Mathias | Avocats

SÛRETÉ BÂTIMENTAIRE : IDENTIFIER LES RISQUES EN CAS DE DÉFAILLANCE ET ADOPTER LES BONNES PRATIQUES

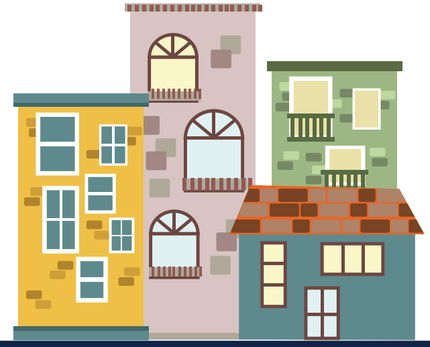
CE DOCUMENT EST FOURNI À TITRE PUREMENT INFORMATIF ET NE CONSTITUE EN AUCUN CAS UN CONSEIL JURIDIQUE

CONTACT@AVOCATS-MATHIAS.COM

WWW.AVOCATS-MATHIAS.COM

Mathias | Avocats

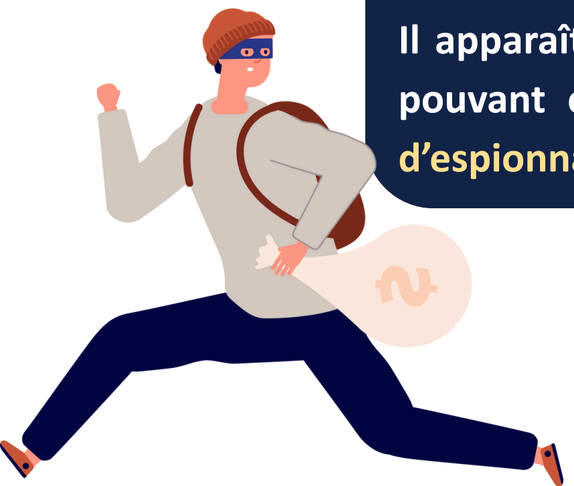
SÛRETÉ BATIMENTAIRE : IDENTIFIER LES RISQUES EN CAS DE DÉFAILLANCE ET ADOPTER LES BONNES PRATIQUES

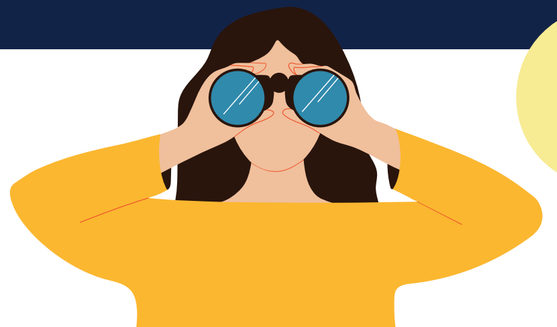


Les organisations sont de plus en plus confrontées à des menaces provenant d'acteurs aux profils multiples. Bien que les risques cyber soient de manière générale bien identifiés, les menaces issues de failles dans la sécurité physique sont parfois négligées, ouvrant alors la voie à des actions malveillantes.

En ce sens, toute organisation doit établir une politique de sécurité, en prenant en compte l'intégralité des risques auxquels elle peut être exposée, qu'ils soient internes ou encore externes.

Il apparaît donc crucial d'adopter une politique de sûreté bâtimentaire, afin de limiter les risques d'intrusion, pouvant conduire à des vols d'information ou de matériel sensible, de dégradation ou encore des actes d'espionnage.





