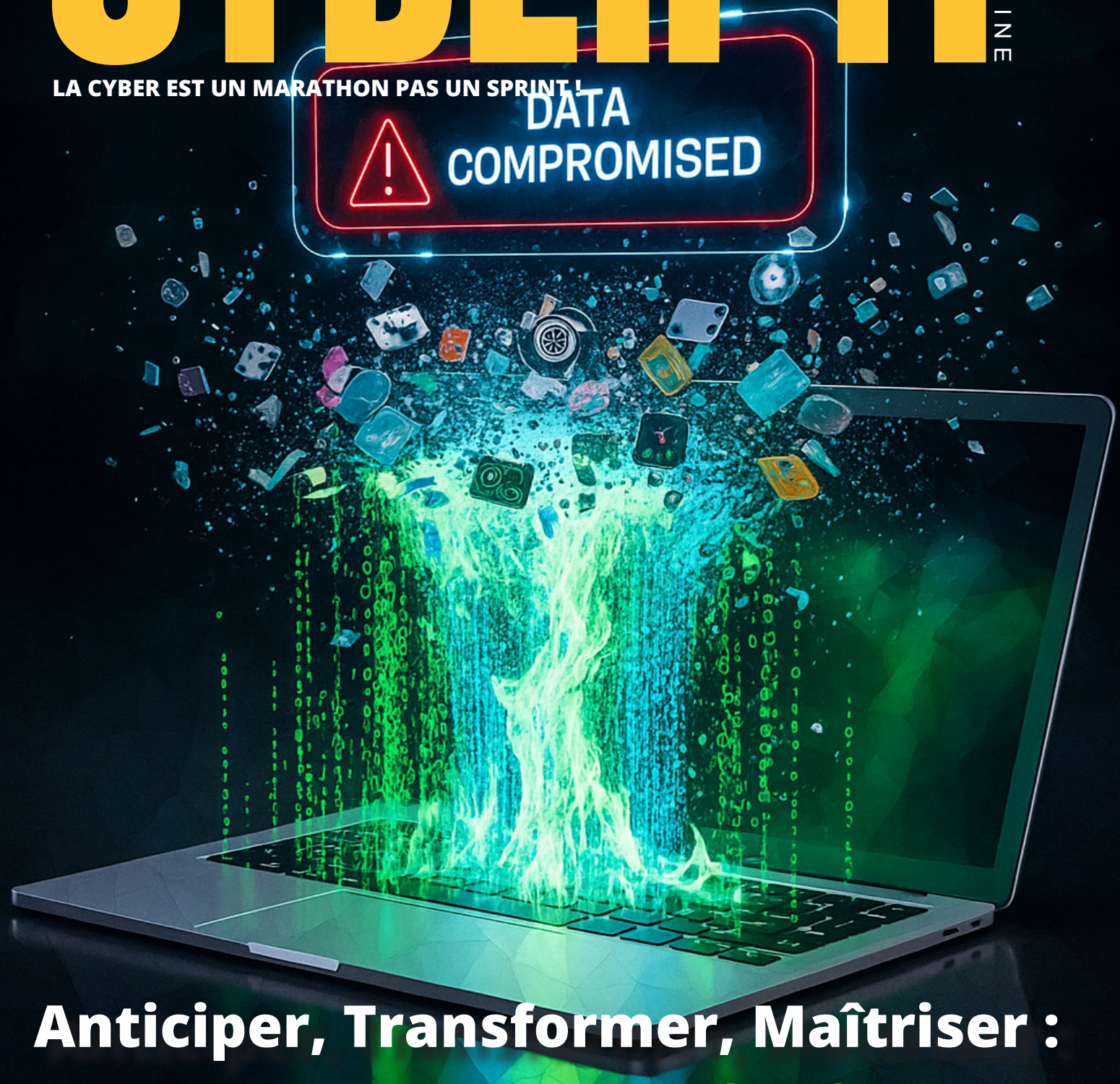
HORS-SÉRIE° 2

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !



Anticiper, Transformer, Maîtriser : L'essence de la GRC

En partenariat avec crise box

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Chers lecteurs,

Notre dossier concernant la GRC, composé de plusieurs posts et d'un sondage, a été très apprécié et vous nous avez sollicités pour que l'on puisse regrouper les éléments en un seul numéro spécial. Voilà, chose faite !

Vous avez donc sous les yeux le second hors-série qui est entièrement consacré à la gestion, au risque et à la gouvernance. Il est parfois difficile de parler de ces sujets sans répéter les mêmes choses au fil des pages. Nous avons donc essayé de mettre en corrélation les différentes normes et règlements avec une réalité de terrain. Comment les certifications ou les règles imposées peuvent contribuer au développement de la confiance client ? Est-ce un vrai bon investissement que de faire le nécessaire pour être certifié ?

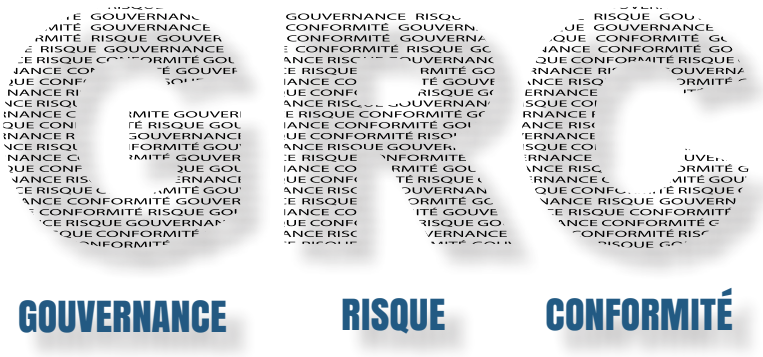
Y a-t-il eu des cas où la GRC aurait pu éviter ou tout au moins atténuer les dégâts causés par une cyberattaque ? C'est à ces questions que nous avons tenté de répondre. Il est évident que toutes les normes et réglements n'ont pas pu être abordés dans ce hors-série, tant le sujet est complexe et vaste. Néanmoins nous avons voulu mettre en avant les éléments suivants : DORA, NIS2, ISO27001 ainsi que le RGPD.

Chaque brique de ce shéma complèxe de la GRC a son rôle à tenir, aujourd'hui il est essentiel pour chacun de mieux comprendre et appréhender ce qu'est la GRC et comment elle peut être utile et même parfois salvatrice dans nos entités.

Je vous souhaite une excellente lecture !

ARNAUD LEROY

SOMMAiRE



Bien avant que le terme cybersécurité ne s'impose dans le langage courant, la gouvernance et la gestion des risques occupaient déjà une place centrale dans l'organisation des sociétés humaines. Depuis toujours, les hommes ont cherché à se prémunir contre l'incertitude, à protéger leurs biens et à instaurer des règles collectives pour prévenir les abus. L'histoire regorge d'exemples où la recherche de sécurité et de prévisibilité a façonné les pratiques économiques et sociales.

