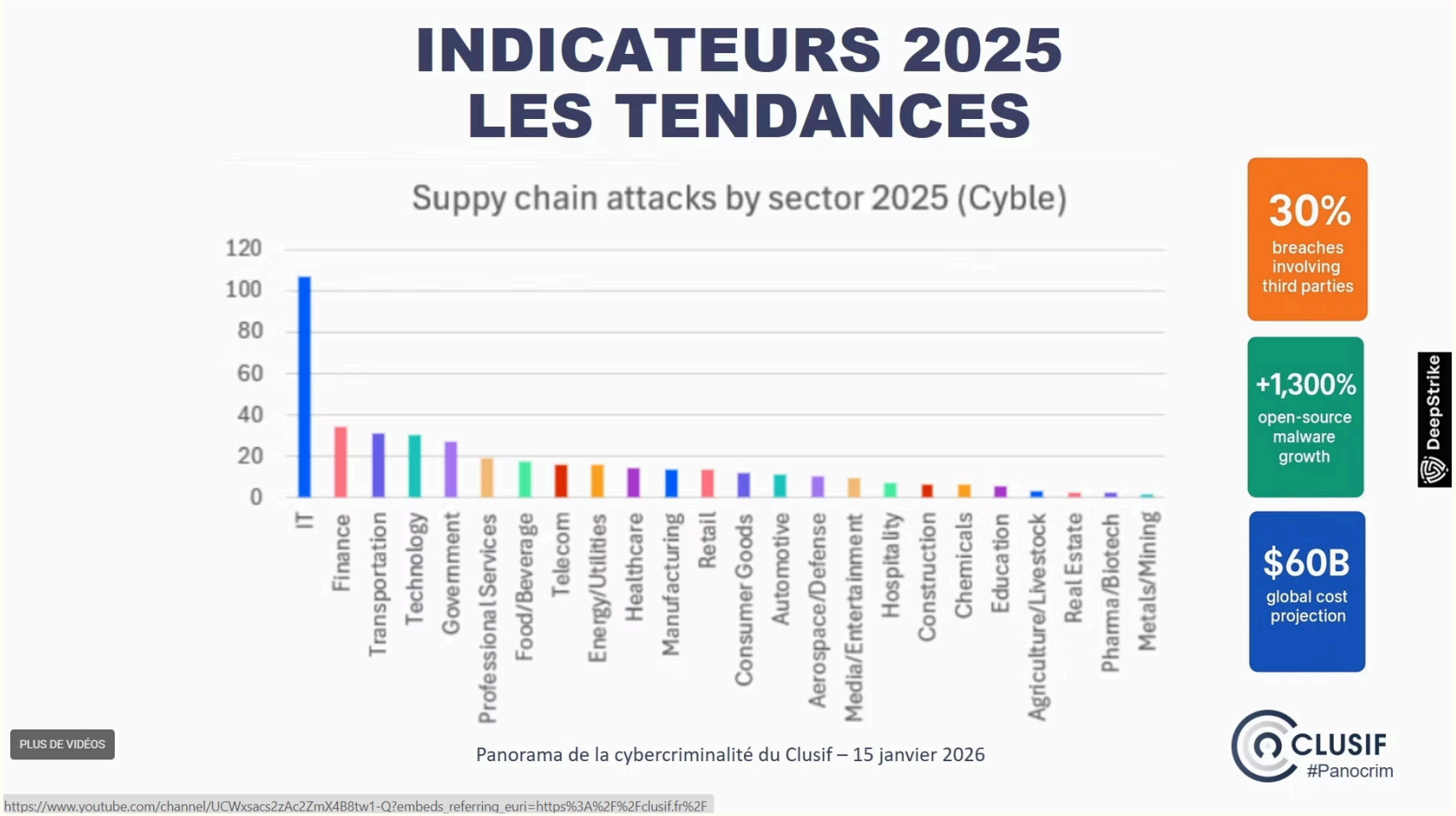
Supply chain : porte d'entrée

Etablissement hospitalier victime d'une cyberattaque/ support d'une application métier

