*Analyse Sectorielle*

*Avril 2024*

CROSS CHANNEL INSTITUTE

*for the promotion of Franco - British sustainable prosperity*

# Cybersecurité

## *Alliance franco-britannique*
## *Les Grands Défis*

FRANCO BRITISH Chamber

# Sommaire

# Introduction

*Olivier Campenon,*
*Chairman of the Cross-Channel Institute,*
*CEO, Group Lefebvre*

Cette analyse sectorielle dédiée aux **enjeux de la cybersécurité dans les relations commerciales franco-britanniques**, est une étude commandée par le Cross-Channel Institute, le think tank apolitique et indépendant de la Chambre de Commerce franco-britannique. L'étude se penche sur les défis auxquels sont confrontées les entreprises dans le paysage de la cybersécurité en 2024, en mettant l'accent sur l'ère de la polycrise, les menaces liées à l'IA, les ransomwares et la multi-extorsion, l'adoption du cloud et les risques liés à la chaîne d'approvisionnement, ainsi que sur l'intensification des réglementations.

L'étude fournit des indications précieuses sur la façon dont les entreprises et les organisations peuvent se préparer à ces menaces et favoriser la résilience. En outre, le document examine minutieusement les cadres réglementaires et les obstacles à la conformité auxquels sont confrontées les organisations opérant dans les deux pays. Il met également en évidence la poursuite de la collaboration et du dialogue transfrontaliers sur les questions de cybersécurité. Malgré certaines disparités et divergences, le document affirme qu'une trajectoire mutuelle et une ambition partagée de sauvegarder et de libérer de la valeur en favorisant un cyberespace plus sûr pour le commerce sont évidentes.

Par ailleurs, cette analyse accorde une attention particulière au concept de gouvernance de la cybersécurité. Ce processus - le contrôle et la direction des activités de cybersécurité d'une organisation - est développé. Le document examine l'importance de la gouvernance de la cybersécurité pour la résilience des entreprises, détaille certaines des principales caractéristiques d'une gouvernance efficace et décrit les approches et les défis actuels au Royaume-Uni et en France. Il examine également les tendances futures et les meilleures pratiques en matière de gouvernance de la cybersécurité, telles que la norme ISO/IEC 27001, le code de pratique britannique en matière de cybergouvernance et les ramifications de l'IA.

En conclusion, bien que ce document ne prétende pas être exhaustif, il vise à servir de ressource fiable pour aider les entreprises et les organisations à mettre en œuvre et à maintenir durablement des mesures de cybersécurité efficaces, en particulier pour les entités engagées dans des échanges commerciaux entre le Royaume-Uni et la France.

# Cybersécurité : Un Partenariat Franco-Britannique Stratégique.

*Ministère de l'Europe et des Affaires étrangères*

Tout au long des 120 années d'Entente cordiale, la France et le Royaume-Uni ont travaillé de concert dans les domaines stratégiques traditionnels : la terre, la mer, l'air et l'espace. Désormais, l'importance croissante du cyberespace pour la sécurité et la prospérité de nos sociétés a conduit nos deux pays à investir dans la cybersécurité afin d'en tirer toutes les opportunités et de surmonter les défis soulevés par l'ère numérique. Dans un monde plus complexe, interconnecté et volatile, la cybersécurité est devenue une dimension essentielle de la relation franco-britannique. Dans ce contexte en constante évolution, nos deux pays peuvent s'appuyer sur une proximité stratégique de longue date, inscrite dans l'Entente cordiale et les traités de Lancaster House de 2010.

120
ENTENTE CORDIALE
1904 • 2024

En mars 2023, le 36e Sommet franco-britannique a réaffirmé l'amitié et le partenariat qu'entretiennent nos deux pays depuis de longues années et scellé une vision commune de l'avenir, y compris dans le domaine cyber. Au-delà des célébrations de nos liens diplomatiques étroits tout au long de l'année, il ne fait aucun doute que 2024 est et sera pour nos deux pays une année des enjeux cyber. L'existence d'intérêts communs a été illustrée au plus tard le 6 février par le lancement officiel du processus de Pall Mall, une initiative internationale conjointe visant à lutter contre la prolifération et l'utilisation irresponsable des capacités commerciales d'intrusion cyber, dans le bâtiment historique de Lancaster House à Londres.

Le dialogue cyber annuel France – Royaume-Uni a bénéficié d'un nouvel élan en 2023. Ce format nous permet de faire le point sur notre coopération et de construire une vision commune pour l'avenir de nos projets communs et respectifs. Des deux côtés de la Manche, nous partageons la volonté de faire respecter le cadre normatif de comportement responsable des États dans le cyberespace, fondé sur le droit international, et de promouvoir un cyberespace libre, ouvert, inclusif, non fragmenté et sécurisé. Dans cette optique, nous renforçons notre coordination au sein des Nations Unies. Au niveau bilatéral, nous échangeons régulièrement sur l'évolution du panorama de la menace cyber, soulignant ainsi notre compréhension commune de menaces spécifiques, y compris le marché des capacités d'intrusion cyber, qui pourrait être utilisé à des fins offensives. La coopération entre nos deux pays est également essentielle pour assurer la cybersécurité des grands événements, d'autant plus que les Jeux Olympiques et Paralympiques se dérouleront à Paris dans quelques mois.

Au fil des années, la France et le Royaume-Uni ont également développé leurs propres modèles de gouvernance de la cybersécurité qui continuent d'être une source d'inspiration mutuelle et un élément d'intérêt pour les entreprises désireuses de se faire une place sur les deux marchés.

En tant que membre du marché unique européen, la France participe activement à l'élaboration des réglementations (*directive NIS2, Cyber Resilience Act, Cybersecurity Act, Cyber Solidarity Act*) et des stratégies de l'Union *(EU Cybersecurity Strategy)*. En exigeant le renforcement de la cybersécurité pour les institutions, les infrastructures critiques et les produits dans l'ensemble de l'UE, ces règlements garantissent notre protection commune et offrent des opportunités de marché au secteur de la cybersécurité. En outre, cette dernière est l'une des priorités des investissements pour l'avenir de l'Union de la Commission européenne : le budget à long terme de l'UE, associé à *NextGenerationEU*, inclus des investissements supplémentaires dans la cybersécurité, tout comme divers programmes d'investissements (*Digital Europe Programme, InvestEU*) et de soutien à la recherche et à l'innovation dans le cadre d'Horizon Europe.

Dans ce contexte, la France reste la première destination européenne pour les projets d'investissements directs étrangers en 2023 selon l'*EY Attractiveness Report Europe*, confirmant ainsi l'attractivité de l'innovation et de l'environnement économique français. Le plan d'investissement "France 2030" comprend une stratégie nationale d'accélération pour la cybersécurité d'un milliard d'euros, qui vise à développer des solutions souveraines et innovantes de cybersécurité, à renforcer les liens et synergies entre les acteurs de la filière, à soutenir la demande en sensibilisant à la cybersécurité et à former une nouvelle main-d'œuvre aux métiers de la cybersécurité.

L'écosystème florissant de la cybersécurité en France reflète celui du Royaume-Uni, puisque le NCSC évalue la contribution du secteur britannique de la cybersécurité à l'économie à 10 milliards de livres. Grâce à une expertise cyber de pointe, les deux marchés connaissent une croissance rapide. Dans ce domaine concurrentiel en constante évolution, nous encourageons les acteurs privés à tirer le meilleur parti des opportunités existantes et à en créer de nouvelles. A cette fin, nous pensons que la France et le Royaume-Uni ont tout à gagner à encourager le développement d'entreprises et d'organisations de premier plan pour renforcer la confiance et la sécurité dans le cyberespace et dans l'ensemble de nos sociétés. Vive l'Entente cordiale !

*Ministère de l'Europe et des Affaires étrangères*

Dans un cadre sécuritaire de plus en plus incertain, les grandes entreprises doivent s'équiper de dispositifs d'alerte, de restauration et de nettoyage de leur Système d'Information. La réglementation européenne DORA impose déjà un certain nombre d'actions chez les grandes entreprises et nous pouvons imaginer que le dispositif sera étendu outre-manche.

Dans ce contexte Infotel a développé des logiciels et services Cyber aussi bien en France qu'en Grande-Bretagne pour ses clients.

**Nettoyage et Résilience**

*Qui veut cambrioler une maison vide ?*

Parmi les solutions développées, le logiciel **Deepeo** permet le nettoyage des données sensibles et des données personnelles. Il permet également d'anonymiser des données en production au sein du SI.

*L'attaque Cyber étant toujours possible.*

Les systèmes bancaires étant particulièrement visés par les risques Cyber, Infotel distribue et installe un **système de surveillance** pour les grands SI des Banques et Assurance. Pour garantir la résilience de nos entreprises, il est impératif de savoir détecter au plus vite les attaques et leurs cibles, afin de redémarrer les systèmes dans l'état originel le plus rapidement possible.

*Arnaud Siminski*

*Business Unit Director, INFOTEL*

## *Ambassade du Royaume-Uni en France*

L'Ambassade du Royaume-Uni en France est heureuse de soutenir le travail du Cross-Channel Institute, le groupe de réflexion indépendant de la Franco-British Chamber, à l'occasion d'une année importante pour les relations entre le Royaume-Uni et la France. L'année 2024 marque le 120e anniversaire de l'Entente Cordiale, l'occasion pour nos deux pays de célébrer notre amitié historique et notre partenariat mondial.

L'année dernière, les relations commerciales bilatérales entre le Royaume-Uni et la France ont atteint plus de 103 milliards de livres sterling, retrouvant ainsi les niveaux nominaux observés pour la dernière fois en 2019. Nos deux gouvernements se sont engagés à renforcer les liens commerciaux et les investissements bilatéraux entre le Royaume-Uni et la France afin de protéger notre sécurité économique et de favoriser notre prospérité future. Selon l'étude EY Attractiveness Survey 2023, la France et le Royaume-Uni sont les deux premières destinations des investissements directs provenant de l'étranger en Europe. Le Royaume-Uni s'est à nouveau classé au premier rang en Europe pour le nombre de nouveaux projets d'investissement direct étranger (greenfield) et a continué à créer plus d'emplois (en tout et par projet) que la France et l'Allemagne.

En mars 2023, le gouvernement britannique a lancé son Science and Technology Framework. Ce cadre, soutenu par notre Premier Ministre Rishi Sunak, a placé le Royaume-Uni à l'avant-garde des technologies émergentes, notamment l'intelligence artificielle, les technologies quantiques, les semi-conducteurs, les télécommunications du futur et la cybersécurité.

Au niveau bilatéral, le Royaume-Uni s'est engagé à travailler avec la France pour développer notre coopération dans les domaines de la science, de la technologie et du cyber :


**Sommet sur la sécurité de l'IA**
En novembre 2023, le Royaume-Uni a accueilli le premier AI Safety Summit, qui a été convoqué par le Royaume-Uni pour identifier les prochaines étapes dans le développement sans danger d'un "frontier AI" à travers la signature de la Déclaration de Bletchley. Sachant que la France accueillera sur son territoire le prochain sommet sur la sécurité de l'IA, nous sommes impatients de travailler en étroite collaboration avec le gouvernement français pour mener à bien ce programme important.

**Comité mixte sur la science et la technologie**
Le 29 février, le Royaume-Uni et la France ont tenu leur premier comité mixte pour la science, la technologie et l'innovation à Londres, où 800 000 livres sterling de financement conjoint ont été annoncées pour soutenir davantage de candidatures franco-britanniques pour le financement de la recherche, comme Horizon Europe.

**Dialogue cyber :**
Lors du Sommet franco-britannique de mars 2023, le Royaume-Uni et la France ont convenu de donner un nouvel élan au dialogue cyber franco-britannique. Ils ont ainsi réaffirmé leur engagement commun à défendre un cyberespace libre, ouvert, inclusif, non fragmenté et sécurisé. Le Royaume-Uni et la France ont convenu de s'attaquer à la prolifération et à l'utilisation irresponsable des capacités commerciales de cyberintrusion.

**Prolifération commerciale**
Le 6 février 2024, le Royaume-Uni et la France ont réuni une communauté internationale à Londres pour discuter des préoccupations grandissantes concernant la prolifération et l'utilisation irresponsable des capacités commerciales de cyberintrusion. La conférence a lancé le processus du Pall Mall, une nouvelle initiative internationale visant à explorer les options politiques et les nouvelles pratiques pour faire face à cette menace commune.