Dans l'Antiquité, les marchands phéniciens, réputés pour leurs routes maritimes commerciales, mettaient en commun des fonds destinés à compenser les pertes liées aux naufrages ou aux attaques de pirates. Cette forme embryonnaire d'assurance illustre déjà une compréhension intuitive de la mutualisation du risque. Quelques siècles plus tard, les guildes médiévales imposent des chartes et des mécanismes de solidarité interne. Leur but : protéger leurs membres contre les faillites individuelles, encadrer la concurrence et limiter la fraude. Ces pratiques, loin d'être anecdotiques, posent les jalons de ce que l'on qualifierait aujourd'hui de dispositifs de contrôle et de conformité.

Avec l'émergence de l'informatique dans les années 1960-1970, la donne change radicalement. L'information devient un actif critique, au même titre que les infrastructures ou les biens matériels. Pour la première fois, les organisations doivent penser à protéger non seulement des biens physiques, mais aussi des données, des systèmes et des réseaux.

Les premiers audits informatiques voient le jour, souvent menés par des pionniers qui improvisent des méthodes de vérification dans un univers encore peu structuré. Mais l'importance de ces démarches va croître à mesure que les systèmes d'information deviennent le cœur battant de l'économie moderne.

Des scandales pour tout changer

Le véritable tournant s'opère au début des années 2000. Les scandales financiers retentissants d'Enron et de WorldCom révèlent au grand jour les dérives possibles d'un système dépourvu de contrôles robustes. La chute de ces géants, qui manipulaient leurs comptes pour masquer leurs pertes, provoque une onde de choc mondiale. En réaction, le Congrès américain adopte en 2002 la loi Sarbanes-Oxley. Ce texte impose la transparence des pratiques financières, des mécanismes de contrôle internes solides et engage directement la responsabilité pénale des dirigeants. Il marque le point de départ de la formalisation moderne de la GRC. Initialement pensée pour la finance, cette approche intégrée s'élargira rapidement à d'autres domaines, dont le numérique.

Car pendant que les régulateurs redéfinissent les règles financières, le monde numérique devient le théâtre d'une autre révolution. Le début des années 2000 est marqué par une série d'attaques informatiques spectaculaires. Le ver SQL Slammer en 2003 se propage en quelques minutes seulement, affectant des dizaines de milliers de serveurs et perturbant durablement des services essentiels, allant des distributeurs de billets aux systèmes de réservation aérienne.

Quelques mois plus tard, le virus Blaster infecte des millions de machines et oblige Microsoft à revoir en profondeur ses mécanismes de sécurité. Puis vient MyDoom, considéré comme l'un des vers les plus destructeurs de l'histoire, qui ralentit Internet à l'échelle mondiale. Ces attaques démontrent brutalement que la résilience numérique est devenue aussi cruciale que la solidité des bilans comptables.

L'exportation en Europe

L'Union européenne prend alors conscience de la nécessité de protéger ses infrastructures et ses citoyens. À travers un vaste chantier réglementaire, elle entend affirmer sa souveraineté numérique. L'adoption du **RGPD en 2018** constitue un tournant : pour la première fois, les données personnelles deviennent un objet de régulation exigeant. Les entreprises doivent documenter la gestion de leurs risques, notifier toute violation dans un délai de 72 heures et concevoir leurs services selon le principe du privacy by design. Cette obligation transforme en profondeur la manière dont les organisations collectent, stockent et utilisent les données.

Mais l'Europe ne s'arrête pas là, **la directive NIS de 2016, renforcée en 2022** par NIS2, impose des standards de sécurité stricts aux secteurs jugés stratégiques : santé, énergie, transports, numérique, administrations publiques. **Le règlement DORA, applicable à partir de 2025**, vise à renforcer la résilience opérationnelle du secteur financier. Enfin, **le Cyber Resilience Act**, élargit encore le spectre en imposant à tous les fabricants de produits numériques de prendre en compte la cybersécurité dès la conception. En France, c'est l'ANSSI qui pilote la stratégie nationale. Sa méthode EBIOS Risk Manager, révisée en 2018, aide les organisations à identifier et hiérarchiser leurs risques en partant des enjeux métiers. Elle incarne une approche pragmatique : ne pas se limiter aux aspects techniques, mais prendre en compte la valeur stratégique de l'information et l'impact potentiel d'une attaque sur l'activité.

L'ANSSI s'appuie également sur des référentiels exigeants **SecNumCloud** pour les prestataires de services cloud, **PASSI** pour les auditeurs de sécurité, **PDIS** pour les prestataires de détection qui structurent tout un écosystème de confiance.

À l'échelle internationale, un langage commun s'est imposé : celui des **normes ISO**. La **27001**, centrée sur la sécurité de l'information, est devenue incontournable pour prouver la maturité d'une organisation. Elle est complétée par la **27005** sur la gestion des risques, la **27701** sur la protection de la vie privée et la **31000** sur le management global des risques. Ensemble, ces normes composent un écosystème robuste, reconnu sur tous les continents, qui facilite les échanges et renforce la confiance entre partenaires économiques.

Mais l'avenir réserve des bouleversements d'une ampleur inédite. L'informatique quantique, en développement rapide, menace de rendre obsolètes les systèmes de chiffrement actuels. Les algorithmes RSA ou ECC, qui sécurisent aujourd'hui nos communications, pourraient être cassés en quelques secondes par les ordinateurs quantiques de demain. D'où la course mondiale vers des protocoles dits « post-quantiques », capables de résister à cette puissance de calcul décuplée. En parallèle, l'essor de l'intelligence artificielle générative rebat les cartes du cybercrime. Déjà, des campagnes de phishing entièrement automatisées voient le jour, avec des messages d'une qualité linguistique et stylistique quasi indétectable. Les deepfakes, eux, permettent de reproduire la voix ou le visage d'une personne à des fins de fraude, de chantage ou de désinformation.

LE SAVIEZ-VOUS ?

En 2019, une entreprise britannique nomée Arup a perdu près de 26 Millions de dollars après que des escrocs eurent utilisé une imitation vocale générée par IA pour tromper son dirigeant.

Face à ces menaces, la GRC devra évoluer. Elle ne pourra plus se limiter à appliquer des normes et à cocher des cases de conformité. Elle devra intégrer l'intelligence artificielle dans ses outils de détection et d'anticipation, élaborer des scénarios prospectifs, anticiper l'arrivée de nouvelles réglementations internationales et construire une véritable résilience collective.

C'est à cette condition que nos sociétés pourront continuer à fonctionner dans un environnement numérique en perpétuelle mutation, où les menaces évoluent aussi vite que les technologies censées les contrer.

RGPD

Règlement Général sur la Protection des Données

Anatomie d'une révolution numérique européenne

Derrière les centaines d'articles du règlement, il y a un objectif simple mais fondamental : redonner aux citoyens le contrôle sur leurs données personnelles et restaurer la confiance dans l'économie numérique.