- Faiblesse des engagements contractuels, anciens, en particulier en matière de protection des données personnelles et de sécurité IT
- Pas de déclaration de sous-traitant de rang 2
- Coopération complexe avec les prestataires de la chaine de sous-traitance
- Sous-traitant de rang 2 : TPE

La cybersécurité **se négocie, se contrôle et se prouve dans les contrats fournisseurs.**

Croissance des attaques via la chaine d'approvisionnement



Source : Cyble – Supply Chain Attacks 2024-2025 / CLUSIF – Panorama de la cybercriminalité, janvier 2026

La Supply Chain IT : une constellation d'acteurs et de ressources critiques

Éditeurs de logiciels

Développeurs des solutions critiques, responsables des mises à jour et correctifs de sécurité (paquets logiciels, éditeurs connus…)

Intégrateurs

Configurateurs et déployeurs des systèmes, détenant souvent des accès privilégiés étendus

Hébergeurs et cloud

Gardiens de vos données et infrastructures critiques, point névralgique de disponibilité

Infogérants

Gestionnaires quotidiens de vos SI avec accès permanents et privilèges d'administration

Sous-traitants en cascade

Acteurs de rang 2, 3 et au-delà, souvent invisibles mais techniquement critiques

Les "vulnérabilités" juridiques majeures (1/2)

Six points de défaillance contractuelle récurrents

1. Cadre inadapté à un environnement complexe

Modèle de contrats plaqués sans adaptation à la réalité technique (nombreux intervenants, fortes dépendances en cascade)

Dilution des responsabilités.

2. Clauses de sécurité imprécises

Obligations de moyens génériques sans référentiel technique opposable.

3. Sous-traitance non encadrée

Autorisation tacite de sous-traiter sans validation, audit ou clause de solidarité. Vous découvrez l'existence du sous-traitant lors de l'incident.

Les "vulnérabilités" juridiques majeures (2/2)

Six points de défaillance contractuelle récurrents

4. Notification des incidents défaillante

Absence de délais contractuels ou délais incompatibles avec DORA et NIS 2. Le prestataire prend « connaissance » de l'incident mais ne le notifie que plusieurs semaines après.

5. Plafonds de responsabilité inadaptés (répartition des risques)

Limitation à 1x le montant annuel du contrat alors que le coût réel d'un incident peut atteindre 50 à 100 fois cette somme. Asymétrie totale du risque.

6. Réversibilité inexistante

Pas de procédure de reprise des données ni de plan de sortie sécurisé. En cas de rupture brutale post-incident, vous êtes en situation de dépendance critique.

Reprendre la main sur le contrat: un outil de gestion des cyber-risques

Bonne pratiques : focus sur certaines clauses

Matrice de responsabilités (RACI)

- R : Responsable
- A : Approbateur
- C :Consulté
- I : Informé

Processus cyber	Client métier	DSI client	RSSI client	Prestataire IT	SOC
Définition de la politique de sécurité	I	C	A/R	I	I
Analyse de risques SI	I	C	A/R	C	I
Gestion des identités et des accès	R	A	C	C	I
Gestion des correctifs de sécurité	I	A	C	R	I
Gestion des vulnérabilités	I	C	A	R	C
Supervision sécurité (logs, SIEM)	I	C	A	C	R
Détection d'incident cyber	I	I	C	C	R
Qualification d'incident	I	I	A	C	R
Réponse technique à incident	I	C	A	R	C
Plan de gestion de crise cyber	I	C	A/R	C	I
Sauvegardes	I	A	C	R	I
Tests de restauration	I	A	C	R	I
Tests d'intrusion	I	C	A	C	R
Sensibilisation sécurité	R	C	A	I	I

Clauses de sécurité : nature de l'obligation de sécurité IT Conséquences juridiques ?