**Jeux olympiques et paralympiques de Paris 2024**
Les gouvernements britannique et français et l'industrie franco-britannique coopèrent étroitement en vue des Jeux olympiques et paralympiques de Paris 2024. Il a été important de partager les meilleures pratiques en matière de sécurité des événements, en s'appuyant sur l'expérience du Royaume-Uni dans l'organisation des Jeux olympiques et paralympiques de Londres 2012 et des Jeux du Commonwealth de Birmingham 2022.

Au-delà de la coopération entre nos gouvernements, les secteurs de la technologie et du numérique font déjà partie intégrante des relations commerciales et d'investissement entre le Royaume-Uni et la France. Le secteur technologique britannique est évalué à plus de 1 000 milliards de dollars - le troisième au monde derrière les États-Unis et la Chine - et nous abritons plus de 140 licornes. Aux dernières nouvelles, les services de télécommunications, d'informatique et de technologie de l'information représentaient la troisième plus grande exportation de services du Royaume-Uni vers la France, avec 2,9 milliards de livres sterling au cours de l'année dernière. L'intelligence artificielle sera un moteur essentiel dans ce secteur, et le gouvernement britannique s'est engagé à travailler avec les entreprises pour accélérer son adoption. C'est pourquoi nous avons lancé le AI Opportunities Forum, co-présidé par Michelle Donelan, secrétaire d'État à la science, à l'innovation et à la technologie, et Lord Franck Petitgas, le conseiller spécial du Premier Ministre pour l'investissement, afin de continuer le dialogue avec le secteur privé dans le but d'exploiter à bon escient le potentiel de l'intelligence artificielle dans l'économie.

Bien entendu, la cybersécurité est essentielle à la prospérité du secteur technologique. Le Royaume-Uni se félicite d'un écosystème de cybersécurité développé, avec près de 2 000 cyberentreprises et plus de 50 000 personnes employées dans ce secteur. D'importantes entreprises britanniques présentes en France concentrent une grande partie de leurs activités sur la cybersécurité. Par exemple, British Telecoms (BT) en France aide les entreprises à gérer les risques cyber par l'intermédiaire de son centre d'opérations de sécurité parisien. En outre, ces dernières années, Darktrace, une entreprise britannique de cybertechnologie, s'est développée avec succès sur le marché français en ouvrant un bureau à Paris. Créée en 2013, Darktrace s'est rapidement développée pour atteindre le statut de licorne avec une valorisation de 3 milliards de livres sterling. Ces cyberentreprises jouent non seulement un rôle essentiel dans la protection des infrastructures et de l'industrie, mais contribuent également de manière importante aux exportations britanniques.

L'Ambassade du Royaume-Uni en France a un programme scientifique et technologique passionnant pour 2024. Le 21 mars, nous avons organisé une exposition technologique franco-britannique "Bienvenue au Royaume des Audacieux" au sein la résidence de l'ambassadrice. Le Royaume-Uni reviendra à VivaTech en mai prochain avec un pavillon britannique et une délégation d'entreprises pour mettre en avant notre pays en tant que superpuissance technologique. En juin, nous accueillerons une délégation d'entreprises et d'investisseurs français qui se rendront à la London Tech Week, où un programme d'activités sera mis en place pour soutenir les entreprises désireuses de s'implanter au Royaume-Uni. La dynamique est forte et nous souhaitons saisir les opportunités offertes par ce secteur technologique en pleine évolution en renouvelant et renforçant les liens commerciaux et les partenariats entre le Royaume-Uni et la France.

*Vive l'Entente cordiale et vive l'amitié franco-britannique !*

*Ambassade du Royaume-Uni en France*

**Les challenges sécurité d'un opérateur Telco mondial.**

La transformation digitale, un des vecteurs indispensables à la croissance des organisations, a pour conséquence directe l'accroissement de la surface d'attaque et la complexité des sujets cyber. Le volume considérable de données qui transitent dans les infrastructures de BT (> 1 Tera byte /s) nous offre une place de choix pour analyser l'internet mondial et anticiper les menaces.

Il est dans notre ADN de faire bénéficier à nos clients du savoir-faire développé en interne de longue date pour protéger nos propres infrastructures. *We drink our own Champagne!* Dans un contexte d'augmentation des cyberattaques, de « cloudification », de risques liés aux « third parties », d'explosion du nombre d'objets connectés et d'évolution des modes de travail, les dirigeants ont compris que le risque cyber peut nuire à leur business, leurs réputations, entre autres impacts-clés. Il s'agit d'un sujet devenu prépondérant dans l'agenda des conseils d'administration.

*Nicolas Huguet*

*President, BT France*

II

# Défis pour les entreprises : **Le paysage cyber en 2024**

*Richard Absalom,*
*Principal Research Analyst,*
*Information Security Forum Limited (ISF)*

## *L'ère de la « polycrise »*

Dans un contexte d'incertitude politique et économique, de fragmentation sociale, de tensions géopolitiques et de détérioration de l'environnement, le monde entre dans l'ère de la « polycrise » : de multiples crises se produisent simultanément. Dans le même temps, la technologie continue de progresser et d'innover à un rythme effréné, promettant des solutions à certaines crises mais en exacerbant d'autres. Les gouvernements, les régulateurs et les entreprises s'efforcent de suivre le rythme de ces changements. Ce double paysage de menaces est propice aux abus : les cybercriminels, les hacktivistes et les groupes de pirates informatiques soutenus par des États prospèrent.

La nature même de la cybercriminalité fait qu'elle ne connaît pas de frontières : les menaces peuvent provenir de n'importe où, il est difficile de connaître leur source et il est presque impossible d'obtenir justice contre leurs auteurs. Par conséquent, les organisations en France et au Royaume-Uni sont confrontées à une série de défis communs qui pourraient empêcher le bon fonctionnement de la vie des affaires. En 2024, le paysage cyber est axé sur les menaces liées à l'intelligence artificielle (IA), l'extorsion par des techniques telles que les ransomwares et le vol de données, l'adoption continuelle du cloud par les organisations couplée des risques liés à la chaîne d'approvisionnement, ainsi que la progression exponentielle des réglementations en guise de réponse du législateur. Pour continuer à se développer, les entreprises doivent consolider leurs efforts dans un but ultime de résilience. Relever ce défi va au-delà des attributions des individus ou des équipes chargées de la sécurité. Elle exige des solutions inter-organisationnelles et la mise en place d'une culture de la coopération entre les entreprises.

# *L'IA est source d'opportunités et de risques*


L'IA continue de faire la une des médias. Ce sont particulièrement les avancées en matière d'outils d'IA générative tels que ChatGPT qui agitent les passions. Cette technologie promet d'énormes progrès en matière d'efficacité et d'innovation, et les entreprises sont naturellement désireuses de l'adopter rapidement pour éviter d'être distancées par leurs concurrents. Cependant, si l'IA présente de nombreux avantages, elle comporte aussi de nombreux risques dont les entreprises doivent être conscientes. Il s'agit notamment des risques suivants :

- **Garantir l'intégrité des informations utilisées et créées par les systèmes d'IA** – des données d'entraînement biaisées ou incorrectes peuvent conduire à des résultats de mauvaise qualité qui compromettent la confiance et finiraient par rendre le système inutilisable.
- **La non-conformité aux exigences éthiques et juridiques** – l'utilisation de données personnelles peut être la source de potentiels problèmes juridiques si elles sont utilisées sans consentement. Elles peuvent aussi être la source de résultats faussés en raison des biais présents dans l'ensemble des données d'apprentissage. De telles difficultés peuvent créer des problèmes éthiques et réputationnels.
- **L'émergence de l' « IA fantôme » (Shadow AI)** – les utilisateurs professionnels achètent et adoptent des systèmes d'IA sans la supervision des équipes informatiques ou chargées de la sécurité, ce qui peut conduire à la compromission des données organisationnelles et à l'introduction de nouvelles vulnérabilités dans les systèmes.
- **Amélioration des cyberattaques** – les acteurs malveillants utilisent des outils d'IA pour permettre des attaques plus rapides, plus sophistiquées et à plus grande échelle (par exemple, en automatisant l'identification des failles).
- **L'utilisation malveillante de « deepfakes »** peut être utilisée pour diffuser des « fake news », ce qui peut avoir des conséquences politiques graves et préjudiciables. En dehors de la sphère politique, ils peuvent également permettre un phishing sophistiqué, un « spear phishing » (c'est-à-dire des attaques de phishing ciblant une personne spécifique) et des attaques de type « whaling » (c'est-à-dire des attaques de phishing ciblant une personne très haut placée).

## Comment les organisations peuvent se préparer aux menaces liées à l'IA :

- Les conseils d'administration des entreprises doivent **jouer un rôle central** dans la supervision du déploiement des systèmes d'IA dans l'ensemble de leur organisation.
- Les équipes chargées de la sécurité doivent scrupuleusement **s'aligner sur les objectifs de l'entreprise** : comprendre les besoins spécifiques en systèmes d'IA et informer les parties prenantes de l'entreprise des risques.
- Les équipes chargées de la sécurité devraient **déployer des contrôles de sécurité améliorés par l'IA** pour ne pas se laisser distancer par les hackers.
- À tous les niveaux de l'organisation, les employés doivent être **sensibilisés et formés aux risques de l'IA** et à la manière d'identifier les « deepfakes » potentiels et l'ingénierie sociale basée sur l'IA. Ils devraient être habilités à prendre les mesures nécessaires lorsqu'ils pensent que quelque chose déroge à l'ordre établi.

# *Les entreprises continuent d'être victimes de ransomwares et de la triple menace d'extorsion*

Les cybercriminels suivent l'argent, et les techniques de chantage telles que les ransomwares constituent pour eux un marché lucratif, peu risqué et très rémunérateur. Le ransomware est un gros business et est géré comme tel. Il existe une industrie souterraine exhaustive : des développeurs de produits, des courtiers et des offres « as a service » pour les criminels dénués de compétences techniques mais qui veulent tout de même participer à l'entreprise criminelle commune.

Les ransomwares continuent d'être l'une des menaces les plus courantes auxquelles sont confrontées les organisations tant au Royaume-Uni qu'en France – et ces deux pays figurent également parmi les plus ciblés au monde. Entre avril 2022 et mars 2023, 163 organisations britanniques ont subi des attaques (en deuxième position derrière les organisations américaines), tandis que la France était le cinquième pays le plus ciblé avec 108 attaques connues[1].

Cependant, les organisations sont moins nombreuses à payer des rançons – seules 29 % des victimes l'ont fait au cours du dernier trimestre 2023[2] – et les groupes criminels changent donc de tactique. Les organisations sont désormais confrontées à une triple menace d'extorsion : le hacker ne se contente pas de crypter les systèmes et les informations et d'en interdire l'accès, il exfiltre également des données et menace de les divulguer, puis il intimide les clients, les employés et toute autre partie prenante de l'organisation victime. Les entreprises des deux côtés de la Manche doivent rester vigilantes et résistantes face à cette menace en constante évolution.

## Comment les organisations peuvent se préparer, réagir et se relever de la crise après une attaque de ransomware :

- **Préparez-vous** en vous concentrant sur l'hygiène cyber et la résilience des systèmes (y compris en effectuant des sauvegardes régulières), en simulant les attaques lors d'exercices et en s'assurant des plans de réponse.
- **Réagir** en communiquant et en collaborant efficacement avec les employés, les fournisseurs et les clients, en gérant le personnel lors d'événements de crise, en révisant la gouvernance organisationnelle et en évaluant les options technologiques sûres et pragmatiques pour reprendre les opérations.
- **Se relever de la crise** en soutenant la restauration des systèmes ; en continuant d'assurer la bonne gouvernance et la conformité de l'organisation ; en se préparant à arrêter ou à répondre à la prochaine attaque en ajustant les comportements et en appliquant les enseignements tirés d'une telle crise.

