Avocat Cybersécurité Cyberdéfense

Le cyberespace est l'espace de communication virtuel dans lequel s'inscrit le droit de la cybersécurité et de la cyberdéfense.

Le cyberespace est devenu le cinquième champ de conflictualité après la terre, la mer, l'air et l'espace.

Le besoin de sécurité globale du citoyen et de l'entreprise entraîne également une augmentation des contrôles et donc une possible violation des libertés individuelles. C'est pourquoi, il est nécessaire d'accompagner toute démarche de cybersécurité et de défense cyber d'un encadrement juridique.

Le droit de la cybersécurité adresse tous les risques et toutes les menaces volontaires d'origine humaine qui sont susceptibles de porter atteinte aux différents patrimoines (technologique, scientifique, économique, image) de l'entreprise. La cybersécurité consiste dans la recherche d'un état pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait donc appel à des techniques de sécurité de systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Le droit de la cyberdéfense investit le champ des exigences de sécurité qui s'impose aux opérateurs de services essentiels (OSE) qui doivent prendre les mesures techniques et organisationnelles nécessaires, proportionnées et adaptées à la gestion des risques menaçant la sécurité des réseaux et systèmes

Ils nous font confiance

Droit et technologie

Action de groupe

Acoustique

Activités spatiales

Aéronautique

Agriculture numérique

Algorithme prédictif

Application mobi

Authentification d'oeuv

d'informations essentiels au maintien d'activités économiques et sociales critiques. Les modes d'attaques des systèmes d'informations et des réseaux sont de plus en plus ciblés et complexes et sont rendus possibles par l'utilisation de technologies. La France a identifié environ 200 opérateurs d'importance vitale répartis sur 12 secteurs et sous-secteurs.

Les entreprises doivent prendre en compte le risque cybersécurité. Pour ce faire, les entreprises doivent mettre en œuvre une veille spécifique pour identifier les cybermenaces sur leurs activités. C'est à cette condition, que les dirigeants seront en mesure d'anticiper et de réagir aux différentes cybermenaces pesant sur leurs activités.

Avocat spécialiste en cybersécurité cyberdéfense

Sommaire

- Cyberespace
- Cyberpiratage
- Cyberrisques
- Directive NIS
- Pacte Défense Cyber
- Robotique et cybersécurité
- Vulnérabilités et menaces

L'entreprise face aux menaces dans le cyberespace : une démarche volontaire.

Les entreprises sont quotidiennement victimes de nouvelles formes de vulnérabilités :

- acte contrevenant aux traités internationaux ou aux lois nationales effectué dans le cyberespace ou au moyen d'un système informatique : cybercriminalité ;
- piratage informatique qui permet d'accéder à des informations tenues secrètes. L'objectif est d'en

Autoroute intelligente
Avatar
Banque et bourse électroniques
Base de données
Big data
Blockchain
Brevet
Biométrie
Centre de données
Cerveau artificiel
Cloud computing
Concurrence Consommation
Contract management
Cybersécurité Cyberdéfense
Crowdsourcing
Data Protection Officer
Dématérialisation
Dessins et modèles
Domotique

tirer un avantage personnel, économique, patrimonial : cyberespionnage ;

- acte de terrorisme utilisant des systèmes informatiques ou la technologie des ordinateurs comme une arme ou comme une cible (...). Le cyberterrorisme a des motivations politiques, sociales ou religieuses, il vise à semer la peur ou la panique dans la population civile ou à déstabiliser l'appareil militaire et civil. : cyberterrorisme ;
- risques de guerre informatique exposant les entreprises qui sont sur le territoire d'Etat étranger dans lequel un conflit classique dont au moins une des composantes, dans la réalisation, les motivations et les outils (armes au sens large du terme) s'appuie sur le champ informatique ou numérique. Il est évoqué le terme de « cyberattaque » (Source : Eric Filiol, auteur et expert en sécurité informatique et ancien militaire). Si l'objectif de cette guerre informatique est politique : sa cible les militaires, un Etat (et ses infrastructures) ou une société et ses équipements informatiques.

De nombreuses installations industrielles fonctionnent grâce à des systèmes de contrôle et d'acquisition de données (SCADA en anglais). Quel que soit le secteur d'activité de l'entreprise, l'énergie, les transports, la santé, et jusqu'à ce que les dispositifs de contrôle et d'acquisition de données soient conçus en adoptant une logique de « Secure by design », ces dispositifs font naître des vulnérabilités face aux enjeux de cybersécurité ou de cyberdéfense.