Lorsqu'il est **entré en application le 25 mai 2018,** le Règlement général sur la protection des données, plus connu sous son acronyme **RGPD**, a marqué une rupture historique dans la manière dont les informations personnelles sont gérées et protégées.

Rarement un texte de loi européen aura eu un tel retentissement international.

Pour certains, il a représenté une contrainte lourde, un frein administratif ou une montagne de paperasse. Pour d'autres, il a été un acte fondateur, un rempart contre les excès d'un capitalisme numérique où l'individu était devenu un produit, sa vie privée réduite à un flux monnayable de données. La portée de ce texte dépasse largement les frontières de l'Union européenne. Aujourd'hui, qu'il s'agisse de start-up californiennes, de groupes bancaires asiatiques ou de géants du e-commerce sud-américains, tous doivent prendre en compte les exigences du RGPD dès lors qu'ils traitent des données appartenant à des citoyens européens.

Le règlement a ainsi imposé une nouvelle philosophie : la donnée n'est pas une ressource illimitée que l'on exploite sans considération, mais un bien fondamental qui engage des responsabilités éthiques, économiques et politiques.

Pour comprendre la naissance du RGPD, il faut remonter aux années 1990, lorsque l'Union européenne tenta une première harmonisation avec **la directive 95/46/CE**.

Cette directive posait déjà quelques principes généraux de protection, mais comme toute directive, elle laissait aux États membres la liberté d'adapter son contenu dans leur droit national. Résultat : une mosaïque réglementaire où la France, l'Allemagne, l'Espagne ou encore l'Irlande adoptaient des régimes juridiques parfois très différents.

Une multinationale opérant dans plusieurs pays devait se plier à autant de régimes qu'elle avait de marchés, créant une complexité juridique coûteuse et fragilisant la confiance des consommateurs.

La donne changea radicalement dans les années 2000 avec l'explosion d'Internet, l'émergence des géants du numérique et la collecte massive de données personnelles. L'affaire Snowden en 2013, révélant l'ampleur de la surveillance de la NSA, renforça la conviction des décideurs européens : il fallait un texte plus fort, plus homogène et capable de tenir tête aux appétits des États comme des entreprises.

C'est ***Viviane Reding***, alors commissaire européenne à la Justice, qui lança le chantier d'un nouveau règlement en 2012. Après des années de débats intenses, souvent marqués par la pression des lobbys technologiques, **le texte fut adopté en avril 2016**

Son objectif ?

Derrière la technicité juridique du texte, les objectifs du RGPD sont multiples et profondément politiques.

Source : CNIL

Le premier est de **protéger les individus** face à l'industrialisation du traitement des données.

Dans une économie où tout se mesure, s'archive et se revend, le citoyen risquait de devenir une simple variable statistique. Le RGPD entend restaurer un équilibre : la donnée appartient d'abord à l'individu, et son traitement doit respecter ses droits fondamentaux.

Le deuxième objectif est **économique et stratégique**. En harmonisant les règles à l'échelle européenne, l'Union crée un marché unique de la donnée. Une start-up de Barcelone ou de Varsovie peut traiter des données dans les mêmes conditions juridiques qu'une multinationale à Paris ou Berlin. Cette simplification renforce la compétitivité et limite les distorsions.

Le troisième objectif est **géopolitique**. L'Europe entend s'imposer comme un « empire du droit », capable d'exporter ses normes. Grâce à son extraterritorialité, le RGPD contraint même les géants américains et asiatiques à respecter ses règles s'ils veulent accéder au marché européen. Cette affirmation de souveraineté place l'UE au centre de la régulation mondiale de la donnée, face aux modèles libéraux des États-Unis et autoritaires de la Chine.

Enfin, l'objectif est aussi **démocratique**. Dans une époque marquée par les manipulations d'opinion (Cambridge Analytica en 2018 en est un symbole), le RGPD vise à protéger la liberté de pensée et d'expression en empêchant une exploitation abusive des données personnelles à des fins politiques.

Son contenu ?

Le RGPD compte 99 articles et 173 considérants. Mais derrière cette architecture juridique, on peut identifier plusieurs piliers structurants :

Les principes de base

Les traitements de données doivent respecter les principes de licéité, loyauté et transparence ; limitation des finalités ; minimisation ; exactitude ; limitation de la conservation ; intégrité et confidentialité ; et responsabilité. Ces principes posent une logique de sobriété et de rigueur : collecter moins, sécuriser plus, documenter toujours.

Les droits des personnes

Le RGPD renforce les droits existants (accès, rectification, opposition) et en crée de nouveaux comme la portabilité et le droit à l'effacement. Ces droits permettent aux citoyens de reprendre la main sur leurs données et imposent une transparence inédite aux organisations.

Les obligations des organisations

Les responsables de traitement et leurs sous-traitants doivent tenir des registres, notifier les violations sous 72h, désigner un DPO dans certains cas, et réaliser des analyses d'impact pour les traitements à haut risque. L'approche n'est plus déclarative (comme sous la directive de 1995), mais responsabilisée : l'organisation doit prouver à tout moment sa conformité.

Les autorités et les sanctions

Chaque État dispose d'une autorité indépendante (CNIL en France, ICO au Royaume-Uni, etc.) qui coopère au sein du Comité européen de la protection des données (EDPB). Les sanctions peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel, ce qui donne au règlement une force de frappe redoutable.

Pour qui ?

Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union européenne et/ou que son activité cible directement des résidents européens.

ÉCONOMIE DE LA CYBERSÉCURITÉ ET BÉNÉFICES DU RGPD

Étude de la CNIL

L'économie de la cybersécurité explique que les entreprises prennent leurs décisions d'investissement en comparant les coûts et les bénéfices directs pour elles-mêmes. Toutefois, ces décisions ne tiennent pas toujours compte des effets sur la société dans son ensemble.

Le cybercrime ne touche pas seulement l'entreprise victime : il peut affecter ses clients, ses partenaires et même d'autres entreprises via un risque de contagion. Ces impacts sont appelés externalités négatives. Par conséquent, le niveau d'investissement en cybersécurité est souvent inférieur à ce qui serait optimal pour la société. Le RGPD corrige ces déséquilibres. Il ne se limite pas à obliger les entreprises à internaliser les externalités, c'est-à-dire à prendre en compte les conséquences de leurs actions sur la société, mais il agit aussi sur l'information et la sensibilisation.

Un exemple concret de l'impact du RGPD concerne les violations de données personnelles. Sans réglementation, une entreprise n'est pas obligée de révéler une fuite de données, ce qui laisse les clients exposés aux conséquences négatives, comme l'usurpation d'identité. Certaines entreprises peuvent être incitées à communiquer sur de petites failles pour protéger leur réputation, mais elles ont tendance à cacher les incidents majeurs afin d'éviter des dommages à leur image. Cette asymétrie d'information contribue au sous-investissement en cybersécurité.