1

Obligations de moyens

Le prestataire s'engage à mettre en œuvre ses **meilleurs efforts pour atteindre un objectif fixé**, finalement incertain (Exemple : Obligation de conseil)

=> Le Client doit prouver par tous moyens le manquement du prestataire à ses engagements.

2

Obligation de moyens renforcée

Le prestataire s'engage à **atteindre un objectif fixé conformément à l'état de l'art** (Exemple : obligation de sécurité)

=> Renversement de la charge de la preuve

3

Obligation de résultat

Le prestataire s'engage à atteindre un **résultat défini contractuellement**, objectif, déterminé et mesurable (Exemples : Respect des SLA et deadlines, etc.)

=> Renversement de la charge de la preuve

Comment rédiger une clause sécurité efficace ?

Obligation contractuelle

Les engagements généraux de sécurité sont définis dans le contrat et sont ensuite détaillés en annexe (PAS, PCA, PRA). Référence à des normes reconnues : ISO/IEC 27001, Guide d'hygiène informatique de l'ANSSI.

Référence à "l'état de l'art" possible.

Obligation légale et réglementaire

Certaines obligations sont imposées directement par la loi (RGPD, NIS 2, DORA). Leur respect s'impose indépendamment de toute stipulation contractuelle.

Une notion évolutive

L'obligation de sécurité doit être maintenue tout au long du contrat. Question : qui supporte la charge des mises à jour imposées par les évolutions réglementaires ?

La répartition des risques - plafond de responsabilité adapté à votre risque

Cas concret - Incendie OVHcloud : quand le plafond de responsabilité limite l'indemnisation

Cour d'appel de Douai, 24 avril 2025

En ne souscrivant pas à cette offre plus complète Bâti Courtage ne pouvait exiger contractuellement une sauvegarde sur un site distant : absence de faute d'OVH sur ce point

Sur les clauses limitatives de responsabilité : la clause qui exonère OVHcloud pour la perte de contenus hébergés car l'hébergeur n'est pas en charge de la continuité d'activité du client, était valide.

De même, la clause qui plafonne l'indemnisation au montant des sommes payées par le client pour le service concerné au cours des six derniers mois, a été jugée applicable.

> **Application du plafond contractuel : 1.800 € (6 mois d'hébergement) . Le client réclamait plus de 6 millions d'euros de dommages-intérêts**

Articuler la responsabilité avec les autres mécanismes de gestion du risque

Garanties contractuelles

Engagements de conformité réglementaire (RGPD, NIS 2, DORA), de sécurité (niveau de service, état de l'art) et de performance (SLA). Le prestataire garantit le maintien de ces engagements pendant toute la durée du contrat.

Pénalités contractuelles

Pénalités automatiques en cas de manquement aux obligations de sécurité ou de non-respect des délais de notification. Effet dissuasif et incitatif à la conformité, sans avoir à prouver un préjudice.

Assurance (cyber)

Exiger une assurance (cyber) professionnelle avec couverture minimale définie contractuellement.

> L'objectif n'est pas de sanctionner mais d'aligner les intérêts du prestataire sur ceux du client en matière de sécurité.

L'arsenal réglementaire se renforce

NIS 2

Obligation de gestion des risques liés aux fournisseurs et sous-traitants pour les entités essentielles et importantes

DORA

Exigences renforcées de résilience opérationnelle numérique pour le secteur financier, avec registre des tiers critiques

RGPD

Responsabilité du responsable de traitement sur les sous-traitants, obligation de garanties contractuelles appropriées

CRA

S'assurer que les produits comportant des éléments numériques sont mis sur le marché avec moins de vulnérabilités et que leurs fabricants assurent leur sécurité durant leur cycle de vie.