[1] *"Les ransomwares en France, avril 2022-mars 2023", Malwarebytes, https://www.malwarebytes.com/blog/threat-intelligence/2023/04/ransomware-review-france*

Voir le lien

[2] *"New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying", Coveware, https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying*

Voir le lien

# *L'adoption des services en nuage ("cloud") ouvre la porte aux attaques contre la chaîne d'approvisionnement*

L'adoption du cloud continue d'augmenter, avec tous les avantages commerciaux liés à leur caractère modulable et à la flexibilité qui en découlent. Cependant, il existe des risques. Une trop grande dépendance à l'égard d'un fournisseur de service de cloud peut aboutir à un « verrouillage » (« vendor lock-in »): c'est-à-dire à l'impossibilité pour les entreprises d'échapper à une relation qui devient de plus en plus onéreuse. Et comme le soulignent les professionnels de la sécurité, « utiliser le cloud, c'est utiliser l'ordinateur de quelqu'un d'autre ». Les fournisseurs de services de cloud sont des fournisseurs clés et constituent un vecteur d'attaque pour les acteurs malveillants : la compromission d'un fournisseur de services de cloud peut ouvrir les portes à de nombreux clients, comme on l'a vu dans divers incidents tels que les pirates soutenus par l'État qui ont compromis Microsoft et obtenu l'accès aux comptes Outlook de plusieurs clients[3].

Bien qu'ils investissent beaucoup dans la sécurité, les trois principaux fournisseurs de services de cloud - Google, Microsoft et Amazon - alimentent 66 % de l'infrastructure mondiale du cloud[4] et constituent donc des cibles difficiles, mais très gratifiantes. Des attaquants sophistiqués, y compris des groupes soutenus par des États, savent qu'ils pourraient causer des dommages économiques considérables s'ils parvenaient à mettre hors service l'un de ces fournisseurs, ne serait-ce que pour quelques heures. Il a été démontré que même des pannes accidentelles de la part de ces fournisseurs ont des conséquences importantes pour l'industrie.

En outre, les défis liés à la souveraineté des données demeurent. Les entreprises françaises doivent s'assurer que les données sont stockées et traitées dans les pays de l'UE ou dans ceux qui ont conclu un accord d'équivalence. Le RGPD britannique est actuellement équivalent à celui de l'UE, mais il s'en écarte dans certains domaines et tout changement futur pourrait rendre le transfert de données et le commerce transmanche plus difficiles.

## Comment les organisations peuvent utiliser les services de cloud en toute sécurité :

- **Évaluer et garantir** la sécurité des fournisseurs de services de cloud.
- **Identifier** les services critiques au sein de l'entreprise et mettre en place un plan de reprise d'activité (par exemple en ayant la possibilité de revenir à des systèmes sur place/en local, ou en ayant des fournisseurs de cloud de secours prêts à intervenir si le fournisseur principal tombe en panne).
- **Surveiller** les changements dans les réglementations sur les données et être prêt à s'adapter en conséquence.

[3] *A. Scroxton, "Microsoft finds Storm-0558 exploited crash dump to steal signing key", Computer Weekly, 7 September 2023, https://www.computerweekly.com/news/366551272/Microsoft-finds-Storm-0558-exploited-crash-dump-to-steal-signing-key* Voir le lien

[4] *F. Richter, "Amazon Maintains Cloud Lead as Microsoft Edges Closer", Statista, 5 février 2024, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/* Voir le lien

# *Les obligations réglementaires s'intensifient*

Au cours des 12 prochains mois, plusieurs réglementations seront introduites, mises à jour ou révisées. Le RGPD de l'UE pourrait être renforcé en 2024 ; la directive NIS2 deviendra active en octobre 2024; le règlement DORA s'appliquera aux entités financières de l'UE en janvier 2025 ; la loi sur l'IA de l'UE a été votée en mars 2024. La non-conformité pourrait avoir de graves conséquences juridiques, financières et réputationnelles. Les cadres supérieurs devront veiller à ce que leur organisation se conforme à toutes les réglementations adéquates, ce qui induit l'existence d'une responsabilité personnelle et les conséquences qu'elle implique.

**Comment les organisations peuvent se préparer à la nouvelle réglementation :**

- **Développer** une compréhension approfondie des réglementations en vigueur dans les juridictions où l'entreprise opère.
- **Mettre en place** de façon proactive les processus et les cadres nécessaires. Une fois que ces réglementations seront appliquées, il sera difficile de corriger le tir a posteriori.
- **Construire** l'environnement informatique de l'entreprise afin qu'elle puisse respecter les différentes réglementations en vigueur dans les différentes régions géographiques.

# *Conclusion : La résilience est essentielle*

En 2024, l'ampleur de la polycrise et les cybermenaces qu'elle entraîne démontrent que le questionnement porte sur le temps dans lequel une organisation subit une cyberattaque, et non pas sur la simple la possibilité d'en subir une. C'est pourquoi les organisations françaises et britanniques doivent s'efforcer de devenir résilientes. Cela signifie qu'elles doivent non seulement faire tout leur possible pour prévenir les cyberattaques, mais aussi être prêtes à y répondre et à s'en relever tout en maintenant leurs activités lorsque l'inévitable se produit.

**Pour renforcer la résilience, les entreprises doivent envisager trois actions essentielles :**

**Identifier** les informations sensibles de l'organisation, c'est-à-dire les actifs cruciaux, afin de planifier et d'améliorer les protections autour d'eux.

**Évaluer** les chaînes d'approvisionnement pour se préparer aux interruptions et aux situations d'urgence.

**Aider** le personnel à faire face à des volumes plus importants d'incidents, de perturbations et de changements.

Les entreprises de part et d'autre de la Manche sont dans le même bateau : elles sont toutes confrontées à des menaces similaires. Elles peuvent coopérer en partageant des informations, en repérant les menaces, en les maîtrisant et en tirant des enseignements de leurs expériences respectives. Une telle collaboration contribuera à renforcer la résilience, à maintenir les activités et à développer les relations commerciales.

**Les défis cyber d'un logisticien international.**

Le Groupe Sterne opère des prestations logistiques premium bas carbone en France et à l'international en B2B.

Le Groupe a connu une forte croissance organique entre 2017 et 2022 et a en parallèle réalisé plusieurs opérations importantes de croissance externe depuis 2018.

Ceci a très rapidement contribué à complexifier et rendre plus hétérogène le paysage IT.

La DSI a dû définir un schéma directeur conjuguant la rationalisation et la modernisation des systèmes d'information tout en s'engageant dans une vaste transformation digitale amenant à la multiplication des flux d'information avec les clients et les partenaires du Groupe.

Dans ce contexte, il était primordial d'inclure une démarche cyber stricte pour permettre une intégration maîtrisée des différentes entités et une réduction drastique de la dette technique.

Le Groupe Sterne s'est ainsi engagé très tôt dans l'implémentation de normes liées à la sécurité de l'information (ISO 27001) et à la protection des données personnelles (ISO 27701) pour bien structurer sa démarche et offrir à ses clients le meilleur niveau de confidentialité et de sécurité.

*Boris Pouderous*

*CIO, Sterne group*

Chez Eurostar, la cybersécurité est gérée de manière uniforme, que les personnes, systèmes et centres de données se trouvent au Royaume-Uni ou en Europe continentale. Outre notre certification ISO 27001, nos opérations de cybersécurité s'inscrivent dans le cadre du *National Institute of Standards and Technology* (Institut national des normes et de la technologie). **Notre approche couvre les personnes, les processus et la technologie.** Des contrôles réguliers sont en place pour détecter les vulnérabilités et les non-conformités, donnant lieu à des mesures supplémentaires pour préserver la sécurité de nos systèmes. L'identification de nos actifs et la gestion des menaces sont essentielles pour adapter nos priorités et affiner nos capacités de détection et de protection. Tous les membres du personnel d'Eurostar reçoivent des informations et des formations appropriées et régulières en matière de sensibilisation à la sécurité. Les différences entre les réglementations nationales pourraient nous obliger à adopter des approches spécifiques au Royaume-Uni et en Europe continentale, ce qui réduirait notre efficacité globale et pourrait entraver notre approche de la cybersécurité au niveau de l'entreprise.

*Olivier Leprêtre*

*Cybersecurity Director, Eurostar*

III

# Cadre réglementaire et conformité

*France Charruyer,*
*Founder, Lawyer & Partner, IP, IT & Data, Altij*

*Nicholas Cullen,*
*Lawyer, Partner, Data, IT & Corporate,*
*Solicitor of England and Wales, Altij*

> *Ici, vois-tu, on est obligé de courir tant qu'on peut pour rester au même endroit. Si on veut aller ailleurs, il faut courir au moins deux fois plus vite que ça !*
>
> *Lewis Carroll, De l'autre côté du miroir*

## *Introduction : des réponses réglementaires à un défi commun*

### Le rôle de la législation sur la cybersécurité dans la " décennie numérique "[1]

Dans un contexte marqué par l'instabilité et l'imprévisibilité, le défi pour les législateurs est de fournir des lois et des normes qui soient claires et lisibles tout en restant adaptées à des menaces multiples et évolutives. Pour être efficaces, ces lois doivent offrir aux organisations qui s'y conforment un avantage pour protéger leurs actifs critiques.

Au cours de la prochaine décennie, les différents pays et les blocs géopolitiques les mieux à même de défendre leurs institutions et leurs économies contre les cybermenaces se verront octroyer des avantages stratégiques considérables.

[1] *L'expression est tirée d'un programme politique de la Commission européenne : "Décennie numérique de l'Europe : objectifs numériques à l'horizon 2030".*

En réponse à ce défi commun, les législateurs de part et d'autre de la Manche poursuivent une démarche de renforcement de leurs cadres réglementaires. Autant la France que le Royaume-Uni analysent la cybersécurité en tant que priorité, essentielle à la préservation de leurs intérêts vitaux, en conséquence de quoi les deux pays ont bati des stratégies nationales propres.

***Tableau 1 : Planification stratégique de la cybersécurité en France et au Royaume-Uni***

| | France | Royaume-Uni |
|---|---|---|
| **Défense** | **Loi de programmation militaire 2024-2025 (LPM)**<br>4 milliards d'euros de besoins en cybersécurité sont programmés sur la période 2024-2030. La LPM vise à « poursuivre le développement d'une cyberdéfense de premier plan, robuste et crédible face à nos compétiteurs stratégiques, apte à assurer, dans la durée, la résilience des activités critiques du ministère et l'interopérabilité avec nos alliés ».<br>La LPM impacte aussi les éditeurs de logiciels par une obligation de notification à l'ANSSI en cas de vulnérabilité significative affectant un de leurs produits ou en cas d'incident informatique (LPM A66). | **Stratégie de cyber-résilience pour la défense**<br>Objectif principal :<br>• Les fonctions critiques en matière de défense seront « considérablement renforcées contre les cyberattaques » d'ici à 2026,<br>• tous les organismes en matière de défense doivent être « résilients face aux vulnérabilités et aux méthodes d'attaque connues » au plus tard en 2030. |
| **Secteur Public** | **Doctrine Cloud au centre**<br>Elle vise à mettre en place l'utilisation par l'État de technologies de type cloud plus sécurisées et « immunisées » contre le droit extracommunautaire, notamment par la mise en place d'une norme appelée « SecNumCloud ». Une norme européenne équivalente appelée EUCS (schéma européen de certification de sécurité pour les services cloud) est en cours de préparation par l'agence de cybersécurité de l'UE, l'ENISA – actuellement en pourparlers sur des possibles exigences en matière de localisation des données et de souveraineté. | **Stratégie gouvernementale en matière de cybersécurité 2022-2030**<br>La stratégie repose sur deux "piliers" : (1) les bases de la résilience organisationnelle en matière de cybersécurité et (2) la défense collective : partage entre les organisations, de données, de l'expertise et des capacités en matière de cybersécurité, en se concentrant sur cinq objectifs : (1) gérer le risque cyber, (2) se protéger contre les cyberattaques, (3) détecter les événements liés à la cybersécurité, (4) minimiser l'impact des incidents et (5) développer les compétences, les connaissances et la culture adéquates. |

## Principaux points communs : responsabilité au niveau du conseil d'administration, gestion des chaînes d'approvisionnement, formation du personnel.

