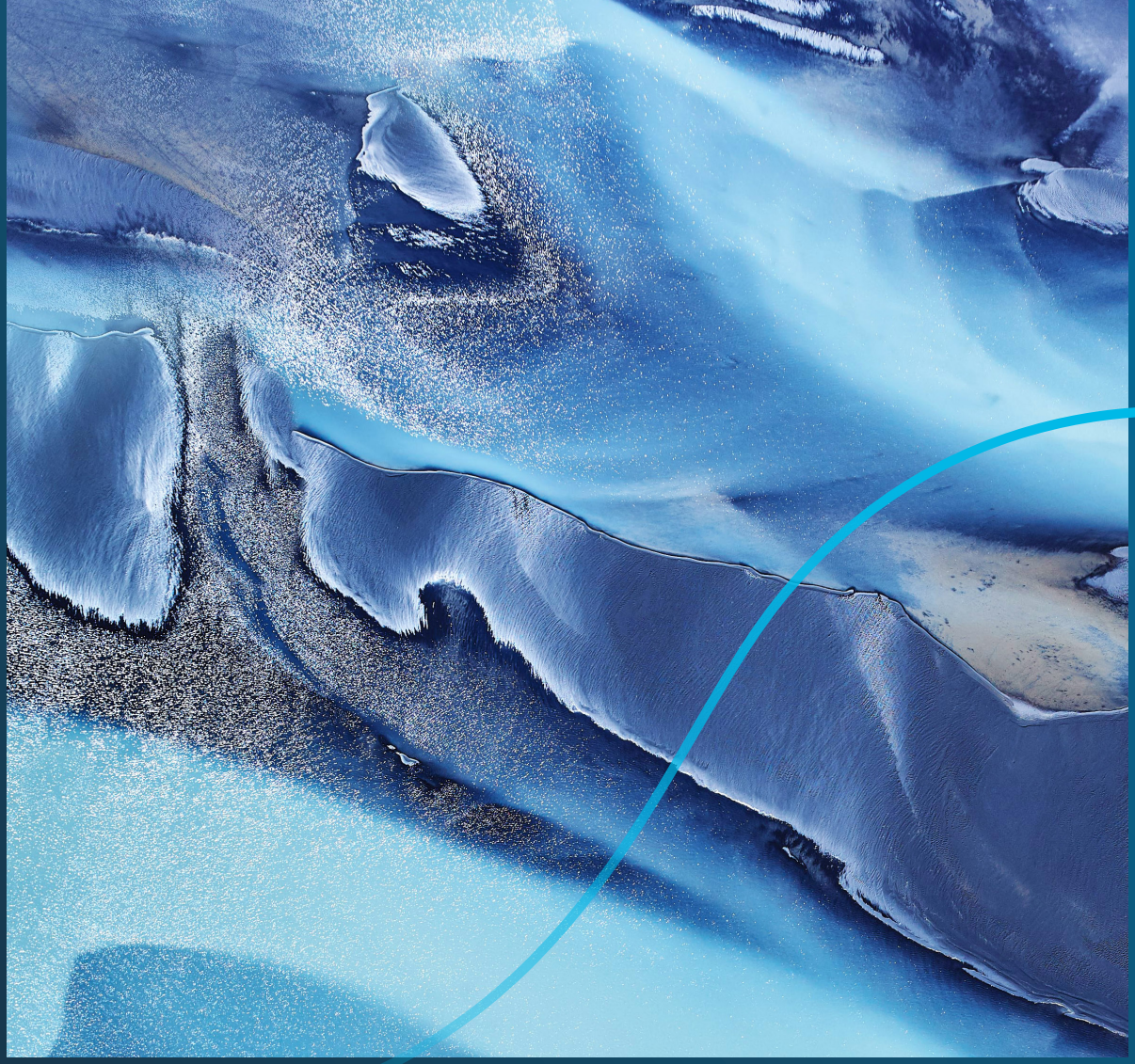


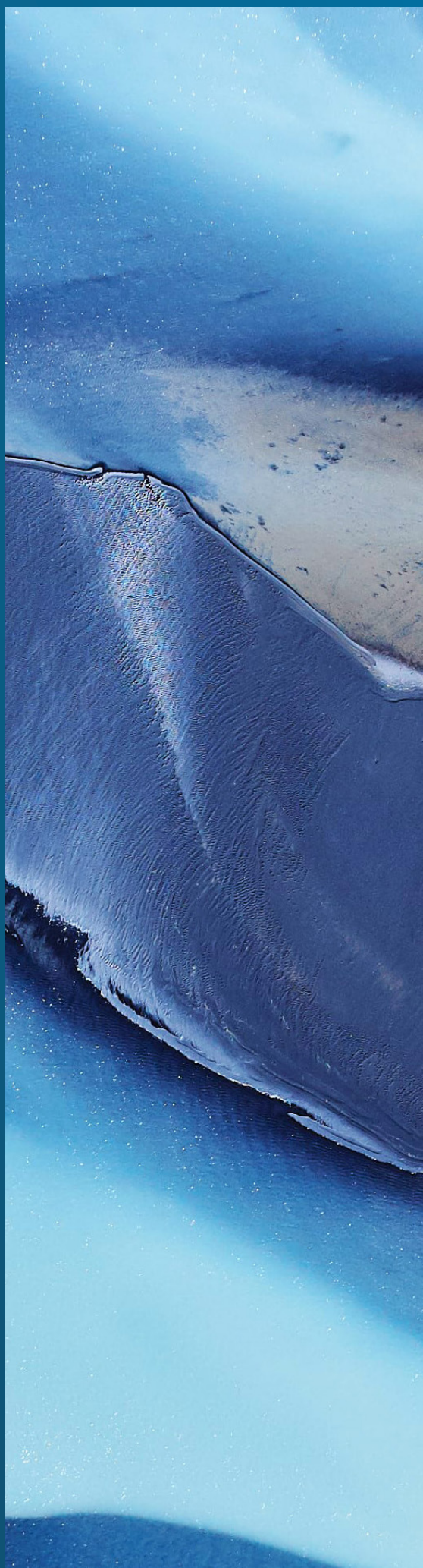
NIS 2 & DORA : naviguer dans le *nouveau cadre réglementaire* de la cybersécurité

Capgemini

Note introductive

Ce livret consacré aux règlementations NIS 2 et DORA rassemble une série d'articles précédemment publiés mais récemment enrichis par nos experts afin de fournir une analyse approfondie et la plus à jour possible. À travers ces contributions, nous espérons offrir des éclairages précieux et des conseils pratiques pour naviguer dans le paysage réglementaire complexe de la cybersécurité. Que vous soyez un professionnel de la sécurité informatique, un responsable de la conformité ou un décideur stratégique, ce livret vous aidera à renforcer la résilience opérationnelle de votre organisation.

Table des matières



Edito

Avec DORA et NIS 2, la résilience entre dans une nouvelle ère.

Les réglementations DORA (Digital Operational Resilience Act) et NIS 2 (Network and Information Systems), auxquelles il faut ajouter le Cyber Resilience Act, marquent un tournant majeur dans la perception de la sécurité numérique en Europe et, par conséquent, dans la façon de l'aborder.

Reconnaissant la place fondamentale qu'occupent désormais les infrastructures et les services numériques dans tous les domaines, le législateur fait de la résilience un enjeu vital, systémique, et non plus seulement une question technologique. Elle doit par conséquent devenir une priorité pour tous les acteurs qui jouent un rôle clé dans le fonctionnement de la société, en l'occurrence les établissements financiers (DORA) et les entités des secteurs sensibles (NIS 2).

La résilience des entreprises repousse les limites de la cybersécurité en intégrant l'ensemble de la chaîne cyber : prévention, protection, détection, réaction, reprise, reconstruction, activités métier et l'écosystème des tiers. La sécurité numérique devient l'affaire de tous car tous appartiennent aux mêmes écosystèmes interconnectés et sont exposés aux mêmes menaces, susceptibles de se propager et de fragiliser l'ensemble. En renforçant les exigences individuelles, les autorités européennes entendent par-dessus tout renforcer la posture collective.

