L'impact de la LOPMI sur l'assurance cyber : ce qui change pour les entreprises et les assureurs

La loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) est entrée en vigueur le 24 avril 2023, marquant un tournant majeur en matière d'assurance du risque cyber pour les entreprises. Cette loi introduit l'article L12-10-1 dans le code des assurances français, qui aborde spécifiquement les risques de cyberattaques et leur assurabilité. Dans cet article, nous examinerons les conséquences de cette loi pour les entreprises en matière d'assurance cyber et les mesures à prendre pour être en conformité.

1. Obligation de dépôt de plainte

L'article L12-10-1 de la LOPMI impose aux victimes d'attaques informatiques malveillantes de porter plainte dans un délai de 72 heures à compter de la connaissance de l'attaque. Cette obligation s'applique tant aux personnes morales qu'aux personnes physiques exerçant une activité professionnelle.

Il est important de noter que la loi ne fait pas de distinction entre les systèmes de traitement automatisé de données hébergés ou gérés par l'assuré et ceux externalisés auprès d'un prestataire de services."La loi impose aux victimes d'attaques informatiques malveillantes de porter plainte pour préserver leur droit à indemnisation au titre de leur contrat d'assurance." -
La charge de la preuve repose sur l'assuré, il est donc recommandé de documenter minutieusement toutes les preuves et éléments relatifs à l'attaque.

2. Les atteintes concernées par l'obligation de dépôt de plainte

L'obligation de dépôt de plainte s'applique exclusivement aux atteintes malveillantes, telles que définies aux articles 323-1 à 323-3-1 du code pénal français. Les atteintes accidentelles du système d'information ne sont pas soumises à cette obligation. Il est donc crucial de faire la distinction entre les attaques malveillantes et les incidents purement accidentels afin de déterminer si le dépôt de plainte est nécessaire.

3. Les contrats d'assurance impactés par la LOPMI

La LOPMI modifie les conditions d'indemnisation des contrats d'assurance cyber. L'article L12-10-1 vise toute indemnité versée à un assuré en réparation des pertes et dommages causés par une atteinte malveillante. Les contrats d'assurance concernés comprennent notamment les contrats d'assurance cyber, les contrats de fraude, les contrats dommages couvrant les dommages consécutifs à une atteinte cyber, ainsi que les contrats Kidnap & Ransom (Assurances K&R).

4. Les entités concernées par l'obligation de dépôt de plainte

L'article L12-10-1 s'applique aux personnes morales et aux personnes physiques exerçant une activité professionnelle. Cela inclut les entreprises, les associations, les administrations publiques, ainsi que les professions libérales et les travailleurs indépendants. Il est également important de souligner que cette obligation s'applique aux entités étrangères victimes d'une atteinte et assurées par un contrat d'assurance de droit français.

5. Les modalités de dépôt de plainte

Le dépôt de plainte peut être effectué auprès de la police, de la gendarmerie ou du Procureur de la République. Dans le cas d'un dépôt de plainte auprès du Procureur de la République, il est recommandé d'envoyer la plainte par lettre recommandée avec accusé de réception. Il est important de noter que le pré-dépôt de plainte ne satisfait pas à la condition imposée par la loi, il est donc essentiel de respecter le délai de 72 heures à compter de la connaissance de l'atteinte.

La notion de "connaissance" n'est pas définie par la loi, mais il est généralement admis qu'il s'agit du moment où l'entité a la certitude de l'existence d'une atteinte à son système de traitement automatisé de données.

7. Les conséquences en cas de non-respect du délai de 72 heures

En cas de non-respect du délai de 72 heures pour le dépôt de plainte, l'assureur sera en droit d'invoquer une déchéance de garantie. Cela signifie que l'assuré risque de ne pas être indemnisé par son assureur en cas de sinistre.

8. Les programmes d'assurance master et les polices locales

Pour les contrats d'assurance master de droit français, la plainte doit être déposée auprès des autorités compétentes du pays où l'infraction a été constatée par l'assuré victime. Cependant, il est recommandé pour la société souscriptrice du programme d'assurance master français de déposer plainte auprès des autorités françaises dans le délai de 72 heures.

9. Les garanties de gestion d'incident / mesure d'urgence

Les garanties de gestion d'incident sont conçues pour prendre en charge les opérations d'assistance immédiatement après la cyberattaque : expert informatique, restauration des données, frais de monitoring et de surveillance, conseils juridiques…. Ces garanties ne sont pas censées être soumises au dépôt de plainte mais celles portant sur les pertes et dommages, qui n'ont pu être évités malgré les actions d'urgence, demeurent assujetties au dépôt de plainte.

Le dépôt de plainte sous 72 heures doit donc toujours être intégré à la stratégie de réponse à l'incident cyber des organisations.

L'entreprise doit l'intégrer et le positionner dans ses procédures d'urgences.

La LOPMI modifie les conditions d'assurance du risque cyber et impose des obligations de dépôt de plainte aux victimes d'attaques informatiques malveillantes. Les entreprises doivent se conformer à ces nouvelles exigences et prendre les mesures nécessaires pour protéger leurs intérêts.

La coopération entre les entreprises, les assureurs et les autorités compétentes est essentielle pour lutter efficacement contre la cybercriminalité et garantir une indemnisation adéquate en cas de sinistre.

21 aout 2023

Vos contats

Alain Rabouyt
01.53.04.22.78

Rosa Lecoquil
01.53.78.21.53