Définir vos objectifs stratégiques en matière de cybersécurité

Parmi les menaces majeures auxquelles toute entreprise sera confrontée, il convient de retenir les cyberattaques informatiques et les cybermenaces contre les systèmes d'information et les données de l'entreprise.

Pour se prémunir, chaque entreprise doit adopter sa propre stratégie de cybersécurité afin de définir ses objectifs stratégiques. Dans la stratégie de toute entreprise, les objectifs stratégiques qui devraient être pris en compte sont les suivants :

- garantir la sécurité de l'ensemble de vos systèmes d'information ;
- maintenir et renforcer la sécurité de vos systèmes d'information les plus critiques ;
- engager une réflexion et un travail de sensibilisation de l'ensemble de l'entreprise au risque cybersécurité.

Données publiques
Drone
E-cosmétique
E-réputation
E-sport
Energie et environnement
Evaluation de préjudices
Expertise juridique
Fabrication additive Impression 3D
Failles de sécurité
Fiscalité et Société
Génie urbain numérique
Génie génétique
Grands systèmes informatiques
Informatique
Informatique embarquée
Informatique et international
Informatique et libertés conseil
Informatique et libertés

Définir vos axes d'effort en fonction de votre politique globale de sécurité et de cybersécurité

Après avoir définis vos objectifs stratégiques en matière de cybersécurité, toute entreprise devra nécessairement évaluer ses axes d'effort par rapport à sa stratégie et politique de sécurité et de cybersécurité.

Pour atteindre les objectifs d'une stratégie de sécurité, l'entreprise doit se concentrer sur de nombreux axes d'efforts en fonction de l'évaluation faite par chaque entreprise.

Les axes d'efforts communs au monde de l'entreprise que nous avons identifiés quel que soit le secteur d'activité sont les suivants :

- mieux anticiper et analyser l'environnement afin de prendre des décisions adaptées ;
- détecter les attaques et les contrer, alerter les autorités et vous faire accompagner si nécessaire ;
- accroître et pérenniser vos capacités scientifiques, techniques, industrielles et humaines dans l'objectif de conserver l'autonomie nécessaire pour prendre en charge et faire face aux menaces cyber ;
- protéger l'ensemble de vos systèmes d'information et en particulier vos systèmes d'information critiques et essentiels pour une meilleure résilience ;
- prendre en compte les évolutions technologiques et les nouveaux usages ;
- communiquer, informer et sensibiliser l'ensemble des acteurs de l'entreprise afin de permettre aux dirigeants de prendre les bonnes décisions en matière de sécurité des systèmes d'information.

Expertise avocat cybersécurité cyberdéfense

Notre expertise et nos compétences nous permettent d'anticiper, d'analyser et d'évaluer les risques, afin de vous permettre de pérenniser et renforcer votre stratégie de cybersécurité mais aussi de défendre contre les conséquences dommageables sur les patrimoines et l'image de votre entreprise, en cas de dommages portés aux réseaux et systèmes d'information de votre entreprise.

contentieux
Intelligence artificielle
Intelligence économique
Interfaces homme machine
Internet contentieux
Internet et droit
Internet des objets
Jeux vidéo
Marchés publics
Marques et noms de domaine
Média
Mode et luxe
Moyens de paiement
Navigation intelligente
Objets communicants
Optique
Paiement mobile
Pénal numérique
Plateforme technologique de paiement

Le cabinet est distingué Law Firm of the Year pour l'année 2017 dans la catégorie Technologies de l'Information pour la France par la revue américaine « Best Lawyers« . Cette distinction fait suite à la désignation d'Alain Bensoussan comme Lawyer of the Year de 2011 à 2015 dans les catégories Nouvelles Technologies et Droit des Technologies.

Prestations avocat cybersécurité cyberdéfense

Anticiper

Les missions réalisées poursuivent l'objectif de vous permettre de développer une action d'anticipation et d'analyse des risques :

- définition de plan de veille et d'anticipation des menaces cyber ;
- identification des modes opératoires de collecte, d'analyse, de valorisation, de diffusion et de protection de l'information économique stratégique.

En fonction de votre domaine d'activité et de votre plan de veille stratégique et de vos besoins, nous travaillons avec un réseau de correspondants spécialisés en matière d'intelligence économique.

Analyser et évaluer

L'évaluation des risques a pour objectif de vous permettre de définir ou d'adapter votre stratégie globale de cybersécurité aux risques et aux vulnérabilités relatives au patrimoine technologique, scientifique, économique de votre entreprise, aux données stratégiques de votre entreprise mais aussi à l'image de votre entreprise.