En France et au Royaume-Uni, les réformes et les actualisations des lois sur la cybersécurité montrent à bien des égards une orientation commune. L'UE et le Royaume-Uni ont tous deux pris des mesures visant à renforcer et étendre leurs législations respectives en matière de sécurité des réseaux et de l'information, ou prévoient de le faire[2]. Cette évolution réglementaire permanente oblige les organisations, tant en France qu'au Royaume-Uni, à améliorer leur gouvernance en matière de cybersécurité, en particulier s'agissant de :

**Responsabilisation** accrue **des organes de gestion**, qui doivent désormais **assumer une responsabilité directe en matière de cybersécurité.**

Mise en œuvre des **obligations** dites **"dès la conception"** (intégration de la protection de la vie privée et de la sécurité dans les systèmes d'information).

Renforcement des **exigences techniques et organisationnelles en matière de cybersécurité.**

**Des exigences** plus strictes en **matière d'alerte et de notification** des incidents et des violations (y compris la notification horizontale, encouragée par la protection juridique accordée aux lanceurs d'alerte).

Obligations de **vérification des niveaux de sécurité des données des fournisseurs** et de **garanties contractuelles appropriées** (protection de la chaîne de valeur).

Responsabilité de veiller à ce que le personnel **reçoive une formation appropriée en matière de cybersécurité.**

[2] *Ainsi, la directive "NIS 2" entrera en vigueur en France au plus tard en octobre 2024, tandis qu'au Royaume-Uni, le gouvernement a mené une consultation en 2022 et a depuis annoncé son intention de mettre à jour les réglementations NIS britanniques dès que le temps parlementaire le permettra.*

[3] *https://www.eeas.europa.eu/eeas/cyber-eu-and-uk-launch-cyber-dialogue_en*

Voir le lien

## Coopération transfrontalière en cours au niveau de l'UE et au niveau bilatéral

Les gouvernements et les services répressifs français et britanniques continuent de collaborer pour lutter contre les menaces liées à la cybersécurité. Ainsi, en décembre 2023, l'UE et le Royaume-Uni ont tenu leur premier cyberdialogue à Bruxelles[4] dans le cadre de l'accord de commerce et de coopération entre l'UE et le Royaume-Uni. Cet accord établit des principes sur les questions cyber, notamment le dialogue sur l'évolution des politiques, le partage des meilleures pratiques et la coopération entre des organismes tels que les agences de cybersécurité et les équipes d'intervention d'urgence[5].

Agissant de manière bilatérale, la France et le Royaume-Uni ont organisé une conférence à Lancaster House à Londres les 6 et 7 février 2024, où se sont tenues des discussions centrées sur les préoccupations relatives à la prolifération et à l'utilisation irresponsable des outils de cyber-intrusion disponibles sur le marché[6].

La coopération se poursuit entre les forces de l'ordre. Ainsi, en février 2024, la National Crime Agency (NCA) du Royaume-Uni a annoncé qu'une coalition internationale d'agences de 10 pays, comprenant la France et les États-Unis, avait pris le contrôle de l'infrastructure du groupe de pirates informatiques Lockbit[7].

Au niveau de l'Union Européenne, la proposition de « *Cyber Solidarity Act* », faisant l'objet d'un accord politique en mars 2024, établit un système d'alerte européen en matière de cybersécurité (« *Cybersecurity Alert System* »). Ce système d'alerte est composé d'un réseau de cyber-hubs à travers l'UE, ainsi qu'un mécanisme d'urgence en matière de cybersécurité (« *Cybersecurity Emergency Mecanism* ») qui vise à améliorer la préparation et la réponse aux cyberincidents graves et de grande échelle.

## Une approche holistique de la conformité : transparence et confiance

Malgré les différences juridiques et culturelles entre les deux pays, les organisations en activité au Royaume-Uni et en France doivent prendre conscience que le paysage législatif global exige une approche holistique et conjointe de la cybersécurité.

Les concepts clés comprennent la responsabilité, la gestion des risques et la gouvernance. Ils s'inscrivent dans un contexte où la conformité à la cybersécurité devient de plus en plus un indicateur de performance pour les entreprises, les investisseurs incluant la cybersécurité dans leurs processus de diligence raisonnable.

[4] *https://www.eeas.europa.eu/eeas/cyber-eu-and-uk-launch-cyber-dialogue_en* — Voir le lien

[5] *Accord de commerce et de coopération entre l'UE et le Royaume-Uni : Quatrième partie : Coopération thématique, Titre II : Cybersécurité*

[6] *https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/cybersecurite-communique-conjoint-de-la-france-et-du-royaume-uni-sur-la#:~ :text=Les%206%20et%207%20février,cyber%20disponibles%20sur%20le%20marché.* — Voir le lien

[7] *Voir https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/* — Voir le lien

# *Base réglementaire commune : RGPD et NIS*

Les équipes juridiques et de compliance en France comme au Royaume-Uni trouveront de nombreux points communs entre les régimes juridiques des deux pays.

En particulier, le Règlement général sur la protection des données (RGPD), dans ses versions britannique et européenne, fournit un cadre relatif à la sécurité des données personnelles. Il est désormais bien ancré dans les cultures d'entreprise en France et au Royaume-Uni, en plus d'obligations sectorielles propres à certains acteurs[8].

Les deux pays imposent également des exigences en matière de « NIS » (Network and Information Security ou sécurité des réseaux et de l'information) aux opérateurs de services essentiels et à certains fournisseurs de services numériques. Comme le RGPD, les exigences NIS ont une source commune dans le droit européen[9]. Elles ont également fait l'objet, des deux côtés de la Manche, de mises à jour législatives, notamment avec la directive NIS2 de l'UE, qui doit entrer en vigueur en France d'ici octobre 2024.

Comme le résume le tableau ci-dessous, les obligations dans chaque pays sont comparables et, à certains égards, identiques en ce qui concerne les données à caractère personnel.

*[8] Outre les cadres RGPD et NIS, il existe des sources d'obligations en matière de cybersécurité pour les entreprises au Royaume-Uni et en France, applicables à des acteurs et secteurs spécifiques. Sans essayer de les énumérer de manière exhaustive, elles comprennent par exemple, en France, des obligations pour les acteurs du secteur de la santé, qui doivent utiliser des fournisseurs de services d'hébergement ayant une certification "HDS" (hébergeur de données de santé) et au Royaume-Uni des obligations spécifiques en matière de cybersécurité pour les fournisseurs de réseaux et de services de télécommunications publiques (Communications Act 2003, tel que modifié par le Telecommunications (Security) Act 2021). En outre, au Royaume-Uni et en France, les prestataires de services de "confiance" qui vérifient l'identité des personnes en ligne sont tenus, en vertu des règlements eIDAS (identification électronique et services de confiance), d'informer les autorités compétentes d'une violation de la sécurité dans un délai de 24 heures.*

*[9] Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*

***Table 2 : RGPD et NIS***

| | France | Royaume-Uni |
|---|---|---|
| **RGPD** (traitement des données personnelles) | **RGPD UE**<br><br>Règles supplémentaires contenues dans la Loi Informatique et libertés de 1978.<br><br>Autorité de contrôle : la *Commission Nationale de l'Informatique et des Libertés* (CNIL).<br><br>Article 5.1(f) : Garantir une sécurité appropriée des données à caractère personnel. | **RGPD RU**<br><br>Règles supplémentaires contenues dans la *Data Protection Act*, 2018.<br><br>Autorité de contrôle : le bureau du commissaire à l'information - Information Commissioner's Office (ICO).<br><br>Article 5.1(f) : Garantir une sécurité appropriée des données à caractère personnel. |

| | France | Royaume-Uni |
|---|---|---|
| **RGPD** (traitement des données personnelles) | Article 28 : Garanties obligatoires de la part des sous-traitants de données.<br><br>Article 32 : Obligation générale de sécurité :<br><br>- Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.<br><br>- Parmi les mesures possibles figurent la pseudonymisation, le chiffrement, la garantie de l'intégrité du système, des mécanismes de récupération des données en cas d'incident, des procédures de test régulières, etc.<br><br>Articles 33 et 34 : Obligations de notifier à la CNIL toute violation de données à caractère personnel et d'en informer les personnes concernées.<br><br>Article 83 :<br><br>- La CNIL peut imposer des amendes administratives allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu (pour les violations relatives aux principes de base ou aux droits des personnes concernées).<br><br>- En cas d'infraction à l'article 32 (sécurité des données), la CNIL peut imposer des sanctions administratives pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu. | Article 28 : Garanties obligatoires de la part des sous-traitants de données.<br><br>Article 32 : Obligation générale de sécurité :<br><br>- Mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.<br><br>- Parmi les mesures possibles figurent la pseudonymisation, le chiffrement, la garantie de l'intégrité du système, des mécanismes de récupération des données en cas d'incident, des procédures de test régulières, etc.<br><br>Articles 33 et 34 : Obligations de notifier à l'ICO toute violation de données à caractère personnel et d'en informer les personnes concernées.<br><br>Article 83 :<br><br>- L'ICO peut imposer des amendes administratives allant jusqu'à 17,5 millions de livres ou 4 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu (pour les violations relatives aux principes de base ou aux droits des personnes concernées).<br><br>- En cas de violation de l'article 32 (sécurité des données), l'ICO peut imposer des sanctions administratives pouvant aller jusqu'à 8,7 millions de livres ou 2 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu. |

NIS
Network and Information Security

| France | Royaume-uni |
| --- | --- |
| **NIS 1 : Loi de transposition n° 2018-133 du 26 février 2018.** (N.B. Cette loi doit être actualisée au plus tard en octobre 2024 par la directive NIS2).<br><br>S'applique à :<br>1. *Opérateurs de services essentiels* (OSE) : énergie, transports, banques, marchés financiers, santé, eau, infrastructures numériques.<br>2. *Fournisseurs de services numériques* (FSN) : places de marché en ligne, moteurs de recherche, services d'informatique de type cloud.<br><br>Autorité compétente : *l'Agence nationale de la sécurité des systèmes d'information* (ANSSI)<br><br>Les obligations comprennent :<br>✓ Identification des OSE et de leurs systèmes d'information essentiels auprès de l'ANSSI,<br>✓ Application d'exigences spécifiques en matière de sécurité,<br>✓ Signalement des incidents à l'ANSSI.<br><br>Articles 9 et 15 : Amendes de 75.000 à 125.000 euros pour les administrateurs ayant enfreint diverses dispositions de la loi.<br><br>**N.B.** La directive NIS2 renforcera considérablement les pouvoirs d'infliger des amendes aux entreprises en cas de non-conformité - voir le tableau 4 page 29-30. | **The Network and Information Regulations 2018 (NISR)** (Mise à jour en 2020. Nouvelle actualisation à réaliser en fonction du calendrier parlementaire)<br><br>S'applique à :<br>1. *Opérateurs de services essentiels* (OSE) : énergie, transports, santé, eau, infrastructures numériques.<br>2. *Fournisseurs de services numériques* (FSN) : places de marché en ligne, moteurs de recherche, services d'informatique de type cloud.<br><br>Autorités compétentes : ICO pour les RDSPs et le département d'état compétent pour les OESs.<br><br>Les obligations comprennent :<br>✓ Identification des OES auprès de leur autorité compétente,<br>✓ Application d'exigences spécifiques en matière de sécurité,<br>✓ Signalement des incidents à l'autorité compétente.<br><br>Article 18 : L'ICO ou l'autorité compétente, si elle est différente, peut infliger des pénalités allant jusqu'à 17 millions de livres sterling pour une infraction importante qui a occasionné ou qui pourrait occasionner "un incident entraînant une menace immédiate pour la vie ou un impact négatif important sur l'économie du Royaume-Uni". |

**NB. Lignes directrices réglementaires et "soft law"**

Outre les obligations légales "dures" évoquées dans la présente section, les institutions publiques et autorités de régulation (ex. en France : l'ANSSI, la CNIL et cybermalveillance.gouv.fr, au Royaume-Uni : la NCSC et l'ICO), fournissent des documents d'orientation sur les meilleures pratiques en matière de cybersécurité. Aussi, les associations et corporations professionnelles de référence (ex. en France : CLUSIF, CESIN, CIGREF et au Royaume-Uni : CIISec et UK Cyber Security Council) œuvrent pour soutenir les entreprises et les professionnels de la cybersécurité dans ce domaine.

Sur le plan européen, la Commission européenne a approuvé le premier système de cybersécurité de l'UE, le 31 janvier 2024, destiné à certifier les produits TIC, sur la base de critères communs (EUCC) afin de garantir la fiabilité du cycle de vie des produits, services et processus TIC sur le marché de l'UE.