RISQUES LIÉS AUX DÉFAILLANCES EN MATIÈRE DE SÛRETÉ BÂTIMENTAIRE

Mathias | Avocats

EXEMPLES D'INTRUSIONS

Intrusion nocturne d'un individu dans un site sensible placé sous alarme par une porte laissée non-verrouillée

Un individu s'est introduit de nuit dans une infrastructure sensible par une entrée secondaire restée ouverte. Bien qu'il n'ait pas commis de vol ni de dégâts, ce dernier a pris plusieurs photos suspectes, suggérant un possible repérage. L'incident, rapidement détecté grâce à la vidéosurveillance et au gardiennage, souligne **l'importance de vérifier systématiquement la fermeture des accès pour éviter de telles intrusions.**

Vol d'ordinateurs et de disques durs au sein d'un centre de recherche en raison d'une sûreté bâtimentaire insuffisante

Un centre de recherche a subi, durant les vacances universitaires, un vol mené par des individus ayant contourné les dispositifs anti-intrusion. Plusieurs ordinateurs et disques durs non chiffrés ont été dérobés. L'établissement **a porté plainte, renforcé la surveillance et envisagé l'extension des systèmes de sécurité.**

Vol par effraction au sein des locaux d'une entreprise sensible, dépourvue de systèmes de détection et de protection

Lors d'un week-end prolongé, des individus ont cambriolé le site d'une entreprise stratégique en accédant à des bureaux non sécurisés et ont volé du matériel et des données sensibles. **L'entreprise a porté plainte et renforcé la sécurité de ses locaux.**

RISQUES LIÉS AUX DÉFAILLANCES EN MATIÈRE DE SÛRETÉ BÂTIMENTAIRE

RENFORCER LA RÉSILIENCE PHYSIQUE : LA DIRECTIVE REC

Face à ces menaces, la directive « REC » vise à réduire les vulnérabilités et à renforcer la résilience physique des entités critiques, qui sont définies par ladite directive (en annexe) et qui, plus généralement « fournissent des services indispensables pour maintenir les fonctions sociétales vitales, les activités économiques, la santé et la sécurité publiques ainsi que l'environnement ».

La directive « REC » précise que « La sécurité physique et la cybersécurité des entités critiques étant liées, les États membres veillent à ce que la présente directive [Directive REC] et la directive (UE) 2022/2555 [Directive NIS 2] soient mises en œuvre de manière coordonnée ». (article 1, 2. Directive REC)

Consulter notre article sur la directive "REC"

La directive dite « NIS 2 », concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, vise quant à elle à répondre aux mêmes préoccupations en ce qui concerne la dimension cyber.

Consulter notre article sur la directive NIS 2

Mathias | Avocats

QUELQUES PRÉCONISATIONS

Effectuer un bilan des dispositifs de sûreté existants

- Effectuer un audit de sûreté bâtimentaire
- Effectuer des tests d'intrusion physique pour évaluer son dispositif de sûreté
- Réévaluer périodiquement les processus de sécurité

Instaurer des mesures de protection adaptées au niveau de sensibilité des locaux

- Mettre en place des mesures élémentaires d'ordre organisationnel visant à contrôler les accès aux différents espaces
- Renforcer les protections extérieures du site
- Envisager d'installer un système de détection d'intrusion pour protéger l'intérieur des locaux

En cas d'incident lié à une intrusion physique :

- Déposer plainte auprès des services de police ou de gendarmerie
- Contacter la DGSI afin de signaler l'incident

RISQUES LIÉS AUX DÉFAILLANCES EN MATIÈRE DE SÛRETÉ BÂTIMENTAIRE

Mathias | Avocats

Besoin d’une veille juridique sur mesure ?

Sur les thématiques qui vous intéressent, sur votre secteur d’activité, votre métier, les nouvelles exigences / le cadre juridique de vos missions, vos opportunités…

