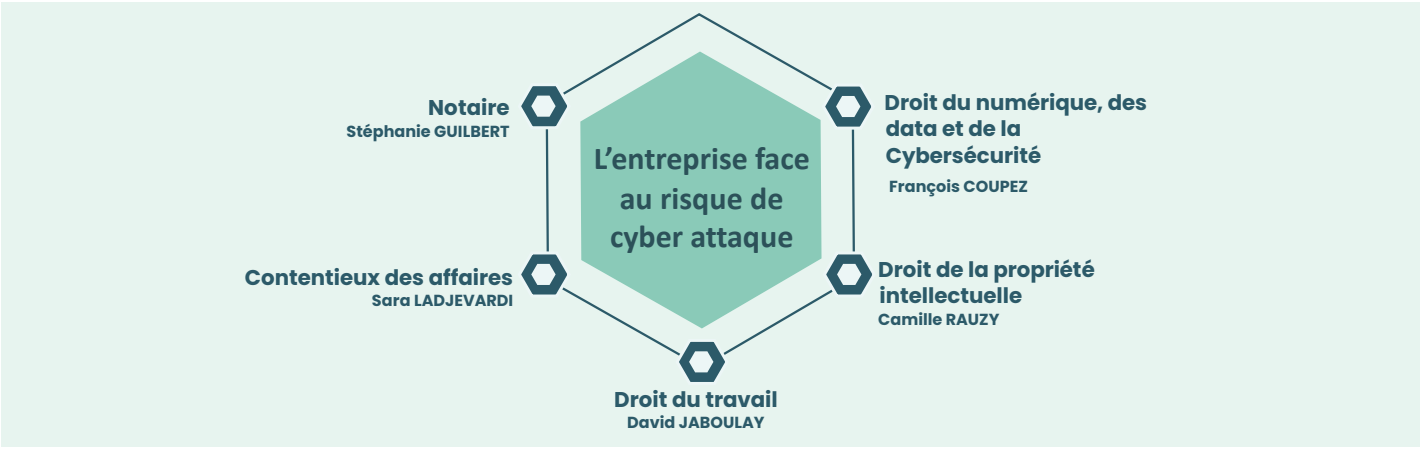
RÉSEAUMOLIÈRE
L'agilité d'experts indépendants du droit

L'entreprise face au risque de cyber attaque



ACTUS DU RÉSEAU

Bienvenue à Elodie CHRISTOPHE (droit social) qui rejoint le Réseau Molière à compter du 2 janvier 2024

Félicitations à Loanne DA SILVA (Level Up Legal) et Valentine GIRAY (Eclo) pour avoir récemment intégré la profession d'avocat !

NIS 2

Directive sur la Sécurité des Réseaux et des Infrastructures visant de nombreux secteurs d'activité
Elle sera transposée en France au 1er semestre 2024.

DORA

Règlement sur la résilience opérationnelle numérique dans le domaine financier, qui rentre en application en janvier 2025

Les deux textes prévoient des dispositions pour renforcer les obligations des entreprises face aux risques de cyber attaque.

Stéphanie GUILBERT
Notaire

Sara LADJEVARDI
Contentieux des affaires

Les 10 bonnes pratiques en matière de cybersécurité

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier (Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés).

Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques.

On vous donne les 10 bonnes pratiques essentielles à adopter pour assurer votre cybersécurité. :

1. Protégez vos accès avec des mots de passe robustes (au moins 12 caractères parmi lettres, chiffres, majuscules, caractères spéciaux ou une suite d'au moins 7 mots par exemple) et stockez-les au besoin dans un logiciel de coffre-fort de mot de passe spécifique (hors Chrome) ;

2. Sauvegardez vos données régulièrement ;

3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…) ;

4. Utilisez un antivirus et un pare-feu qui va filtrer les connexions à votre ordinateur ;

5. Téléchargez vos applications uniquement sur les sites officiels ;

6. Méfiez-vous des messages de personnes inconnues, vous demandant de cliquer sur un lien en particulier ou de vous communiquer des informations sensibles (mot de passe, etc.)