La mise en place de l'obligation de notification des viola-

tions de données responsabilise les entreprises et incite à investir davantage pour éviter des pertes financières et une dégradation de leur réputation.

Les études montrent que ces communications réduisent le nombre d'usurpations d'identité, démontrant ainsi l'effet positif de la réglementation sur la sécurité.

L'interdépendance des entreprises constitue un autre facteur de sous-investissement. Une cyberattaque peut se propager d'une entreprise à l'autre, comme l'illustrent le virus WannaCry ou les botnets, qui utilisent des ordinateurs infectés pour commettre divers actes malveillants. Lorsqu'une entreprise investit en cybersécurité, elle vise surtout à protéger ses propres systèmes, sans toujours tenir compte de l'impact sur l'ensemble de l'écosystème. De plus, dans le cas de relations de sous-traitance, la sécurité des données dépend du niveau de protection du sous-traitant. Si celui-ci néglige ses investissements, le responsable de traitement est exposé.

Le RGPD impose la responsabilité juridique du sous-traitant, ce qui l'incite à maintenir un niveau de sécurité élevé et améliore la cybersécurité globale.

Le marché des rançongiciels est un autre exemple de l'importance des externalités. Le montant des rançons que les cybercriminels exigent dépend de la disposition des victimes à payer. Les entreprises qui ne prennent pas de mesures de cybersécurité augmentent la demande de rançons, ce qui accroît le coût pour la société dans son ensemble. Cela illustre à nouveau le sous-investissement en cybersécurité et la nécessité d'une intervention réglementaire pour corriger cette externalité.

Les modèles économiques, comme celui de Gordon et Loeb, montrent que le sous-investissement des entreprises peut être significatif, représentant entre 20 % et 66 % de l'investissement optimal lorsque l'on prend en compte les externalités. Les données d'Eurostat indiquent que l'entrée en vigueur du RGPD a conduit à une augmentation des mises à jour des protocoles de cybersécurité dans les entreprises françaises, confirmant son impact positif sur la prévention du cybercrime.

Une étude de cas sur les usurpations d'identité permet de quantifier certains bénéfices directs du RGPD.

> **En France, la communication obligatoire des violations de données a permis d'éviter entre 90 et 219 millions d'euros de pertes sur quatre ans.**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

À l'échelle de l'UE, ces gains se situent entre **585 millions et 1,4 milliard d'euros**. Une large part de ces gains, environ 82 %, bénéficie aux entreprises, tandis que le reste profite aux individus. Ces gains ne tiennent compte que des usurpations d'identité et ne considèrent pas d'autres types de cybercrime, comme les rançongiciels, ni l'impact des mesures de sécurité obligatoires prévues par le RGPD, ce qui suggère que l'impact réel pourrait être encore plus important.

Au-delà de la communication des violations, le RGPD encourage également l'adoption de mesures de sécurité comme le chiffrement, la minimisation des données collectées et la limitation de leur durée de conservation. Ces mesures réduisent le coût moyen des cyberattaques et limitent l'exposition des individus et des entreprises aux risques. Elles contribuent à renforcer la confiance dans les activités en ligne et favorisent l'innovation en sécurisant les services numériques.

En conclusion, le RGPD incite les entreprises à investir davantage en cybersécurité, ce qui profite non seulement à elles-mêmes, mais aussi à leurs clients, partenaires et concurrents. Les chiffres présentés ne représentent qu'une partie des avantages potentiels, et de nombreuses autres pistes restent à explorer pour mesurer l'impact complet du RGPD sur la cybersécurité.

La réglementation, en combinant obligations légales et sensibilisation, contribue donc à un environnement numérique plus sûr et résilient pour l'ensemble de la société.

NIS 2 : l'Europe veut transformer la cybersécurité en une assurance collective

Adoptée en décembre 2022 et transposée en droit national depuis octobre 2024, la directive NIS 2 (Network and Information Security) élargit et renforce le cadre européen de cybersécurité. Elle succède à NIS 1, jugée trop limitée.

Le principe est simple : imposer à un plus grand nombre d'entreprises et d'administrations de renforcer leur cybersécurité, avec des obligations précises en matière de gestion des risques, de gouvernance, de détection et de signalement des incidents.

Là où NIS 1 ne visait qu'une poignée de secteurs stratégiques (énergie, transport, santé), NIS 2 concerne désormais **plus de 160 000 entités en Europe**, y compris des acteurs de la logistique, des services postaux, de la chimie, de la production industrielle et même certaines administrations publiques. L'ANSSI, en tant qu'autorité nationale en matière de cybersécurité et de cyberdéfense, pilote la transposition en droit national de la directive et assure sa mise en œuvre.

La transposition de la directive a commencé par une phase de préparation du projet de loi, qui a été présentée en Conseil des Ministres le 15 octobre 2024 et déposée au Parlement en vue de son adoption dans les prochains mois.

Dans les mois suivants, la promulgation de la loi, la transposition se poursuivra par la phase de production des décrets et arrêtés. NIS 2 entrera en vigueur en France dès que l'ensemble des textes de transposition (loi, décrets, arrêtés) sera promulgué. Il est utile de préciser que la date d'entrée en vigueur ne correspond pas à la date d'application de l'ensemble des exigences réglementaires qui seront imposées aux entités régulées.

Son objectif ?

Selon **Vincent Strubel** , Directeur général de l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**)

> ***La directive NIS 2 permet d'élever le niveau global de cybersécurité par l'application de règles harmonisées et simplifiées. Face à une cybermenace qui s'accroît, NIS 2 relève le défi d'une meilleure sécurisation des tissus économique et administratif de la France.***

Les exigences prévues par la directive européenne invitent de nombreuses entités à construire une solide

feuille de route pour déployer et renforcer leurs moyens de cyberdéfense, avec pour objectifs un fonctionnement structurel plus sûr, davantage de confiance vis-à-vis de leurs parties prenantes et une meilleure compétitivité pour les entreprises.

À terme, et de concert avec les autres États membres de l'Union européenne (UE), c'est une maturité cyber à l'échelon européen que nous voulons atteindre.

Son contenu ?

En pratique, on peut considérer que NIS 2 comprend environ **44 articles principaux** qui codifient toutes les obligations. Chaque article contient souvent plusieurs paragraphes ou « sous-règles » qui précisent les exigences.

Les organisations doivent être en mesure d'identifier, d'analyser et de traiter les menaces susceptibles de toucher leurs systèmes d'information.

Cela passe par la mise en place de politiques de cybersécurité formelles, ainsi que par l'élaboration de plans de continuité d'activité et de réponse aux incidents.

En matière de notification, toute attaque ou incident ayant un impact significatif doit impérativement être signalé aux autorités nationales compétentes dans un délai maximum de 24 heures lorsqu'il s'agit d'incidents majeurs. Un rapport plus détaillé doit ensuite être fourni dans les 72 heures, afin de permettre une évaluation complète de la situation et une réponse adaptée.