NOUS CONTACTER

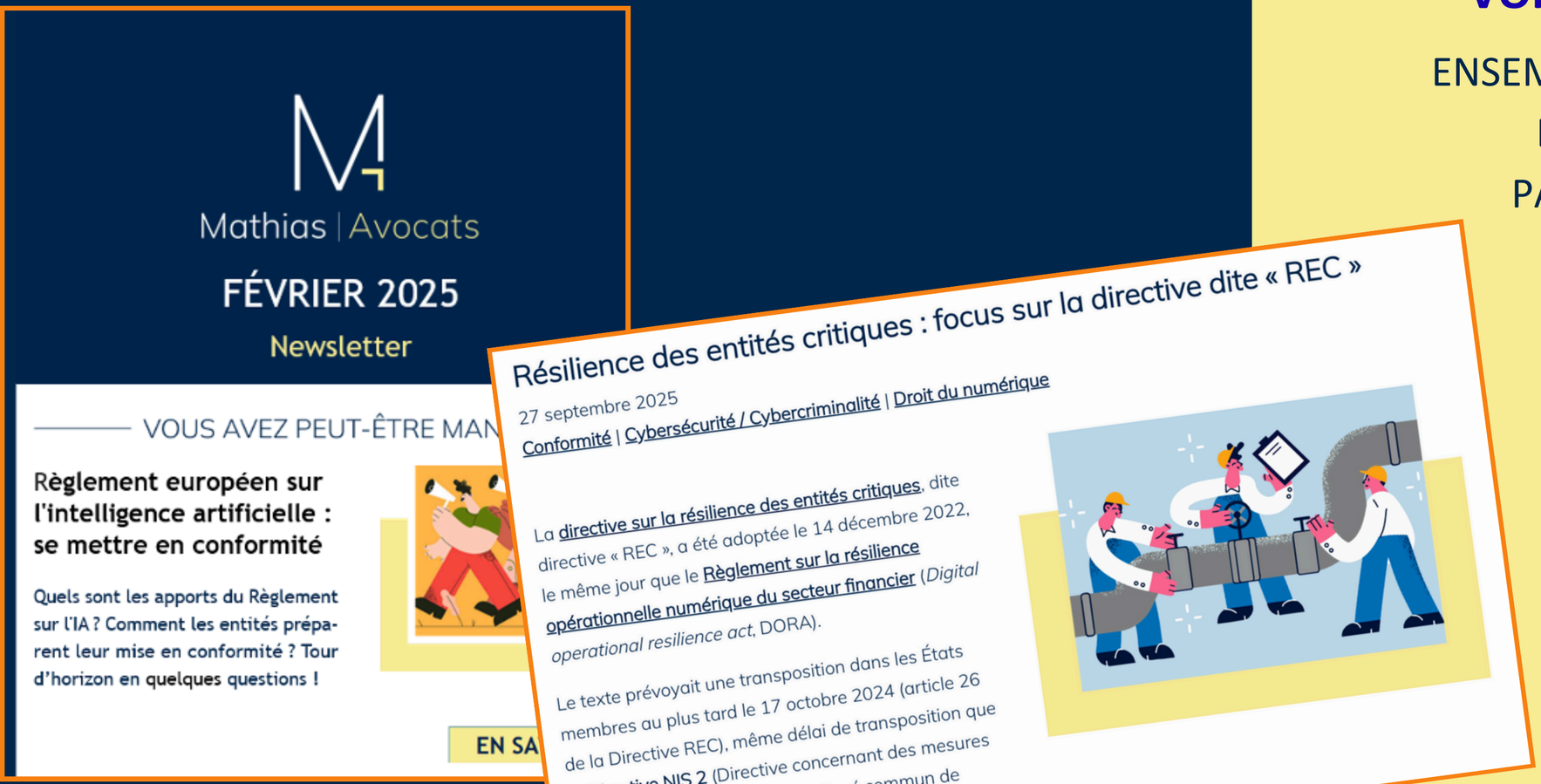
Mathias Avocats réalise des veilles sur-mesure pour ses clients, selon les thématiques sélectionnées, secteurs d’activités, métiers.

- **Une veille pour vous et vos équipes, chaque mois dans votre boîte mail**
- **Contenu, Format, Périodicité, Tarif : contactez-nous !**

Mathias | Avocats

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE



L'ACTUALITÉ DÉCRYPTÉE POUR VOUS !

VOIR LES ARTICLES DU BLOG

ENSEMBLE, DÉVELOPPONS VOS PROJETS
ET FORMONS VOS ÉQUIPES !
PARTAGEONS NOS EXPERTISES !

AU QUOTIDIEN

CATALOGUE DES FORMATIONS

Mathias | Avocats

CONTACTEZ-NOUS !

19 rue Vernier 75017 PARIS

+33 (0)1 43 80 02 01

contact@avocats-mathias.com

https://www.avocats-mathias.com/

@MathiasAvocats