Elle comprend les prestations suivantes :

- audit flash des risques de sécurité globale ;
- audit flash des risques et menaces Cyber ;

Politique P3P
Propriété intellectuelle
Publicité – Marketing électronique
Quantified self
Réalité virtuelle
RFID
Risques technologiques, industriels et sanitaires
Robot et droit
Santé
Sécurité des systèmes d'information
Serious game
Start-up
Technologie des déchets
Technologies policières
Télécoms et droit
Télémédecine
Textile intelligent

- cartographie des risques avec validation préalable des enjeux de sécurité globale pour l'entreprise ;
- notes d'alertes et de notes de recommandations sectorielles ;
- note de ciblage des risques cyber ;
- mise en place et tenue d'un registre des failles de sécurité.

Pérenniser et renforcer

Les missions comprennent :

- la définition de la politique d'intelligence économique d'une entreprise ;
- la définition de la charte de gouvernance des systèmes d'information ;
- la définition de la politique globale de sécurité de l'entreprise ;
- l'analyse, l'identification des faits générateurs de risques de sécurité et la hiérarchisation des risques ;
- la définition, la mise en place de politique de formation et de sensibilisation aux risques cyber de l'ensemble des acteurs de l'entreprise à la cybersécurité ;
- l'audit des contrats avec les concepteurs de produits informatiques et de systèmes d'information afin de s'assurer qu'ils ont pris en compte les questions de sécurité dès l'origine de leurs développements.

Défendre

Il s'agit de la réalisation de toutes actions contentieuses en cas d'atteintes ou d'infractions commises via les réseaux et systèmes d'informations de l'entreprise aux patrimoines technologique, scientifique, économique de l'entreprise.

Nous intervenons pour assister les entreprises de tous secteurs d'activités, souhaitant obtenir réparations pour les atteintes ou infractions portées via leurs systèmes d'informations de toutes natures, technologiques, de gouvernance, de management, de conformité, ainsi que pour tirer parti de la montée en puissance de la norme internationale et européenne.

Tourisme numérique
Train intelligent
Travail numérique
Ville intelligente
Voiture intelligente
Voiture volante

Communiqué

Informations légales

Notice légale
Politique cookies
Politique de protection des données
Téléright

Nous contacter

Lexing Alain Bensoussan Avocats
Immeuble Cap Etoile
58 boulevard Gouvion-Saint-Cyr
75017 Paris
paris@lexing.law
Tél. : +33(0)1 82 73 05 05

International

En s'appuyant sur son réseau international Lexing® et son réseau de correspondants dans le monde entier, le cabinet intervient pour des entreprises multinationales et peut vous mettre en relation avec l'un des membres du réseau.

Equipe avocat cybersécurité cyberdéfense

L'équipe est composée d'avocats spécialisés dans l'identification, la compréhension, la maîtrise des risques et menaces cyber : directeurs et collaborateurs seniors sont orientés selon les deux axes conseil et contentieux. Le cabinet intervient sur le site du client si la nature de la prestation le nécessite et peut constituer de manière immédiate une cellule de gestion de risques en cas de besoin.

Espace d'information avocat cybersécurité cyberdéfense

L'espace d'information de ce site est structuré en 3 parties : la réglementation applicable à la cybersécurité et la cyberdéfense, des thématiques tenant compte de la diversité des risques et des menaces et la jurisprudence accessible à partir d'un tableau.

Chaîne YouTube avocat cybersécurité cyberdéfense

Toutes nos vidéos sont diffusées sur notre chaîne Lexing Alain Bensoussan-Avocats. Abonnez-vous gratuitement.

Fax : +33(0)1 82 73 05 06
Mob. : +33 (0)6 19 13 44 46

Serment de l'avocat

Je jure, comme Avocat, d'exercer mes fonctions avec dignité, conscience, indépendance, probité et humanité.

Communiqué

Informations légales

DPO
ale
ookies
le confidentialité Chatbot
le protection des données
Téléright

Nous contacter

Lexing Alain Bensoussan Avocats
Immeuble Cap Etoile
58, boulevard Gouvion-Saint-Cyr
75017 Paris
paris@lexing.law
Tél. : +33(0)1 82 73 05 05
Fax : +33(0)1 82 73 05 06
Mob. : +33 (0)6 19 13 44 46

Serment de l'avocat

Je jure, comme Avocat, d'exercer mes fonctions avec dignité, conscience, indépendance, probité et humanité.

Accueil
Cabinet
Evénement
Formation
Observatoire
Plateforme SaaS
Boutique juridique
Informatique et libertés
DPO Profession Avocat
Conseils juridiques téléphoniques
Avocats

Publication
Réseau Lexing
Revue de Presse
Nous contacter

Notice légale | Crédit photo | Plan du site