Étant donné que l'article 32 du RGPD exige que les responsables du traitement et les sous-traitants tiennent compte de "l'état de l'art", les entreprises doivent avoir connaissance de ces meilleures pratiques sous forme de lignes directrices réglementaires et adapter leurs processus en conséquence.

***Table 3 : Exemple de directives réglementaires***

| | France | Royaume-Uni |
|---|---|---|
| Cybersécurité | **Agence Nationale de la sécurité des systèmes d'information (ANSSI)**<br>Fournit une série de ressources pour les entreprises sur son site web, y compris, à l'intention des dirigeants et des professionnels de la sécurité informatique, des conseils sur les bonnes pratiques. | **Centre national de cybersécurité (NCSC)**<br>Elle publie des orientations, notamment le "Cyber Security Toolkit for Boards" (boîte à outils de cybersécurité pour les conseils d'administration) , dont les objectifs sont notamment d' intégrer la cybersécurité au sein de l'organisation. |
| Données personnelles | **Commission Nationale de l'Informatique et des Libertés (CNIL)**<br>Publie régulièrement des conseils pratiques et techniques ainsi que des informations sur la cybersécurité.<br>À noter l'importance du travail de la CNIL en matière de sensibilisation au risque cybersécurité, avec son guide de la sécurité des données personnelles qui regroupe les pratiques à l'état de l'art en matière de sécurité des données. | **The Information Commissioner's Office (ICO)**<br>Elle publie des orientations en matière de sécurité à l'intention des grandes organisations des secteurs public, privé et tertiaire, ainsi que des petites entreprises, par l'intermédiaire de son site web dédié aux petites entreprises. |

# *Les réformes en cours dans l'UE, en France et au Royaume-Uni*

Les législateurs français, britannique et européen continuent d'adapter et d'actualiser les exigences en matière de cybersécurité, afin de faire face à des menaces de plus en plus graves.

Tout en tenant compte des différences juridiques et culturelles des deux pays, il existe plusieurs principes sur lesquels ils s'alignent dans leur conception de la cybersécurité :

- Un renforcement de l'obligation générale d'assurer la cybersécurité, que les organisations des secteurs public et privé devront intégrer dans leurs pratiques en matière de planification de la sécurité et de résilience technique et organisationnelle, ainsi que dans l'état de l'art.
- La responsabilité se concentre explicitement sur les plus hauts niveaux de l'organisation, dans le cadre de la législation européenne NIS2 et DORA, mais aussi dans le cadre de la réforme du RGPD proposée par le Royaume-Uni, dans laquelle un "Senior Responsible Individual" sera responsable du contrôle de la sécurité des données et de la formation[10].
- Veiller à ce que la formation à la cybersécurité soit la règle et non l'exception.
- Permettre la coopération et la coordination internationales en matière de cybersécurité[11].

*[10] Les administrateurs des sociétés britanniques ont également des obligations définies dans les articles 170 à 177 de la loi sur les sociétés de 2006, notamment celles de promouvoir le succès de la société et de faire preuve d'un soin, d'une compétence et d'une diligence raisonnables. La première disposition est citée par le UK NCSC dans son "Cyber Security Toolkit for Boards" (kit d'outils de cybersécurité pour les conseils d'administration).*

*[11] La directive NIS2 contient une section étendue sur la coopération au niveau de l'Union et au niveau international, y compris la création d'un groupe de coopération de l'UE, d'un réseau de "CSIRT" (équipes de réponse aux incidents de sécurité informatique) nationaux, l'établissement du réseau européen d'organisations de liaison en cas de cybercrise (EU-CyCLONe) et la possibilité de conclure des accords internationaux avec des pays tiers pour leur permettre de participer aux activités de ces trois groupes.*

***Table 4 : Exemples de mises à jour réglementaires clés dans le domaine de la cybersécurité***

| | France | Royaume-Uni |
|---|---|---|
| Données personnelles | **Le RGPD reste en vigueur.** *(voir le tableau 2 page 25-27)* | **La proposition de réforme du RGPD britannique est actuellement en cours d'examen par le Parlement**. Les dispositions relatives à la sécurité des données ne sont pas directement modifiées par la réforme proposée. Toutefois, le délégué à la protection des données (data protection officer – DPO) sera remplacé par une "personne responsable de haut niveau" (« Senior Responsible Individual ») qui doit faire partie de l'encadrement supérieur de l'organisation et qui sera chargée, entre autres, de contrôler le respect de l'article 32 du UK GDPR (sécurité des données). |

## Sécurité des réseaux et de l'information

| France | Royaume-Uni |
| --- | --- |
| Directive européenne « NIS 2 » 2022/2555 : transposition en droit français avant le 18 octobre 2024.<br><br>Élargit le champ des secteurs concernés aux "entités essentielles et importantes" (administrations publiques, télécommunications, plateformes de réseaux sociaux, services postaux, secteur spatial, etc.) et introduit des exigences strictes en matière de gestion des risques, de notification des incidents et de mesures de sécurité.<br><br>L'ANSSI doit établir des précisions sur le périmètre des entités régulées et les mesures de sécurité à mettre en œuvre.<br><br>L'article 20 confère une responsabilité accrue en matière de cybersécurité aux organes de direction, qui doivent approuver les mesures de gestion des risques et superviser leur mise en œuvre, ainsi que les obligations de formation en matière de cybersécurité. Ces organes peuvent être tenus pour responsables en cas de violation des exigences de cybersécurité.<br><br>Article 34 : Amendes possibles en cas d'infraction :<br><br>Entités essentielles : Amendes administratives d'un montant maximal d'au moins 10 millions d'euros ou de 2 % du chiffre d'affaires annuel mondial total (le montant le plus élevé étant retenu).<br><br>Entités importantes : Amendes administratives d'un montant maximal d'au moins 7 millions d'euros ou de 1,4 % du chiffre d'affaires annuel mondial total (le montant le plus élevé étant retenu). | Actuellement en vigueur : le règlement sur les réseaux et les systèmes d'information de 2018, tel que mis à jour en 2020 *(voir le tableau 2 page 25-27 pour le champ d'application).*<br><br>N.B. Proposition de mise à jour du NISR : après consultation, le gouvernement a annoncé son intention de procéder à la réforme.<br><br>Élargit la définition des fournisseurs de services numériques pertinents (RDSP) pour y inclure les "fournisseurs de services gérés" (MSP), c'est-à-dire les entreprises qui gèrent à distance des éléments des systèmes informatiques de leurs clients. Comme ces acteurs ont accès aux systèmes d'un grand nombre de clients, ils représentent potentiellement un risque systémique en cas de cyberattaque.<br><br>Elle vise également à introduire un régime de surveillance à deux niveaux pour les fournisseurs de services numériques : un nouveau niveau de "surveillance proactive" pour les fournisseurs les plus critiques, parallèlement au niveau de surveillance "réactive" existant pour toutes les autres entités concernées.<br><br>*(Voir le tableau 2 page 25-27 pour les sanctions en vigueur)* |

| | France | Royaume-Uni |
|---|---|---|
| **Services financiers** | DORA (Digital Operational Resilience Act) Règlement (UE) 2022/2554<br><br>Entre en vigueur le 17 janvier 2025.<br><br>Vise à améliorer la résilience opérationnelle numérique des prestataires de services financiers en matière de gestion des risques liés aux technologies de l'information et de la communication (TIC), de notification des incidents et des cybermenaces aux autorités, de tests de résilience opérationnelle numérique, de partage d'informations et de renseignements relatifs aux cybermenaces et de mesures de gestion des risques liés aux prestataires de services TIC tiers.<br><br>Comme pour le NIS2, **l'enjeu est la responsabilisation des organes de direction et la résilience.** | Réglementation par l'intermédiaire de la Financial Conduct Authority (FCA) et la Prudential Regulation Authority (PRA), de la Banque d'Angleterre, qui ont pour mission de lutter contre la criminalité financière et de protéger le système financier britannique.<br><br>Le manuel de la FCA contient des principes, dont le principe 3 qui exige qu'une entreprise "**prenne des mesures raisonnables pour organiser et contrôler ses activités de manière responsable et efficace, en mettant en place des systèmes de gestion des risques adéquats**".<br><br>La FCA dispose de pouvoirs d'exécution importants et a imposé en octobre 2023 une amende de 11 millions de livres sterling à la suite d'une importante violation de données affectant les clients d'une agence de notation de crédit. |
| **Intelligence Artificielle / IA** | Le Règlement sur l'Intelligence artificielle (dit AI Act) de l'UE a été adopté par le Conseil et le Parlement en décembre 2023 et approuvé par les États membres en février 2024, puis par le Parlement européen en mars 2024.<br><br>Le texte final contient des exigences spécifiques en matière de cybersécurité pour les systèmes d'IA à haut risque, y compris des obligations de résilience et de conception ("by design") .<br><br>Le Règlement repose sur une approche graduelle, fondée sur la sécurité des produits et l'approche par les risques. Certains systèmes sont interdits car trop risqués, d'autres très réglementés car à haut risque. | Livre blanc du gouvernement "**Une approche pro-innovation de la réglementation de l'IA**" publié en mars 2023.<br><br>Une approche "agile" dans le cadre de laquelle "nous ne donnerons pas à ces principes une base légale dans un premier temps. De nouvelles exigences législatives rigides et onéreuses pour les entreprises pourraient freiner l'innovation en matière d'IA et réduire notre capacité à répondre rapidement et de manière proportionnée aux futures avancées technologiques. Au lieu de cela, les principes seront publiés sur une base non statutaire et mis en œuvre par les régulateurs existants". |

| | France | Royaume-Uni |
|---|---|---|
| IA | Des systèmes d'IA qui interagissent directement avec des personnes physiques sont soumis à des obligations de transparence vis-à-vis de ces personnes. | L'un des principes étant "la sûreté, la sécurité et la robustesse", la cybersécurité est un critère qui sera pris en compte par les régulateurs tels que l'ICO lors de l'application de ce cadre.<br><br>Par ailleurs, le 1er avril 2024, le Royaume-Uni a signé avec les États-Unis un accord pour tester et évaluer les risques liés aux modèles émergents d'intelligence artificielle. |
| La cyber-résilience | Proposition de règlement de l'UE concernant les exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques (Cyber Resilience Act - CRA).<br><br>Accord annoncé sur le texte par la Commission européenne en décembre 2023. L'entrée en vigueur est prévue en 2024 et l'application des règles 36 mois plus tard.<br><br>Il vise à fournir un cadre juridique pour les obligations en matière de cybersécurité applicables aux produits matériels et aux logiciels comportant des éléments numériques. | Loi de 2022 sur la sécurité des produits et l'infrastructure des télécommunications.<br><br>Ce texte, qui entre en vigueur le 29 avril 2024, impose des exigences de cybersécurité aux fabricants, importateurs et distributeurs de produits de consommation connectés à internet ("intelligents"), qui ont l'obligation de se conformer aux exigences de sécurité, d'enquêter sur les manquements à la conformité et de tenir des registres.<br><br>Les importateurs et les distributeurs ont également l'obligation de ne pas fournir de produits en cas de non-respect des règles par un fabricant ainsi que d'en informer les autorités chargées de l'application de la législation. |

# *Conclusion : Le paradoxe de la Reine Rouge ?*

La législation relative à la cybersécurité vise à fournir un cadre stable permettant à l'état de droit de s'appliquer dans l'espace numérique.

Il est ainsi question d'enjeux de gestion du risque, de responsabilités, de gouvernance et de développement des compétences, tant d'actions que les dirigeants vont devoir mettre en œuvre pour se protéger.

Il s'agit pour les entreprises d'acquérir des compétences vers toujours plus de résilience et de solidarité, dans une logique de redevabilité (accountability), de confiance partagée et de responsabilisation des organes de gouvernance, et de renforcer tous les maillons de la chaîne, dont les PME / TPE, qui représentent la majeure partie du tissu économique de nos deux territoires[12].

L'arrêt ou perturbation d'activité ou la perte de données n'a pas un impact identique selon la taille des entreprises ou leur secteur d'activité mais l'interdépendance croissante des systèmes d'information fait de la cybersécurité des tiers un problème majeur pour la plupart des entreprises.