Les entreprises doivent nommer un responsable de la cybersécurité, souvent un Chief Information Security Officer, chargé de piloter la stratégie en la matière. Les rôles et responsabilités doivent être clairement définis et les conseils d'administration ont l'obligation d'assurer un suivi régulier et rigoureux des mesures mises en place.

Des audits réguliers et des mesures de sécurisation spécifiques doivent être menés pour limiter les risques liés aux partenaires externes.

Enfin, la formation et la sensibilisation des collaborateurs sont considérées comme essentielles pour réduire le facteur de risque humain.

Pour qui ?

Désormais, **deux catégories d'entités** sont définies :

Entités essentielles

Ces entités exercent des activités critiques pour le fonctionnement de la société ou de l'économie

Énergie (électricité, gaz, pétrole), ***Transports*** (aérien, maritime, ferroviaire, routier),

Banque, finance, assurance,

Eau potable et assainissement,

Santé (hôpitaux, laboratoires, fabricants de dispositifs médicaux),

Infrastructures numériques (centres de données, fournisseurs DNS, opérateurs cloud),

Administration publique (États et collectivités)

Entités importantes

Elles sont moins critiques mais tout de même exposées

Services postaux et de messagerie,

Industries chimiques,

Recherche,

Fournisseurs de services numériques intermédiaires,

Fabricants de technologies critiques (électronique, équipements de communication, etc.)

Les sanctions

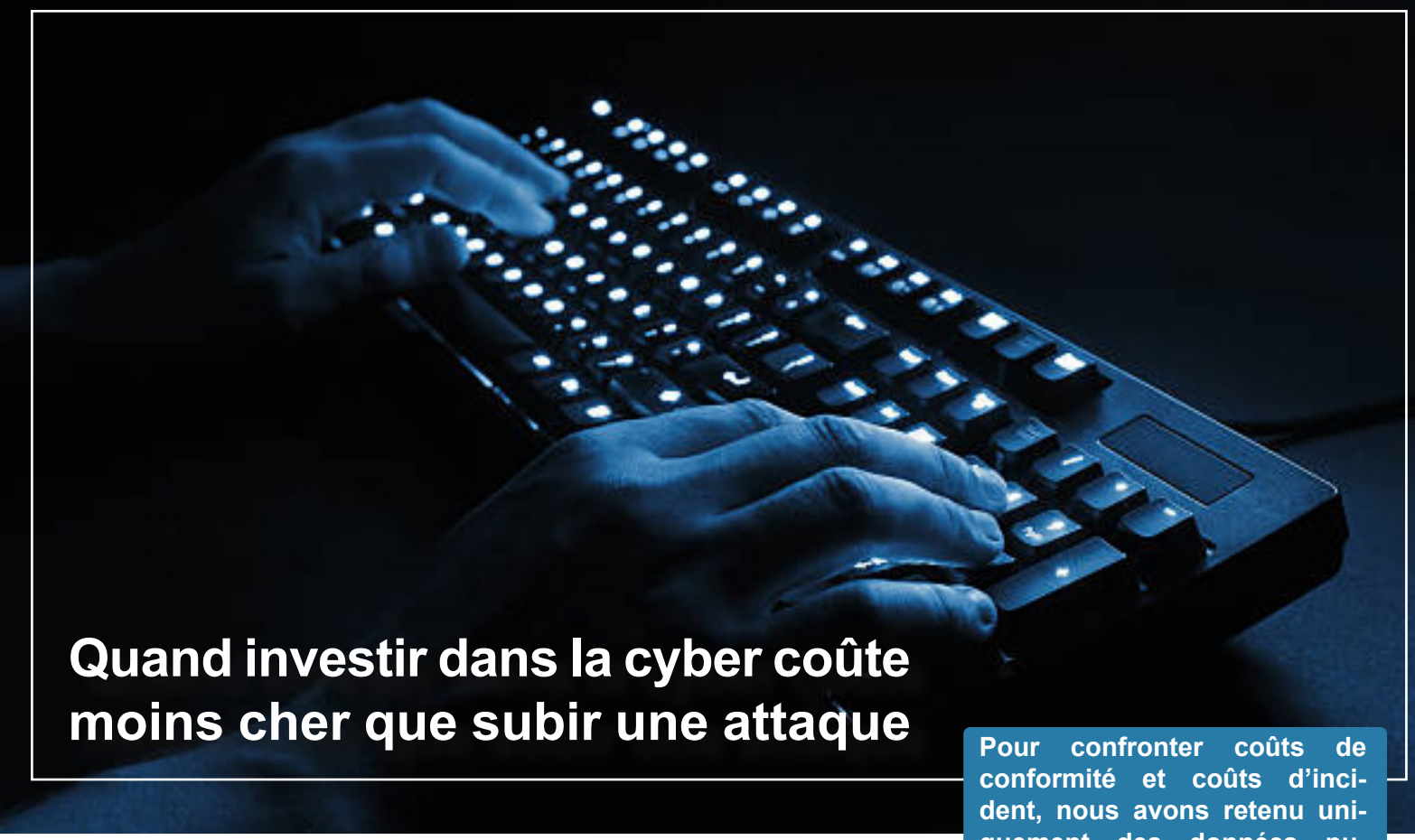
Entités essentielles :
10M€ ou 2 % du CA mondial

Entités importantes :
7M€ ou 1,4 % du CA mondial

Faites le test

Réalisez un test en ligne pour déterminer si votre entité est assujettie à la directive NIS 2 :

monespacenis2.cyber.gouv.fr



Quand investir dans la cyber coûte moins cher que subir une attaque

Pour confronter coûts de conformité et coûts d'incident, nous avons retenu uniquement des données publiques et documentées .

Nous avons retenu l'évaluation d'impact européenne, les estimations sectorielles, l'étude économique de référence utilisée par la Commission (Frontier Economics), les orientations techniques d'ENISA, le rapport IBM Cost of a Data Breach (mesure moyenne d'un sinistre), ainsi que des cas d'entreprises frappées, telles que Maersk, Norsk Hydro, HSE Irlande ou Derichebourg.

Les estimations publiques placent le coût agrégé de la mise en conformité NIS2 à plusieurs dizaines de milliards d'euros pour l'Union, soit un coût moyen « par entité » de l'ordre de quelques centaines de milliers d'euros.

En face, les attaques documentées provoquent des pertes allant de quelques millions à plusieurs centaines de millions d'euros pour une seule victime, souvent bien supérieures au coût de conformité.

Les chiffres publics et les études officielles montrent donc que, dans la majorité des cas et sur la base d'exemples concrets, la dépense pour se conformer à NIS2 est nettement inférieure au coût d'une attaque grave

Voici quelques points de repères pour l'étude.