Impact concret

- Cartographie obligatoire des prestataires critiques
- Due diligence renforcée avant contractualisation
- Supervision continue des tiers
- Plans de contingence documentés
- Reporting régulier aux instances de gouvernance

La traduction des exigences dans le contrat

Comment NIS 2, DORA, CRA, et RGPD transforment vos obligations vis-à-vis de la Supply Chain

Évaluation préalable

Due diligence sécurité avant contractualisation : certifications, audits, questionnaires de sécurité, analyse des sous-traitants.

Annexer les réponses du fournisseur

Contractualisation renforcée : sécurité

Clauses opposables, et conformes aux textes (contenus parfois imposés : article 30 pour DORA, 28 pour RGPD) : ex. PAS, charte de télémaintenance, SLA de sécurité

Supervision continue

Audits périodiques, revue des incidents, contrôle des évolutions, suivi des certifications et suivi des SLA de sécurité.

Gestion des incidents

Procédures de notification formalisées, coordination des réponses, traçabilité des actions, analyse post-incident obligatoire.

Plan de sortie

Réversibilité documentée, procédures de reprise, conservation sécurisée des données, continuité assurée en cas de rupture.

Synthèse : le contrat comme outil de cybersécurité

Huit clauses essentielles pour transformer vos contrats en instruments de maîtrise du risque cyber

Obligations de sécurité opposables

Référence à des normes techniques précises (ISO 27001, référentiels ANSSI).

Droit d'audit étendu

Audit initial, audits périodiques annoncés, audits inopinés en cas d'alerte, droit d'audit des sous-traitants de rang 2 et 3. Aux frais du prestataire ?

Procédure de notification d'incident ou de vulnérabilité

Pour NIS 2 - Délai de notification initial par le client aux autorités : 24h maximum. Notification complète sous 72h.

Le prestataire notifie tout incident de cybersécurité dans les délais contractuellement prévus.

Maîtrise de la sous-traitance

Autorisation préalable écrite obligatoire. Communication de l'identité et localisation des sous-traitants. Les exigences de sécurité du contrat doivent être répercutés aux acteurs de la supply chain.

Assurance obligatoire

Couverture minimale définie contractuellement. Attestation annuelle d'assurance. Maintien de la couverture pendant toute la durée du contrat.

Responsabilité adaptée au risque

Plafond de responsabilité proportionné au risque réel. Exclusion du plafond en cas de violation des obligations de sécurité, et concernant les données personnelles .

Réversibilité et continuité

Procédure de restitution sécurisée des données. Formats ouverts et portables. Assistance lors de la transition. Effacement certifié des copies. Durée de conservation post-contrat limitée.

Gouvernance contractuelle

Comité de pilotage avec points sécurité obligatoires. Revue annuelle des clauses de sécurité. Droit d'adaptation en cas d'évolution réglementaire. Clause d'amélioration continue.

Points clés à retenir

La vulnérabilité juridique est aussi critique que la vulnérabilité technique

Un contrat mal rédigé ou des clauses inadaptées peuvent annuler tous vos efforts de sécurisation technique et vous exposer à des risques majeurs non couverts.

Les nouveaux cadres réglementaires imposent une gouvernance renforcée des tiers

NIS 2, DORA et RGPD créent des obligations légales de maîtrise de la Supply Chain. L'inaction n'est plus une option et expose à des sanctions.

Le contrat est votre premier outil de cybersécurité avec les tiers

Investir dans des clauses de sécurité robustes, des droits d'audit effectifs et une responsabilité adaptée est plus efficace que gérer un incident sans recours.

La maîtrise passe par une approche collaborative RSSI-juridique-achats

La sécurisation de la Supply Chain nécessite un dialogue permanent entre fonctions techniques, juridiques et achats pour traduire les exigences en clauses opposables.

Cécile Vernudachi — Avocate associée, Anders Avocats — Administratrice du Clusif

Q&A - Merci !

Contact

Cécile Vernudachi

Avocat Associé

134 boulevard Haussmann 75008 Paris

Général : +33 (0)1 53 81 50 40

cvernudachi @anders-avocats.com