Par conséquent, l'implémentation de normes, de référentiels, de certifications et de bonnes pratiques pour parvenir à l'état de l'art exige un effort continu tout le long de la chaîne de valeur, que ce soit avec ses salariés, ses partenaires, ses prestataires et ses clients.

Une première problématique reste la posture du dirigeant et des directions opérationnelles et de leur capacité à mobiliser collectivement en termes de prise de conscience, d'allocation de budget et de pilotage du risque.

Une seconde problématique est le passage à l'échelle de nos systèmes de détection et de défense, la capacité des systèmes d'intelligence artificielle (SIA) à produire des stratégies d'attaques originales, et la nécessité de développer de nouvelles compétences pour interagir avec les machines.

Dans ce contexte l'usage ou le mésusage de l'IA est à la fois un défi et une opportunité car les systèmes d'IA sont potentiellement accessibles aux acteurs malveillants comme ils peuvent l'être aux équipes chargées de la sécurité de l'information. Comme le rappelle la Reine Rouge de Lewis Carroll : « Ici il faut courir pour rester à la même place. »

L'émergence de l'IA transforme la dynamique géopolitique mondiale avec des IA hybrides à usage civil et militaire à des échelles démesurées. Dans ce contexte, les états et les blocs géopolitiques sont engagés dans une course effrénée aux talents, et aux financements pour l'extraction de la valeur économique tractée par l'IA et la maîtrise des risques induits.

Le droit de la cybersécurité ne peut donc pas se permettre d'être uniquement réactif : il doit anticiper les risques futurs et fournir un cadre à la fois robuste et suffisamment souple pour s'adapter aux nouveaux défis technologiques.

Les lois sont à bien des égards plus fragiles que les technologies qu'elles tentent de réglementer. Les approches de l'UE et du Royaume-Uni convergent sur la nécessité d'aller au-delà d'une approche purement sécuritaire « par la conception » (by design) et de trouver le bon rapport risque/bénéfice : évaluer un niveau de risque acceptable, garder le contrôle sur les actifs numériques et protéger nos sociétés.

Le défi consiste désormais à faire en sorte que la prochaine génération de réglementation en matière de cybersécurité soit opérationnelle, l'objectif partagé étant de défendre nos actifs vitaux, notre modèle de société et nos valeurs démocratiques contre les cybermenaces croissantes, dans l'intérêt de notre futur commun.

*[12] À ce titre, la stratégie nationale britannique en matière de cyber encourage une approche « globale de la société » de la cybersécurité : Cf. House of Commons Library, Cybersecurity in the UK, Research Briefing 22 June 2023 by Adam Clark*

Getlink fournit des services de mobilité sécurisés de haute qualité à travers l'Europe. **La numérisation étant une pierre angulaire de notre stratégie, la cybersécurité est notre priorité et est prise en compte à chaque instant.** Ce défi est mondial et, en tant qu'entreprise binationale, nous devons prendre en considération les deux côtés de la Manche. La cybersécurité est gérée à tous les niveaux, depuis le conseil d'administration binational qui met en œuvre la politique et vérifie les stratégies et les tableaux de bord tous les trimestres, jusqu'aux équipes informatiques opérationnelles des deux côtés. Nous sommes soumis à des réglementations britanniques et françaises, de forme différente mais de contenu similaire. Nos politiques, notre organisation et nos outils assurent un niveau de sécurité conforme à ces règles. Nous rendons compte régulièrement aux autorités : l'Agence Nationale de la Sécurité des systèmes d'information en France, le Department for Transport (département des Transports) et l'Office of Gas and Electricity Markets (bureau des marchés du gaz et de l'électricité) au Royaume-Uni. Nous investissons des ressources importantes dans des technologies efficaces, y compris dans l'intelligence artificielle, et dans un personnel hautement qualifié.

*John Keefe*

*Chief Corporate and Public Affairs Officer, Getlink Group*

IV

# Gouvernance de la cybersécurité

## La clé de la cyber-résilience

*David Mudd*
*Global Head of Digital Trust Assurance,*
*British Standard Institution (BSI)*

## *Qu'est-ce que la gouvernance en matière de cybersécurité ?*

La gouvernance en matière de cybersécurité est le processus de contrôle et de direction des activités de cybersécurité d'une organisation. Elle appelle à une approche holistique de la cybersécurité qui s'intègre aux opérations de l'organisation afin de prévenir les interruptions d'activité dues aux cybermenaces ou aux cyberattaques. Les principales caractéristiques de la gouvernance en matière de cybersécurité sont les suivantes :

- Cadres de responsabilisation
- Hiérarchies décisionnelles
- Définir les risques liés aux objectifs de l'entreprise
- Stratégies et plans d'atténuation de ces risques
- Processus et procédures de surveillance

# *Pourquoi la gouvernance en matière de cybersécurité est-elle importante ?*

Que ce soit en France ou au Royaume-Uni, la grande majorité des entreprises dépendent grandement des technologies numériques afin d'assurer leur bon fonctionnement. L'expansion de l'économie numérique a dans le même temps fait croître le niveau des menaces relatives à la cybersécurité. Le paysage réglementaire croissant et évolutif qui en résulte entraîne ainsi des risques supplémentaires pour les entreprises, telles que des amendes importantes en cas de non-conformité. Les conséquences potentielles des cyber-incidents sont graves : « Le risque cyber n'est plus seulement un problème informatique, c'est une vulnérabilité critique qui influence directement la santé de l'entreprise collective. » [David Raissipour, Forbes 2023].

Dans une économie de plus en plus numérique, les risques liés à la cybersécurité doivent faire l'objet d'une attention similaire à celle accordée aux risques financiers et juridiques. La raison : leur impact matériel potentiel sur les activités de l'entreprise. Il existe un lien intrinsèque avec la résilience des entreprises qui nécessite des dirigeants et conseils d'administration de toutes organisations de s'impliquer dans la cybersécurité pour comprendre leur exposition au risque cyber. Cette démarche a lieu tout en appréciant comment cette implication se calque à leur appétence pour le risque et leur stratégie d'entreprise. Une gouvernance indéfectible de la cybersécurité leur permettra de tirer parti des possibilités offertes par l'économie numérique, tout en gérant efficacement les risques qui y sont associés.

Au niveau macroéconomique, pour que la société puisse bénéficier des technologies numériques dans le but d'offrir des expériences nouvelles, améliorées et une qualité de vie durable, les organisations doivent adopter un positionnement sûr en matière de gouvernance de la cybersécurité. Une telle approche aura pour finalité de minimiser l'impact de la cybercriminalité, qui est la troisième plus grande économie du monde et qui ne cesse aujourd'hui de croître.

Quant à l'impact de la gouvernance de la cybersécurité sur les entreprises, chaque structure doit choisir son propre positionnement. Une organisation pourrait consacrer toutes ses ressources à la cybersécurité et il y subsisterait tout de même un risque résiduel. À l'inverse, une organisation pourrait ne rien investir du tout. Entre ces deux extrêmes, une entreprise pourrait avoir une approche différente qui consisterait à concevoir de façon plus mature les finances et ressources dédiées, en conséquence de quoi elle déterminerait un plan d'action :

*"Voici ce que nous allons investir"*

À ce stade, êtes-vous sûr de bien comprendre ce risque résiduel ? Dans quelle mesure correspond-il à votre appétence pour le risque et votre stratégie d'entreprise ?

Et si un jour ce risque résiduel devient réalité, dans un monde évoluant rapidement, de plus en plus numérique, où le modèle opérationnel de votre entreprise et les risques associés demeurent, comment pouvez-vous dormir sur vos deux oreilles ?

**C'est là qu'une gouvernance efficace en matière de cybersécurité vous est nécessaire.**

# *À quoi ressemble une bonne gouvernance en matière de cybersécurité ?*

## Une gestion efficace des risques.

L'investissement dans la gestion des risques permet une prise de décision fiable basée sur lesdits risques. Cela permettra aux entreprises d'utiliser des technologies innovantes et adaptées aux risques. Les bonnes pratiques en matière de cybersécurité soutiennent les décisions commerciales au lieu de se contenter d'en gérer les conséquences.

## Délégation efficace des décisions.

Tout en veillant à ce que les responsables à tous les niveaux de l'entreprise disposent de connaissance, d'aptitudes et de compétences nécessaires en matière de cybersécurité, il faut permettre à la direction générale de demeurer responsable en dernier ressort de la gestion des risques cyber, tout en leur permettant de prendre des décisions opportunes et efficaces pour développer l'entreprise.

## Gestion de l'incertitude.

Les systèmes numériques que les entreprises utilisent aujourd'hui lient intrinsèquement la technologie, les processus de l'entreprise et les personnes. Cette complexité entraîne une incertitude dans la gestion des risques qui est, dans une certaine mesure, inévitable. Il est donc essentiel de comprendre les limites des contrôles et des approches en matière de sécurité, ainsi que les stratégies de gestion des risques résiduels et incertains.

## Une communication efficace sur la gestion des risques liés à la cybersécurité.

Une communication efficace est essentielle pour diriger et contrôler la gestion des risques liés à la cybersécurité. La confiance repose sur une bonne communication, ce qui favorise une culture positive de la cybersécurité (voir ci-dessous).

- La communication descendante doit montrer clairement l'orientation de l'entreprise, ses objectifs et son approche du risque, ainsi que les rôles et responsabilités de chacun.
- La communication ascendante et latérale doit clairement fournir des informations techniques et non techniques détaillées pour éclairer la prise de décision en matière de gestion des risques.

## Une culture de cybersécurité efficace.

Une culture de cybersécurité efficace permettra de faire face aux complexités et aux incertitudes mentionnées ci-dessus. Le personnel est la clé d'une défense efficace contre un incident de cybersécurité et le facteur le plus important pour réagir à un incident et s'en rétablir. La culture de la cybersécurité est donc un facteur important de la résilience des entreprises. Si la création d'une culture efficace implique de nombreux éléments, les aspects susmentionnés, ainsi que l'intégration de la gestion de la cybersécurité dans une activité courante de l'entreprise, constitueront un pas dans la bonne direction.

## *Approches actuelles des entreprises en matière de gouvernance de la cybersécurité*

Historiquement, la cybersécurité a été considérée par les entreprises comme un problème technologique relevant de la compétence de l'équipe informatique. Avec l'augmentation rapide de la numérisation et des cyber-risques, couplée à l'émergence des rôles de CISO et de DPO, la situation a évolué. Cependant, la mise en place d'une gouvernance efficace et mature en matière de cybersécurité apparaît encore comme une perspective lointaine.

Les données d'une enquête menée par le gouvernement britannique en 2023 ont révélé que bien que la cybersécurité soit considérée comme une priorité par les dirigeants d'entreprise, cela ne s'est généralement pas traduit par des mesures précises ou une appropriation au niveau du conseil d'administration. Voici quelques-unes des conclusions de cette étude :

**30%**

des entreprises ont des membres du conseil d'administration ou des administrateurs explicitement responsables de la cybersécurité.

**37%**

des entreprises déclarent être assurées contre les risques liés à la cybersécurité.

**16%**

des rapports annuels des entreprises couvrent les cyber-risques.

**49%**

des moyennes entreprises et 68 % des grandes entreprises ont mis en place une stratégie formelle de cybersécurité.

**29%**

des entreprises ont entrepris une évaluation des risques de cybersécurité au cours des 12 derniers mois.

**13%**

des entreprises ont examiné les risques de cybersécurité posés par leurs fournisseurs immédiats.

## *Stratégies gouvernementales en matière de gouvernance de la cybersécurité*

Comme cela a été décrit dans la section précédente, le Royaume-Uni et la France ont mis en place des cadres réglementaires grandement similaires. Bien qu'il n'y ait pas d'exigence explicite en matière de gouvernance formelle, le RGPD a été très clair sur la responsabilité et la gouvernance, toutes deux illustrées par l'exigence du rôle du délégué à la protection des données.

De son côté, la Directive NIS 2 met davantage l'accent sur la supervision par la direction générale du processus de gestion des risques et sur la responsabilité de la direction en cas d'incident. De telles réglementations renforcent ostensiblement le profil de la gouvernance de la cybersécurité au sein des organisations britanniques et françaises.

Le gouvernement britannique a spécifiquement reconnu l'importance de la gouvernance de la cybersécurité et le manque de maturité dans ce domaine au sein des entreprises.