Deux repères politiques et économiques à connaître :

Une évaluation macro faite par des consultants (chiffre repris dans des études d'impact et par la Commission) aboutit à une estimation globale de coûts de mise en conformité mesurés à l'échelle de l'Union de l'ordre de **31,2 milliards d'euros** (chiffre issu des travaux d'évaluation document technique / rapport d'étude utilisé pour l'analyse d'impact).

La Commission a rappelé que NIS2 élargit la portée à environ **160 000 entités**.

31,2Milliards € ÷ 160,000 entités = 195 000 € par entité (moyenne).

En divisant ces deux chiffres on obtient un ordre de grandeur, sans oublier que NIS2 s'applique de façon très inégale : grands groupes et opérateurs critiques auront des coûts unitaires largement supérieurs (millions d'euros), tandis que beaucoup d'entités « importantes » de taille moyenne supporteront des coûts moindres.

La Commission a estimé aussi que l'augmentation moyenne du niveau de dépenses en cybersécurité serait d'environ 12 % pour les secteurs déjà couverts par la première NIS et d'environ 22 % pour les nouveaux secteurs ajoutés par NIS2.

Sur la base des estimations publiques et des sinistres documentés, payer la conformité même quand elle représente plusieurs centaines de milliers d'euros ou quelques millions pour un grand acteur est en général moins coûteux que subir un incident majeur (coûts directs + interruption d'activité + réputation + juridique + pertes indirectes).

Le rapport IBM (Ponemon) 2023 montre que les organisations ayant un plan d'intervention, des tests fréquents, de l'automatisation, du chiffrement, des sauvegardes et une segmentation de leur réseau, réduisent nettement le coût moyen d'une violation (parfois de l'ordre de 1 à 2 M€ d'économie) et diminuent le délai d'identification & confinement.

Autrement dit, investir dans la sécurité n'est pas seulement une dépense; c'est une réduction mesurable du coût du sinistre.

Les cas Maersk, Norsk Hydro, HSE et Derichebourg en chiffres ...

2017 - Maersk
Interruption opérationnelle mondiale, remise à zéro des infrastructures.
Pertes estimées par l'entreprise 300 M€

2019 - Norsk Hydro
Forcée d'arrêter une grande partie de son réseau et réaliser sa production « manuellement »
Pertes estimées par l'entreprise 75 M€

2021 - HSE Irlande
Déploiement d'un ransomware pour chiffrer les données critiques et exiger une rançon en échange de leur restitution
Pertes estimées par l'entreprise 100 M€

2023 - Derichebourg
Indisponibilité temporaire du principal logiciel d'exploitation suite à une intrusion par un tiers
Pertes estimées par l'entreprise 20M€

LABEL DE CONFORMITÉ ET DE CONFIANCE

ISO 27001, la norme internationale dédiée à la protection des systèmes d'information, s'est imposée comme une référence incontournable. Plus qu'un simple cadre technique, elle incarne une véritable méthodologie de gestion des risques, adoptée par des milliers d'organisations à travers le monde.

L'histoire commence dans les années 1990, au Royaume-Uni. **Le British Standard 7799** (BS 7799), publié en 1995, propose pour la première fois un cadre structuré de gestion de la sécurité de l'information. Cette référence pionnière est ensuite reprise par l'Organisation internationale de normalisation (ISO) et l'International Electrotechnical Commission (IEC).

En 2005, la première version officielle de la norme internationale **ISO/IEC 27001** voit le jour, marquant le passage d'une initiative nationale à un standard universel.

La norme connaît une première révision en 2013, avant une mise à jour majeure en 2022. Chaque évolution suit les mutations du numérique : explosion d'internet, essor du cloud, multiplication des cyberattaques ciblant entreprises et États.

Contrairement à une idée reçue, ISO 27001 n'est pas une liste de mesures techniques à appliquer. **Elle impose la création d'un Système de Management de la Sécurité de l'Information**.

Ce dernier repose sur une logique de cycle d'amélioration continue directement inspirée du modèle qualité ISO 9001.

L'objectif est clair : **identifier** les risques qui pèsent sur les données, **définir** des politiques adaptées, **impliquer** tous les collaborateurs et **vérifier** régulièrement l'efficacité des dispositifs.

Son objectif ?

L'objectif central d'ISO 27001 est de garantir que les informations d'une organisation qu'elles soient numériques, papier ou orales, soient protégées de manière systématique et durable contre les menaces qui pèsent sur elles.

Plus précisément, la norme vise à **instaurer un SMSI qui permet d'assurer la confidentialité des données**, c'est-à-dire qu'elles ne soient accessibles qu'aux personnes autorisées , également de **préserver leur intégrité,** pour éviter toute altération volontaire ou accidentelle et également de **garantir leur disponibilité**, afin que les informations et les systèmes qui les traitent soient accessibles en temps voulu aux utilisateurs légitimes.

Au-delà de ces trois piliers (confidentialité, intégrité, disponibilité), ISO 27001 cherche aussi à donner aux organisations une méthode de gestion des risques applicable en continu.

L'objectif n'est pas de promettre une sécurité absolue, impossible à atteindre, mais de démontrer que l'entreprise a identifié ses menaces, évalué ses vulnérabilités et mis en place des mesures proportionnées pour protéger ses actifs les plus critiques.

Son contenu ?

La norme ISO 27001 repose sur deux piliers complémentaires :

Le premier pilier est constitué des clauses principales de la norme, numérotées de 4 à 10. Celles-ci définissent les règles de base pour construire un Système de Management de la Sécurité de l'Information.

Tout commence par **l'analyse du contexte de l'organisation** : identifier les enjeux, les besoins des parties prenantes et délimiter le périmètre de la sécurité.

Vient ensuite la question du **leadership**, qui place la direction au cœur de la démarche, avec une politique claire et des responsabilités attribuées.

La planification occupe une place essentielle : il s'agit d'identifier et d'évaluer les risques pour mettre en place des objectifs mesurables de protection.

Les clauses suivantes portent sur le support, en intégrant les ressources, la formation, la sensibilisation et la communication, ainsi que la gestion documentaire. La partie opérationnelle se concentre sur le déploiement des contrôles et la gestion quotidienne des risques.

La norme insiste également sur **l'évaluation des performances**, qui se traduit par des audits internes, des indicateurs de suivi et des revues de direction.

Enfin, la logique d'**amélioration continue** permet de corriger les faiblesses, traiter les non-conformités et renforcer progressivement la sécurité de l'organisation.

Ces clauses sont obligatoires et doivent être démontrées par toute entité souhaitant obtenir la certification.

Le second pilier se trouve dans **l'Annexe A**, qui constitue un véritable catalogue de mesures de sécurité. Contrairement aux clauses, elles ne sont pas toutes imposées systématiquement, mais chaque organisation doit les examiner et décider lesquelles sont pertinentes selon ses risques.