De ce changement de paradigme, découlent quatre implications fondamentales qui sous-tendent autant DORA que NIS 2 :

1. **l'objectif principal devient la résilience** – au sens de la continuité des activités – et non plus la sécurité numérique stricto sensu ;

2. **la cybersécurité et la résilience sont désormais abordées au niveau de l'écosystème,** toutes les entités européennes étant de plus en plus interconnectées, elles doivent hausser collectivement leur niveau de sécurité et non plus individuellement ;

3. **toutes les fonctions et tous les niveaux de l'organisation doivent être impliqués,** depuis le comité de direction jusqu'à chaque collaborateur ;

4. **la responsabilité est explicitement placée sur les plus hauts dirigeants,** qui doivent faire partie intégrante du dispositif et ne peuvent plus se défausser sur les équipes IT, cyber ou conformité.

Ces principes remettent en question la notion même de conformité. En effet, pour DORA comme pour NIS 2, il s'agit moins de satisfaire à une liste d'exigences techniques que de pouvoir démontrer que l'on a convenablement analysé les risques, déployé les dispositifs permettant de les surveiller et de les maîtriser, et mis en place les outils et les instances de reporting et de gouvernance appropriés.

C'est pour cette raison qu'en dépit de leur différence de nature et de portée, nous abordons ici conjointement ces deux textes : que l'on ne soit concerné que par l'un ou l'autre, ou même aucun des deux, les analyses de nos experts mettent en évidence leur inspiration commune, leurs conséquences voisines sur de nombreux aspects – gouvernance, gestion des incidents, risques liés aux tiers… – et donc la similitude des démarches et des solutions à mettre en œuvre. Au-delà de la mise en conformité, les recommandations qu'ils formulent s'apparentent à des bonnes pratiques en matière de cybersécurité qui pourraient inspirer les organisations souhaitant renforcer leur posture cyber dans un environnement de plus en plus menaçant.

DORA et NIS 2 marquent l'aboutissement d'un long processus de maturation qui a vu la sécurité informatique devenir la cybersécurité, puis la résilience numérique, et enfin, aujourd'hui, la pierre angulaire de la résilience opérationnelle. Lorsqu'elles en adoptent la philosophie, les organisations font bien plus que respecter une obligation réglementaire : elles investissent pour sécuriser durablement la valeur qu'elles créent.

Jeanne Heuré
Head of Digital Trust,
Capgemini Invent

Vincent Laurens
Head of Cybersecurity Business
Development & Solutionning,
Capgemini

Vision des échéances réglementaires DORA & NIS 2

DORA

NIS 2

DORA ou l'approche fondée sur les risques

Entré en vigueur début 2025, le règlement européen DORA adresse la dimension systémique du risque cyber pour le secteur financier en imposant à chaque acteur d'accroître sa résilience opérationnelle en concentrant ses efforts sur ses actifs numériques les plus exposés et les plus critiques.

En 2022, les institutions financières ont été plus exposées aux cyberattaques que la plupart des autres secteurs, en dehors de la santé. La forte numérisation des activités financières, le recours au télétravail lors de la pandémie de Covid-19 et la montée des tensions géopolitiques, ont intensifié les risques cyber, qualifiés de « très élevés » par la Banque de France depuis 2023.

Le secteur financier se distingue par une forte interconnexion, faisant du risque cyber un risque systémique. Le secteur regroupe en effet des acteurs qui concentrent une part importante des actifs et des flux, et qui sont fortement liés entre eux.