- En 2018 et 2019, le Centre national de cybersécurité du Royaume-Uni a publié une série de recommandations à l'intention des entreprises, ce qui a abouti à la création d'une "boîte à outils de cybersécurité pour les conseils d'administration" mentionnée dans la section précédente.
- L'année dernière, à la suite de l'enquête susmentionnée, le gouvernement britannique a lancé un code de pratique pour la cybergouvernance. Ce code a été soumis à l'avis du public en janvier 2024. L'objectif de ce code de pratique est de fournir des conseils clairs sur les actions et les responsabilités des membres du conseil d'administration dans la création d'une gouvernance efficace, rédigés dans un langage commun, en minimisant le jargon technique.

## *Normes et bonnes pratiques en matière de gouvernance de la cybersécurité*

La norme ISO/IEC 27001 constitue un excellent cadre pour la gouvernance de la cybersécurité, car elle définit des exigences en matière de politiques, de processus, de rôles, de responsabilités, de communication, d'évaluation et de gestion des risques, de suivi et d'amélioration continue. Cette norme est largement adoptée au Royaume-Uni, avec plus de 6 000 certifications couvrant près de 12 000 sites à la fin de l'année 2022. Ce nombre est en nette augmentation depuis le lancement de la norme actualisée l'année dernière. En France, l'adhésion est plus faible, mais en augmentation, avec plus de 900 certificats couvrant plus de 2 800 sites à la fin de 2022. Elle se fait principalement dans le secteur des TIC, mais aussi dans les services numériques qui soutiennent d'autres secteurs clés.

En tant que norme mondiale, la certification ISO/IEC 27001 renforce également le commerce mondial, en instaurant la confiance d'acteurs du monde entier dans la gouvernance-cybersécurité d'une organisation. Les entreprises du Royaume-Uni et d'Europe utilisent donc la certification ISO/IEC 27001 à la fois pour leur propre développement commercial régional et interne, mais aussi en tant qu'étalon de référence lorsqu'elles évaluent leurs fournisseurs et partenaires internationaux potentiels en fonction du risque de cybersécurité qu'ils présentent.

Un autre référentiel clé au niveau mondial a été créé aux États-Unis par le National Institute of Standards and Technology (NIST). Connu sous le nom de "NIST Cybersecurity Framework", il s'agit d'un programme volontaire principalement destiné à l'auto-évaluation. L'adhésion à ce référentiel est difficile à quantifier car il n'y a pas de processus de certification formel. Au Royaume-Uni et en France, la participation des entreprises apparaît limitée à cet égard.

La norme internationale ISO/IEC 27001:2022 “**Sécurité de l’information, cybersécurité et protection de la vie privée. Système de management de la sécurité de l’information**” présente les meilleures pratiques mondiales en matière de gestion des risques liés à la cybersécurité.

Tirées de l’ISO :

- “Avec l’augmentation de la cybercriminalité et l’apparition constante de nouvelles menaces, il peut sembler difficile, voire impossible, de gérer les cyber-risques. La norme ISO/IEC 27001 aide les organisations à prendre conscience des risques et à identifier les faiblesses de manière proactive.
- La norme ISO/IEC 27001 promeut une approche holistique de la sécurité de l’information... [et] constitue un outil de gestion des risques, de cyber-résilience et d’excellence opérationnelle”.

## *Que doivent faire les entreprises britanniques et françaises en matière de gouvernance de la cybersécurité ?*

1. Examinez la situation actuelle de votre organisation par rapport aux 5 facteurs de bonne gouvernance en matière de cybersécurité énumérés page 37.
2. Examinez dans quelle mesure vous comprenez votre risque résiduel en matière de cybersécurité et dans quelle mesure il correspond à votre appétence pour le risque et à votre stratégie d’entreprise.
3. Examinez dans quelle mesure votre système de gestion de l’information et de la cybersécurité permet à votre organisation de gérer les risques dans ce domaine.

### Des outils pour vous aider :

| | | |
|---|---|---|
| Code de conduite sur la cyber-résilience proposé par le gouvernement britannique. Annexe A | Kit d’outils cyber NCSC du gouvernement britannique pour les conseils d’administration | ISO/IEC 27001:2022 |
| Voir le lien | Voir le lien | Voir le lien |

# *L'avenir de la gouvernance de la cybersécurité*

L'économie numérique étant essentielle à l'économie mondiale et les risques cyber étant de plus en plus nombreux et en constante évolution, les gouvernements du monde entier mettent de plus en plus l'accent sur la gouvernance en matière de cybersécurité. Dans l'UE, la directive NIS 2 se concentre tout particulièrement sur les principes de gouvernance et l'expansion à d'autres secteurs rendra cette question plus pertinente dans toutes les industries. Parallèlement à la mise à jour imminente du NIS britannique, cette évolution devrait inciter de nombreuses entreprises à adopter une position plus ferme en matière de gouvernance de la cybersécurité au Royaume-Uni et en France.

Les exigences des marchés d'investissement en matière de transparence et de confirmation constituent un autre facteur clé qui favorisera l'amélioration de la gouvernance cyber. Aux États-Unis, la Securities and Exchange Commission (SEC) a adjoint une obligation de déclaration visant à couvrir la gouvernance de la cybersécurité et la divulgation des incidents. Cette mesure aura des répercussions sur les chaînes d'approvisionnement ainsi qu'un impact sur les entreprises britanniques et françaises qui fournissent des services aux entreprises américaines. Par ailleurs, un processus similaire est à l'étude au Royaume-Uni, renforçant de la sorte la pression sur les entreprises britanniques cotées en Bourse pour qu'elles formalisent leur parti pris stratégique en matière de gouvernance cyber.

L'essor fulgurant de l'utilisation de l'IA au sein des entreprises de toutes tailles et de tous secteurs est une autre question qui devrait amener à mettre davantage l'accent sur la gouvernance de la cybersécurité. L'IA apporte de nombreux avantages commerciaux, mais aussi de nouveaux défis auxquels il convient de faire face, propres à la sécurité et à la protection de la vie privée. Les questionnements relatifs à la sécurité et la confidentialité de l'IA ont déjà fait couler beaucoup d'encre. Cette recrudescence significative des risques aura pour effet de mettre en évidence encore davantage l'importance de la gouvernance cyber. La combinaison de réglementations supplémentaires (par exemple la loi européenne sur l'IA), d'une gestion générale des risques des entreprises et une actualité faisant inévitablement état d'incidents significatifs devrait conduire à une amélioration de la gouvernance dans tous les secteurs, et cela tout au long de la chaîne d'approvisionnement.

Pour aider les organisations à mettre en œuvre et à maintenir une gouvernance efficace, la norme ISO/IEC 27001 prévoit tout un dispositif venant au soutien des entreprises. De la formation et du conseil jusqu'à l'évaluation et la certification, la norme ISO/IEC 27001 offre à toutes les organisations la possibilité de mettre en œuvre une gouvernance cyber efficace et d'en attester la véracité. D'autres initiatives telles que le code de pratique britannique en matière de cybergouvernance et le Toolkit for Boards du NCSC britannique fournissent des conseils et des outils facilement accessibles pour débuter.

Ainsi, les organisations au Royaume-Uni et en France de tous secteurs, qu'elles soient grandes ou petites, commerciales ou à but non lucratif, ont la possibilité d'attester une gouvernance efficace de la cybersécurité. Cela permet de protéger les intérêts de leurs clients, de leurs employés et de l'ensemble des parties prenantes, tout en constituant un avantage concurrentiel. Dans le même temps, ce mouvement amorce une transformation numérique vers une société intelligente se tournant vers tout ce qui est fiable et sécurisé.

# *Conclusion*

La gouvernance en matière de cybersécurité repose sur une approche holistique, intégrant la cybersécurité au fonctionnement de l'entreprise, et exige de la direction qu'elle s'engage activement sur ce sujet capital. La dépendance croissante des entreprises à l'égard du numérique, couplée à la forte augmentation de la cybercriminalité et au renforcement de la réglementation en découlant fait que la cybersécurité est considérée comme un risque majeur pour les entreprises qui doit être géré de la même manière que d'autres activités clés telles que les finances.

Les principes essentiels d'une gouvernance efficace de la cybersécurité sont bien documentés, accompagnés des meilleures pratiques mondiales formalisées sous la forme d'une norme ISO. Cependant, la mise en place des procédures adaptées est encore relativement immature au sein des entreprises. La réglementation en vigueur dans l'Union européenne et au Royaume-Uni met davantage l'accent sur la gouvernance de la cybersécurité, ce qui contribue à mettre au premier plan cet aspect important de la direction des entreprises.

Tous les chefs d'entreprise devraient s'interroger sur la manière dont leur organisation gère actuellement la cybersécurité. À cet effet, ils peuvent s'inspirer des principes essentiels d'une gouvernance efficace de la cybersécurité et s'appuyer sur divers outils et normes de gouvernance pour en favoriser une mise en œuvre efficiente. Ils doivent notamment se demander s'ils comprennent bien leur risque cyber résiduel et s'il est en adéquation avec leur appétence pour le risque et la stratégie de l'entreprise.

Une gouvernance efficace de la cybersécurité aide à construire une entreprise résiliente qui peut récolter les fruits de ce que des technologies innovantes peuvent offrir, tout en minimisant leurs risques. Elle contribue également à la mise en conformité avec la réglementation croissante en matière de cybersécurité. Enfin, la conformité aux meilleures pratiques mondiales, sous la forme de la norme ISO, contribue à instaurer une confiance numérique auprès des organisations du monde entier. Il en est ainsi meilleur pour nous tous, en tant qu'individus, entreprises et société tout entière.

Au vu de l'importance croissante des considérations juridiques en matière de cybersécurité, en particulier dans le contexte réglementaire de l'UE, **il est essentiel de changer de perspective et de ne plus les considérer uniquement comme une contrainte, mais plutôt comme une opportunité.** Les entreprises ont la possibilité d'exploiter une attention et une transparence accrues en matière de cybersécurité afin d'améliorer leurs performances. Ce changement d'état d'esprit favorise non seulement un environnement commercial plus sûr et plus conforme, mais donne également aux professionnels et aux entreprises les moyens de naviguer habilement dans des cadres réglementaires complexes tout en tirant parti d'informations juridiques précises. Compte tenu de l'engagement du Groupe Lefebvre-Sarrut à tenir les professionnels et les entreprises au courant des réglementations, des normes de conformité et des meilleures pratiques de l'industrie, il est naturel de considérer la cybersécurité comme un catalyseur pour l'amélioration des performances et le développement structurel.

*Candice TRAN DAI*

*Security Director, Lefebvre Dalloz*

**La plupart des acteurs de la menace ont des motivations purement financières. Ils ne se soucient pas d'où vous venez, leur seule préoccupation est de gagner de l'argent.**

Nous fondons nos cadres, nos politiques et nos contrôles de sécurité sur les principes de réglementation de l'UE, mais nous nous efforçons de les appliquer dans toutes les zones géographiques, dans la mesure du possible. Nous prenons en compte les réglementations locales au cas par cas, mais une approche spécifique à un pays n'a guère de sens, car les menaces peuvent venir de n'importe où. C'est pourquoi nous nous efforçons d'avoir partout la même base de référence.

*Guillaume Balix*

*Resilience Lead, CISO Office & Transformation, L'Oréal*

V

# L'Intelligence Artificielle (IA)
## au service des cybercriminels et de ceux qui les combattent

*Nicolas Arpagian*
*Vice-President, HeadMind Partners*
*Senior Lecturer French National Police Academy (ENSP).*

La cybersécurité se conçoit principalement dans deux dimensions :

- D'une part, les atteintes au fonctionnement des systèmes d'information avec des prises de contrôle à distance, des interceptions et des mises hors d'état de fonctionner.
- D'autre part, des attaques informationnelles fondées sur l'usurpation d'identité, le dénigrement et des fraudes intégrant des éléments mensongers ou l'exploitation de données piratées.

Dans ce monde numérisé, la capacité d'automatisation, de génération de contenus sous des formes variées et de création mécanisée de l'Intelligence Artificielle (IA) expliquent aisément que cette technologie soit déjà un terrain d'expérimentations et d'actions pour les organisations criminelles. Cela correspond en outre à la règle éprouvée qui veut que les escrocs adoptent toujours de manière précoce et anticipée les solutions techniques leur permettant d'améliorer leurs gains et d'amplifier leurs opérations.