Dans sa version de 2013, l'Annexe A comportait 114 mesures réparties en 14 domaines allant de la gestion des actifs à la continuité d'activité, en passant par le contrôle des accès ou la cryptographie. La révision de 2022 a simplifié cette structure pour la rendre plus lisible, réduisant le total à **93 mesures regroupées en 4 grands thèmes organisationnels, humains, physiques et technologiques.**

Ces mesures couvrent des sujets aussi variés que la gestion des fournisseurs, la sécurité des locaux, la protection des données via chiffrement, ou encore la mise en place de processus pour traiter et signaler les incidents.

L'organisation doit expliquer, dans une déclaration d'applicabilité, pourquoi elle applique certaines mesures et pourquoi d'autres ne sont pas retenues.

Pour qui ?

Aujourd'hui, plus de 70 000 organisations dans le monde sont certifiées ISO 27001 Chaque entité peut avoir ses objectifs propres derrière l'obtention d'un certificat de conformité à l'ISO 27001.

ISO 27001 : la norme qui fait de la cybersécurité un atout concurrentiel

La certification ISO 27001 s'impose comme un gage de sérieux et de solidité pour les entreprises. Elle ne se limite pas à un cadre technique, mais traduit une véritable démarche stratégique qui touche à la fois les équipes opérationnelles, la gouvernance et la relation avec les clients. Son intérêt dépasse donc largement la simple conformité : elle participe à la crédibilité et à la pérennité de l'organisation.

Pour une entreprise, le premier bénéfice est de mettre en place une gestion rationnelle et structurée des risques. ISO 27001 impose l'identification des actifs critiques, l'évaluation des menaces et la définition de mesures adaptées pour protéger la confidentialité, l'intégrité et la disponibilité des données.

Cette approche méthodique évite les réponses improvisées et installe une logique d'anticipation. L'organisation gagne en maturité et en résilience : elle devient capable de prévenir les incidents, mais aussi d'y réagir rapidement et efficacement lorsqu'ils surviennent.

Du point de vue des clients, la certification a un impact direct sur la perception de l'entreprise. Dans une relation commerciale, la confiance est un facteur déterminant, surtout lorsqu'il s'agit de données sensibles ou stratégiques. Une entreprise certifiée ISO 27001 démontre qu'elle applique des pratiques reconnues internationalement pour protéger les informations qui lui sont confiées. Cela se traduit par une plus grande solidité perçue : le client sait

que son fournisseur dispose de mécanismes de sécurité robustes, qu'il est audité par des tiers indépendants et qu'il a l'obligation de maintenir ce niveau d'exigence sur la durée.

Dans les secteurs concurrentiels, cet argument peut faire la différence au moment de remporter un appel d'offres ou de convaincre un partenaire hésitant ou un prospect.

L'impact se mesure aussi au niveau du comité exécutif. ISO 27001 oblige la direction à s'impliquer directement dans la stratégie de cybersécurité, à travers une politique claire, la définition de responsabilités et des objectifs mesurables.

Cette responsabilisation change profondément la gouvernance : la sécurité de l'information n'est plus cantonnée aux équipes techniques, elle devient une priorité de pilotage stratégique.

Le comité exécutif bénéficie alors d'**indicateurs précis**, issus des audits et du suivi des performances, pour mesurer l'efficacité des dispositifs en place. Cela permet non seulement de mieux maîtriser les risques financiers et réputationnels, mais aussi de prendre des décisions éclairées sur les investissements en sécurité.

Sur le plan réglementaire, la certification agit comme un **socle de conformité**. Qu'il s'agisse du RGPD, de la directive européenne NIS 2 ou d'exigences sectorielles spécifiques (banque, santé, énergie), ISO 27001 apporte une méthodologie déjà alignée avec la plupart de ces obligations. L'entreprise **réduit ainsi ses risques de sanctions**, démontre sa conformité lors des contrôles et gagne en sérénité face aux évolutions réglementaires.

Pour les dirigeants, cela représente une garantie supplémentaire : ils sont **moins exposés juridiquement** et renforcent la réputation de sérieux de leur organisation.

Enfin, la norme **renforce la continuité d'activité**. Les plans de reprise après incident, la gestion des sauvegardes, les tests réguliers et les scénarios de crise prévus par ISO 27001 garantissent que l'entreprise pourra continuer à fonctionner malgré un événement majeur.

Cet atout est essentiel non seulement pour limiter les pertes financières, mais aussi pour préserver la confiance des clients et partenaires, qui voient dans la résilience de leur fournisseur une preuve de fiabilité à long terme.

En somme, la certification ISO 27001 n'est pas un simple exercice de conformité, mais une véritable transformation de la gouvernance et de la relation client. Elle donne aux entreprises les moyens d'anticiper les menaces, de renforcer leur crédibilité commerciale et de sécuriser leur stratégie à l'échelle du comité exécutif.

Les pilliers de l'ISO 27001

DORA : l'europe des finances

Lorsqu'on se penche sur l'évolution récente de la régulation européenne en matière de cybersécurité, un texte revient avec insistance : la directive DORA, pour **Digital Operational Resilience Act.** Derrière cet acronyme au ton technocratique se cache en réalité une réforme de grande ampleur qui bouleverse les règles du jeu dans le secteur financier européen. Adoptée en décembre 2022 par le Parlement et le Conseil européens, entrée en vigueur en janvier 2023 et pleinement applicable depuis janvier 2025.

DORA transforme la sécurité en enjeu stratégique pour toute la finance européenne

L'histoire de DORA s'inscrit dans un contexte précis : celui d'un monde financier de plus en plus dépendant des technologies de l'information et donc particulièrement vulnérable aux cyberattaques.

Mais cette dépendance croissante aux infrastructures numériques a également engendré un nouveau type de risque systémique. Là où, hier, la menace principale venait de la fragilité des marchés ou des crises de liquidité, elle provient désormais aussi d'un piratage, d'une panne informatique ou d'un incident chez un prestataire externe comme un fournisseur de cloud.

Les régulateurs européens, alertés par plusieurs épisodes marquants, notamment des attaques par rançongiciel paralysant des groupes financiers, ou des incidents touchant des prestataires de services critiques, ont pris conscience de la nécessité d'un cadre unique, harmonisé et contraignant. C'est dans ce terreau que DORA a germé.

La directive DORA marque un tournant dans la manière dont les institutions financières européennes doivent envisager leur sécurité numérique. Derrière ses centaines de pages de dispositions, elle impose une nouvelle réalité : la cybersécurité n'est plus seulement une question technique confiée aux équipes informatiques, mais un enjeu stratégique qui engage directement la survie, la réputation et la compétitivité des acteurs financiers

Son objectif ?

Son intérêt premier est de mettre fin à une mosaïque de règles disparates. Avant DORA, chaque pays de l'Union imposait ses propres obligations aux banques et compagnies d'assurance en matière de cybersécurité, souvent avec des exigences hétérogènes et parfois contradictoires. Le résultat était une complexité accrue pour les groupes opérant à l'échelle européenne, mais aussi des failles potentielles que pouvaient exploiter les cybercriminels.