7. Ne faites des achats sur internet que via des sites de confiance, à la réputation établie et auxquels vous vous connectez directement ;

8. Maîtrisez votre expression sur les réseaux sociaux, vos propos engageant votre responsabilité ;

9. Séparez vos usages personnels et professionnels

10. Évitez de vous connecter à partir de réseaux WiFi publics ou inconnu, sauf à passer par un VPN de confiance.

Ces bonnes pratiques s'appliquent dans tous secteurs d'activité y compris au notaire. À titre d'exemple il doit brancher sa clé « Real » lui permettant d'authentifier ses actes uniquement en cas d'utilisation (signature) et, à défaut, la débrancher !

Il est indispensable de mettre en place des process en matière de cybersécurité pour être couvert par votre compagnie d'assurance en cas d'attaque cyber. En l'absence de mesure de sécurité, votre responsabilité peut se trouver engagée.

RÉSEAUMOLIÈRE
L'agilité d'experts indépendants du droit

L'entreprise face au risque de cyber attaque : pour que les salariés soient aussi responsabilisés

David JABOULAY
Droit du travail

En cas de cyber attaque d'une entreprise, les salariés peuvent faire l'objet de sanctions disciplinaires, pouvant aller du simple avertissement au licenciement pour faute grave.

Mais, pour activer son pouvoir disciplinaire et éviter au maximum les condamnations des juridictions sociales en cas de contentieux, l'employeur doit absolument se doter des outils juridiques destinés à contrôler l'utilisation par ses salariés des outils informatiques et numériques mis à leur disposition, et ce que le salarié travaille sur site ou en télétravail.

Ainsi, cette utilisation doit être encadrée par le règlement intérieur et une charte informatique (cf. article suivant).

Afin de sensibiliser les salariés à leurs obligations et aux limites de leurs libertés, il est recommandé d'insérer une clause de confidentialité dans chaque contrat de travail.

Les salariés doivent également suivre des formations régulières sur le thème de la cybersécurité. Plus particulièrement, le personnel stratégique doit bénéficier d'une information spécialisée dès sa prise de fonction, mais également, et de façon régulière, de formations renforcées à cet égard.

La charte d'usage des outils numériques, outil indispensable de l'entreprise

François COUPEZ
Droit de la Cybersécurité et des Data

L'entreprise, confrontée à des cyber-risques croissants d'une part, et à une réglementation de plus en plus stricte de l'autre, se doit aujourd'hui plus encore qu'hier de se doter d'outils, procédures et logiciels afin d'assurer sa cybersécurité. Tant les régulateurs (ANSSI, CNIL, etc.) que les normes techniques reconnues (ISO 27001) imposent de s'assurer que ces règles sont connues du personnel et, surtout, peuvent leur être effectivement opposables en cas de non-respect.

C'est le rôle de la charte d'usage des outils numériques (charte informatique, ou titre similaire), **annexée au règlement intérieur de l'entreprise.** Ce document hybride, aussi bien technique que juridique, est la colonne vertébrale de l'application des règles internes : toute formulation doit être très soigneusement choisie au risque de restreindre de façon drastique les contrôles que l'employeur serait en droit de faire. **Sa rédaction doit donc être l'objet de toutes les attentions et pensée à l'aune des centaines de décisions de justice qui la guide. Bien rédigée, exhaustive (règles d'usage d'IA, d'outils cloud, de décès d'un salarié, etc.), elle guide les bons comportements et permet une répression efficace des violations de sécurité.** De plus, elle peut être adaptée afin de faire lien avec l'encadrement contractuel des prestataires informatiques.