## *Des données recherchées, des données exposées, donc des données à protéger*

L'Intelligence Artificielle a besoin de données pour fonctionner. Et d'un savoir-faire mathématique pour concevoir la mécanique algorithmique permettant de les valoriser. La chasse est donc désormais ouverte afin d'accéder aux informations pertinentes pour alimenter des modèles d'IA. Ainsi, dans le cas des IA génératives (LLM), leur aptitude à produire des contenus susceptibles de convaincre leurs destinataires (courriels, messages audio, séquences vidéo…) exige d'avoir préalablement identifié les éléments de vocabulaire, les noms/fonctions des personnes invoquées, et le scénario le plus à même de conduire à la concrétisation de l'action visée. Par exemple, une demande de procéder à une démarche émanant prétendument d'une autorité légitime ou l'amorce d'une polémique par la prétendue tenue de propos diffamatoires ou outranciers par une personnalité. En l'espèce, un recours à l'IA permettra au criminel de gagner en crédibilité pour faire valoir sa demande avec une mise en scène utilisant précisément les codes sociaux de sa cible. Une nouvelle fois, la technologie ne crée pas de nouvelles fraudes mais permet de les porter à un niveau de qualité et de détail qui les rend plus difficilement détectable.

La menace sur les données dans le cadre d'un usage d'IA ne porte pas que sur le vol. Mais aussi sur leur fuite, qui peut être aussi involontaire faute de comprendre le fonctionnement des outils. À l'instar de salariés de la société Samsung Electronics qui au printemps 2023 ont injecté[1] des informations confidentielles appartenant à leur entreprise pour utiliser ChatGPT. Rendant potentiellement accessibles lesdits éléments à un utilisateur ultérieur. Les politiques d'interdiction technique, par le blocage mécanique d'accès aux sites de LLM, décidées par certains comités de direction, sont vaines. Puisque les moyens de contournement, avec un téléphone portable ou un ordinateur personnel, sont à la portée de tous. C'est bien une approche pédagogique qu'il convient d'adopter pour limiter de tels mésusages.

*[1] Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak, Bloomberg, May 2nd, 2023. https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak*

Voir le lien

## *Des fraudes éminemment humaines*

L'illustration ultime de la contribution d'une Intelligence Artificielle à un dispositif frauduleux bâti sur l'expérience humaine est le recours à des productions de deepfakes. Sur le modèle de celle proposée à ce salarié de Hong Kong qui s'est vu intimer l'ordre[2] lors d'une visioconférence avec son comité de direction en début d'année 2024 de procéder à un virement de 25 millions de dollars. Tout semblait vrai : l'apparence des participants à la réunion, le vocabulaire employé, le ton de la voix des protagonistes… Une illusion parfaite qui a eu raison des réticences naturelles et des règles de procédure. Une usurpation obtenue par un travail conséquent d'ingénierie sociale et le

maniement des outils de *computer vision & image processing*. Il s'agit ici d'adapter un mécanisme d'escroquerie avec des capacités logicielles de plus en plus accessibles. Le pilotage de ces outils pourtant très complexes est simplifié par l'instauration d'interfaces appréhendables par des non-spécialistes.

[2] *Finance worker pays out $25 million after video call with deepfake 'chief financial officer', CNN, February 4. 2024.*
*https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html*

Voir le lien

## *Une IA utilisée aussi en défense*

La modélisation mathématique est particulièrement pertinente dans un univers techniquement normé. Elle fait des merveilles pour détecter des anomalies, des doublons, des oublis ou des fonctions superfétatoires dans des programmes informatiques. Ainsi, dans un contexte de pénurie d'experts en cybersécurité, le passage en revue des logiciels et des systèmes par des IA est de nature à gagner en efficacité. Notamment pour des tâches fastidieuses et donc peu attractives pour des praticiens.

Les algorithmes peuvent servir également à établir des scénarios d'attaque à des fins d'entraînement. Des facultés de simulation de nature à élaborer des dispositifs de protection. Alors que nombre d'éditeurs de solutions d'IA affichent dans leurs conditions générales d'utilisation l'interdiction d'employer leurs outils à des fins malveillantes, l'imagination des pirates dans la formulation de consignes de production (prompts) permet de contourner ces bridages techniques. Cette maîtrise des techniques offensives par l'IA documente utilement des méthodes de détection de comportements malintentionnés générés par des Intelligences Artificielles. La compréhension des modes opératoires des attaquants est mise à contribution pour élaborer des stratégies d'identification et donc de neutralisation des maliciels et autres vecteurs de fraude conçus ou animés par des instances algorithmiques. L'alliance de puissances de calcul adaptées et de l'ingéniosité humaine pour concevoir des situations propices à convaincre les adversaires d'effectuer des tâches est particulièrement redoutable. Ces travaux intéressent tant les états-majors militaires, les services de renseignement que les organisations criminelles. Ce qui signifient que les entreprises, les administrations, les collectivités et même les particuliers directement comme autant de portes d'entrée pour atteindre des cibles institutionnelles, sont susceptibles d'être visés par ces campagnes mêlant technologies et ingénierie sociale.

Plus que jamais, les délimitations entre les mondes militaires, économiques et la sphère grand public deviennent poreuses. Confirmant la notion des « frontières.com », analysée et documentée dans ce livre éponyme[3].

[3] *Frontières.com, Nicolas Arpagian, Editions de l'Observatoire, 2022.*

## *Des technologies d'IA intégrées dans l'arsenal des États et de leurs sous-traitants*

Les parades militaires sont l'occasion pour les gouvernements d'afficher aux yeux du monde leurs matériels et l'ampleur de leur puissance de feu. Difficile de transposer cet affichage hautement symbolique avec les ressources cyber, même si les unités de cybercombattants trouvent de plus en plus leur place dans les défilés aux côtés des armes conventionnelles. Néanmoins, les déclinaisons de l'Intelligence Artificielle sont d'ores et déjà intégrées dans l'arsenal offensif des États.

Ainsi, en février 2024, les sociétés Microsoft et OpenAI affirment officiellement dans un document[4] public que des entités affiliées à la Corée du Nord, à l'Iran, la Chine et la Russie conduisaient des expérimentations combinant l'IA et des grands modèles de langage (LLM) pour compléter leurs opérations de cyberattaque. Les deux firmes ont indiqué que les travaux concernaient diverses phases de la chaîne d'attaque, telles que la reconnaissance, l'assistance au codage et le développement des logiciels malveillants. Elles ont établi que les pirates sollicitaient OpenAI pour interroger des bases de données accessibles en sources ouvertes, effectuer des traductions, repérer des erreurs de codage et exécuter des tâches de codage de base. La communication des deux éditeurs précise qu'ils ont stoppé ces activités en bloquant notamment leurs comptes utilisateurs.

*[4] Staying ahead of threat actors in the age of AI - Microsoft Threat Intelligence – February 14, 2024*
*https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/*

Voir le lien

## *Un cadre juridique qui cherche à anticiper les dérives, mais sans brider l'innovation*

Alors que la vague ChatGPT a inondé le monde en laissant le grand public accéder à ses services en novembre 2022, les principaux États ont dans la foulée cherché à juguler les menaces nées d'un usage malveillant de ces modèles algorithmiques mis à portée de claviers. En octobre 2023, le Président Biden a ainsi signé un décret[5] qui établit en termes non équivoques que « les développeurs des plus puissants services d'IA devront partager les informations relatives à leur sûreté et à tout sujet jugé critique avec le gouvernement fédéral ». Une exigence qui démontre l'importance pour l'Exécutif US de disposer d'une connaissance intime du fonctionnement de ces systèmes complexes. La Chine a de son côté adopté une loi[6] dédiée, entrée en vigueur le 15 août 2023. En Europe, le Parlement européen a approuvé, en mars 2024 le texte final d'un nouveau Règlement : l'IA Act[7].

Ce corpus juridique a pour objectif de veiller à « ce que les systèmes d'IA mis sur le marché européen et utilisés dans l'UE soient sûrs et à ce qu'ils respectent les droits fondamentaux et les valeurs de l'UE ». Les termes employés caractérisent l'équilibre visé entre une volonté de ne pas brider des innovations de nature à contribuer à la compétitivité et au leadership technologique du Vieux Continent, et de laisser sans contrôle ni encadrement de possibles usages nocifs qui sont encore loin d'être tous documentés.

[5] *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence - White House - October 30.2023 - https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/* Voir le lien

[6] *Interim Measures for the Management of Generative Artificial Intelligence Services - July 13. 2023 - Cyberspace Administration of China - www.cac.gov.cn/2023-07/13/c_1690898327029107.htm* Voir le lien

[7] *Artificial intelligence act : Council and Parliament strike a deal on the first rules for AI in the world – February 2nd. 2024 - https://www.consilium.europa.eu/fr/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/* Voir le lien

# *Conclusion*

Habitués à maîtriser l'ordonnancement des règles de vie en société, et avec l'avènement de l'ère de l'IA, les États se trouvent impliqués dans une triple compétition pour conserver leur magistère sur leurs populations respectives et en matière de géopolitique. D'une part, pour acquérir et maîtriser les infrastructures techniques (GPU, serveurs, services de clouds...) nécessaires au fonctionnement des modèles d'Intelligence Artificielle. D'autre part, pour attirer et fidéliser les talents capables de concevoir et de piloter ces batteries d'algorithmes. Enfin, pour s'organiser de manière à ne pas se laisser concurrencer par des organisations privées – qu'elles soient strictement commerciales ou criminelles – qui par leur taille, leur rayon d'action et leur puissance financière en viendraient à discuter l'autorité légitime des instances gouvernementales. La rapidité de conception, d'exécution et de diffusion de ces outillages numériques est sans précédent. D'autant que les impacts concernent l'ensemble du spectre des activités humaines : santé, éducation, industrie, gestion, arts, commerce, administrations... ainsi que les activités illicites. Autant de ruptures technologiques qui exigent une appropriation accrue de ces thématiques relatives à l'Intelligence Artificielle tant par les autorités démocratiques que par les citoyens.

## *Contributeurs*

- **Richard Absalom**, *Principal Research Analyst,* **Information Security Forum Limited (ISF)**
- **Nicolas Arpagian**, *Vice President*, **HeadMind Partners**
- **France Charruyer**, *Founder, Lawyer & Partner, IP, IT & Data*, **Altij**
- **Nicholas Cullen**, *Lawyer, Partner, Data, IT & Corporate , Solicitor of England and Wales,* **Altij**
- **Mahé Dersoir**, *Policy Officer at the Cyber Policy Unit,* **Ministère de l'Europe et des affaires étrangères**
- **David Mudd**, *Global Head of Digital Trust Assurance,* **British Standard Institution (BSI)**
- **James Pearn**, *Head of Innovation, Health and Creative - Trade,* **British Embassy Paris**

## *Sous la présidence de*

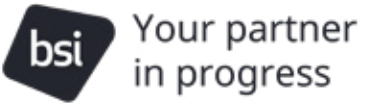
**Olivier Campenon**, *Chairman of the* **Cross-Channel Institute**, *CEO,* **Group Lefebvre**

## *Directrice de la publication*

**Catherine Le Yaouanc**, *General Manager,* **Franco-British Chamber**

## *Coordination*

**Jérôme Testut,** *Head of Communications, Marketing & Partnerships,* **Franco-British Chamber**






**Avec le soutien de**

Cette analyse sectorielle dédiée à la cybersécurité est une publication du Cross-Channel Institute, le think tank de la Franco-British Chamber.

Les contributeurs de cette étude sont Altij, British Standard Institution, HeadMind Partners et Information Security Forum. Les opinions et les interprétations contenues dans ce rapport sont exclusivement et uniquement celles de la Franco-British Chamber et des partenaires susmentionnés.

**Cross-Channel Institute**
c/o Franco-British Chamber
22 rue de Londres - 75009 Paris
+33 (0) 1 53 30 81 30
contact@crosschannelinstitute.com
**www.crosschannelinstitute.com**

Linkedin : Cross-Channel Institute
Twitter : @CrossCInstitute
Instagram : crosschannelinstitute
Facebook : Cross-Channel Institute