En instaurant un règlement applicable directement dans tous les États membres, l'Union européenne vise à élever le niveau global de résilience tout en simplifiant le paysage réglementaire.

Son contenu ?

Le contenu de DORA se décline en **cinq grands volets.**

Le premier impose aux acteurs financiers la mise en place d'un dispositif robuste de gestion des risques liés aux technologies de l'information et de la communication. Concrètement, chaque institution doit identifier ses actifs critiques, cartographier ses dépendances numériques, évaluer les menaces pesant sur ses systèmes et instaurer des politiques adaptées pour réduire la probabilité et l'impact d'incidents. Cette approche ne se limite pas à l'installation d'outils techniques, mais intègre également des dimensions organisationnelles et humaines : formation, clarification des responsabilités.

Le deuxième volet concerne les tests de résilience numérique. Les établissements ne pourront plus se contenter d'affirmer qu'ils disposent d'un plan de continuité ou de reprise après sinistre : ils devront le prouver par des simulations régulières, allant jusqu'à des exercices de type « red teaming », où des équipes spécialisées jouent le rôle de pirates pour tester en conditions réelles la solidité des défenses. Ces tests, obligatoires pour les entités les plus critiques, doivent permettre d'identifier les vulnérabilités avant que des attaquants malveillants ne les exploitent.

Le troisième particulièrement novateur, vise les fournisseurs tiers de services technologiques, et notamment les géants du cloud sur lesquels reposent désormais une grande partie des infrastructures financières. Jusqu'à présent, ces acteurs échappaient largement au contrôle direct des régulateurs financiers. DORA change la donne : les fournisseurs considérés comme critiques seront placés sous la supervision directe des autorités européennes, avec des obligations spécifiques de transparence, de résilience et de coopération.

Le quatrième volet concerne la déclaration des incidents. Tout événement majeur ayant un impact significatif sur la disponibilité, l'intégrité ou la confidentialité des systèmes devra être notifié rapidement aux autorités compétentes. L'objectif est double : permettre une réaction coordonnée à l'échelle européenne et renforcer la transparence vis-à-vis du public. Dans certains cas, les clients directement touchés devront également être informés.

Enfin, **le cinquième** encourage le partage d'informations entre institutions financières sur les menaces émergentes, les vulnérabilités découvertes et les modes opératoires des cyberattaquants. Cette coopération, qui peut sembler contre-intuitive dans un univers concurrentiel, est en réalité un levier de sécurité collective : l'expérience montre que les attaquants échangent et collaborent entre eux, et que la meilleure défense consiste à répliquer cette dynamique du côté des défenseurs.

Pour qui ?

Elle concerne l'ensemble du secteur financier européen, soit **plus de 22 000 entités**.

Banques

Assurances et réassurances

Sociétés de gestion et fonds d'investissement

Entreprises d'investissement et de courtage

Prestataires de services de paiement

Infrastructure de marché (Bourses, chambres de compensation, systèmes de règlement-livraison)

Fournisseurs de crypto-actifs

Fournisseurs tiers critiques

Finances et cybersécurité

Comment DORA redéfinit la confiance au cœur du système financier

Dora redéfinit la relation de confiance entre les acteurs du marché, les institutions, les clients et les investisseurs.

En instaurant une résilience numérique commune à toute la sphère financière européenne, DORA apporte une valeur ajoutée collective : la sécurité devient un bien public, et la confiance, un actif partagé.

L'un des bénéfices les plus tangibles se mesure dans la relation avec les clients et les investisseurs. En affichant une conformité rigoureuse à DORA, une entreprise financière envoie un signal fort : celui de la confiance et de la maîtrise. Les clients savent que leurs données, leurs transactions et leurs actifs numériques sont protégés selon les standards les plus élevés du marché. Les investisseurs, quant à eux, y voient un gage de solidité et de durabilité.

La conformité devient ainsi un facteur de différenciation concurrentielle, renforçant la réputation et l'attractivité de l'entreprise dans un contexte où la confiance numérique est devenue un actif stratégique.

DORA agit aussi comme un accélérateur de transformation numérique responsable. En structurant les exigences de sécurité autour de l'innovation technologique, la directive permet aux entreprises de déployer des outils modernes intelligence artificielle, cloud, blockchain sans compromettre leur intégrité opérationnelle.

Elle crée un cadre de confiance où l'innovation peut s'épanouir en toute sécurité. Cette approche « sécurité dès la conception » (security by design) favorise un environnement où la performance technologique se conjugue avec la prudence réglementaire.

En renforçant la solidité numérique du secteur financier, elle protège la stabilité économique de l'Union européenne. Les attaques contre les institutions financières peuvent avoir des répercussions systémiques : perturbations des paiements, fuites de données sensibles, atteinte à la confiance des marchés.

UBS

En juin 2025, la banque UBS a confirmé que plus de 130 000 dossiers d'employés avaient été exposés après une attaque par ransomware touchant Chain IQ, son fournisseur de services de procurement (achats).

La fuite comprenait des données sensibles : adresses domiciliaires, numéros de téléphone privés de haut niveau (dont celui du CEO), et d'autres informations personnelles.

Cet exemple montre bien que les vulnérabilités ne se situent pas toujours "dans la banque" mais souvent dans son écosystème prestataires, fournisseurs, intégrations externes.

DORA vise précisément à couvrir ces failles externes, à imposer des standards de résilience tout au long de la chaîne, ce qui permettrait de prévenir ce type d'incidents.

Cette homogénéisation du niveau de sécurité réduit les inégalités entre acteurs et rend le marché plus transparent.

Pour le client, cela se traduit par une expérience bancaire plus sûre, une meilleure protection de ses données et une garantie de continuité des services, même en cas de cyberincident majeur. DORA transforme donc la confiance client en une valeur tangible, mesurable et vérifiable.

Les investisseurs, quant à eux, voient en DORA une véritable assurance contre le risque numérique. En imposant aux entreprises de cartographier leurs dépendances, de tester leurs plans de continuité et de renforcer la surveillance de leurs prestataires, DORA réduit considérablement le risque de rupture de chaîne.

Pour les investisseurs, cela se traduit par une plus grande prévisibilité, une réduction du risque systémique et, par conséquent, une meilleure valorisation des entreprises conformes.

Sur un plan plus global, DORA profite également à la stabilité du système financier européen. En établissant un socle commun de résilience numérique, elle crée une immunité collective face aux menaces cybernétiques.

Une cyberattaque contre une banque isolée ou un prestataire critique ne peut plus se propager aussi facilement dans l'écosystème, car chaque maillon de la chaîne est désormais soumis à des exigences de sécurité et de coordination renforcées. Cette approche systémique protège non seulement les entreprises, mais aussi les infrastructures d'intérêt public : systèmes de paiement, chambres de compensation, plateformes de trading.

En ce sens, DORA devient un outil de souveraineté économique.

CREDITS

Rédacteur : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume POUPARD

Septembre 2025

En partenariat avec