UN RÉSEAU INTERPROFESSIONNEL
Un interlocuteur spécialisé pour toutes vos problématiques

DROIT PUBLIC
Parisi avocats

CONTENTIEUX DES AFFAIRES
Sara Ladjevardi

IMMOBILIER
Marie Pochon

PROPRIÉTÉ INTELLECTUELLE
Camille Rauzy

DROIT DES SOCIÉTÉS
Eclo Avocats
Rollux Champliaud Dauphin
Magalie Revillon Persat

FISCALITE
Grégory Vincent

DROIT DU TRAVAIL
David Jaboulay
Elodie Christophe

NOTAIRE
Etude Notaires Molière

DROIT DES PERSONNES
Caroline Brun

NUMÉRIQUE, DATA & CYBERSÉCURITÉ
Level Up Legal

PROFESSIONS LIBÉRALES
Rollux Champliaud Dauphin
Eclo Avocats

ENTREPRISES EN DIFFICULTÉ
Dehlila Micoud
Eclo Avocats

RÉSEAUMOLIÈRE
L'agilité d'experts indépendants du droit

Quand la cybersécurité impose un renforcement drastique des clauses contractuelles

François COUPEZ et Anne-Laure PONS POLINE
Droit de la Cybersécurité et des Data

Si une charte d'utilisation des moyens de communication permet à l'entreprise de se défendre efficacement contre les risques cyber endogènes, il convient également de protéger l'entreprise contre les menaces exogènes, c'est-à-dire provenant principalement de sa chaîne d'intervenants extérieurs.

En effet, de multiples prestataires de services sont amenés à se connecter au système d'information d'une entreprise, que ce soit parce qu'ils fournissent les prestations informatiques (messagerie électronique, solutions cloud, etc..), qu'ils doivent interagir avec l'entreprise (connexion à un portail fournisseur, etc.) ou tout simplement parce qu'ils travaillent au sein de l'entreprise et accèdent à ses données (développeurs informatiques, consultants, etc.).

À la lecture tant des textes applicables aujourd'hui (ex : articles 28 et 32 du RGPD) et demain (DORA, NIS 2 – cf. première page de cette newsletter) que des décisions des autorités de contrôle (CNIL, etc.), un encadrement contractuel strict est indispensable. **Les régulateurs sanctionnent de plus en plus fréquemment les manques en ce domaine et accroissent fortement leur niveau d'exigence quant au contenu que ces clauses contractuelles dédiées doivent prévoir.**

Celles-ci doivent être détaillées et finement adaptées, tant d'un point de vue opérationnel que juridique, au type de service rendu et au niveau de risque découlant de l'analyse de risque préalablement effectuée.

En pratique, cet encadrement doit être envisagé dès la phase de sélection du prestataire, afin que celui-ci puisse connaître et prendre en considération ces exigences dès l'origine.

Typosquatting : jouer malhonnêtement avec l'inattention d'autrui – comment réagir ?

Camille RAUZY
Droit de la propriété intellectuelle

Le typosquatting est le fait de réserver un nom de domaine très proche de celui d'autrui afin de créer une confusion dans l'esprit de la clientèle qui, par inattention, ne percevra pas la différence entre molière.com et molièr.com.

Parmi les divers objectifs poursuivis, l'on trouve :

- Au mieux : diriger la clientèle vers un site concurrent ;
- Au pire : l'escroquerie par exemple via la création d'une adresse email très proche de celle d'un membre de la société pour notifier un changement de RIB et obtenir des paiements de la part de clients.

Face à une telle attaque, plusieurs actions doivent être engagées pour protéger votre société et vos clients :

1. Contacter le registrar du nom de domaine pour obtenir sa suspension et toute information sur son réservataire ; suivant la gravité des faits et la nationalité du registrar, il sera plus ou moins coopératif ;

2. Engager une procédure administrative pour obtenir le transfert du nom de domaine à votre bénéfice (et non son annulation qui le rendrait à nouveau disponible à l'achat) ;

2bis. Alternativement ou cumulativement, engager une action judiciaire contre le réservataire du nom de domaine, en contrefaçon, et/ou concurrence déloyale et/ou parasitisme ou, faute de pouvoir l'identifier, déposer une plainte pénale pour qu'une enquête soit ouverte.

Les atouts du réseau Molière mettent de la magie dans votre année 2024...

Et vous souhaitent une excellente nouvelle année !

Nous vous invitons à cliquer sur l'image pour découvrir ce que nous vous avons réservé...