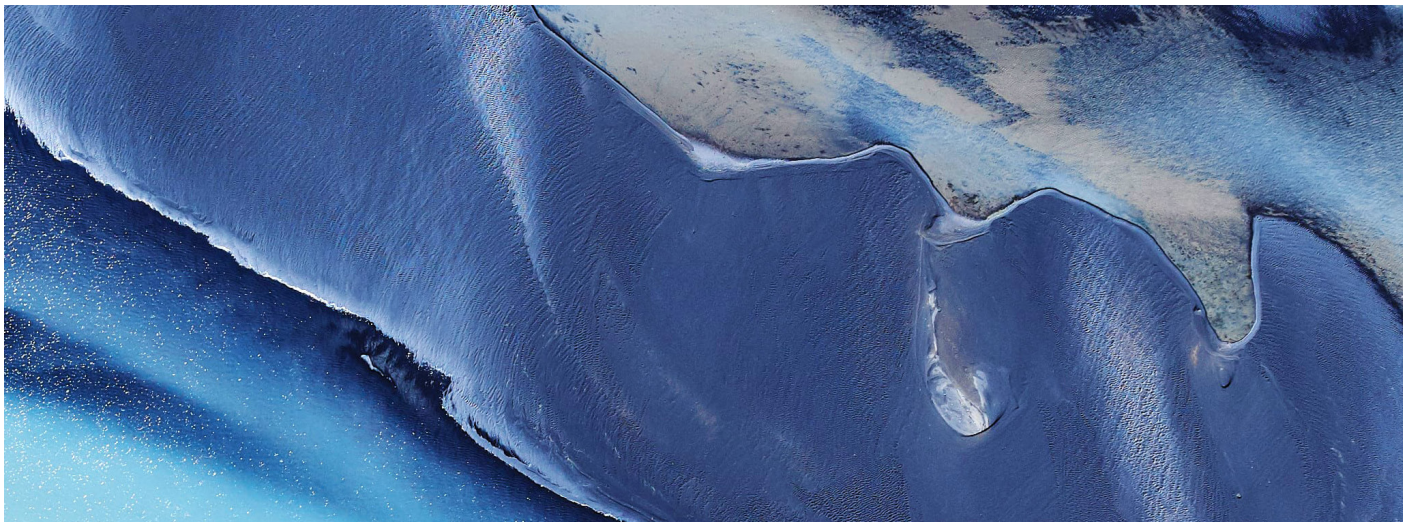
Par conséquent, un évènement isolé peut se propager plus largement, comme l'a démontré la cyberattaque du 9 novembre 2023 contre une division américaine de la Banque Industrielle et Commerciale de Chine.

Face à l'omniprésence de cette menace, la stratégie de cybersécurité d'une entité financière ne peut se limiter à une approche exclusivement préventive des risques. Puisque le risque zéro n'existe pas, elle doit assurer des capacités de gestion de crise et de reconstruction.

Le législateur s'est emparé de cette problématique et a pris des mesures significatives. Ainsi, parallèlement à la directive NIS 2 (Network and Information Systems), la réglementation DORA (Digital Operational Resilience Act), spécifique au secteur financier, est entrée en vigueur en janvier 2025. Elle établit des exigences claires en matière de cyber-résilience et impose d'adopter une approche fondée sur les risques.

L'approche par les risques repose fondamentalement sur la priorisation. Les menaces et les sources de risques doivent être identifiées afin de définir un nombre restreint de macro-scénarios potentiels, dont la criticité doit être caractérisée en évaluant leur probabilité et leur impact sur les activités de l'entité. Ces dernières doivent également être priorisées selon leur criticité afin d'identifier celles qui nécessitent une protection et des contrôles renforcés. Ainsi, en concentrant les efforts sur les scénarios touchant les activités les plus critiques, cette approche permet d'orienter efficacement les ressources vers les aspects les plus essentiels de l'organisation.

DORA préconise un retour à l'essentiel pour assurer la continuité des activités de l'entité. Définir sa stratégie de cyber-résilience nécessite de s'interroger sur ce qui est vital pour les activités de l'entité et indispensable à leur continuité opérationnelle (i.e. infrastructures, applications, assets), en se focalisant sur les scénarios les plus critiques. Adopter cette approche pragmatique permet de concentrer les efforts de résilience sur ce qui contribue au cœur de l'activité de l'entité.



Quelques bonnes pratiques pour adopter l'approche par les risques

Le point de départ incontournable est l'identification des activités critiques pour définir le périmètre de la résilience. Cela nécessite de pouvoir s'appuyer sur un référentiel groupe des activités et des processus de l'entreprise. En fonction de l'entreprise, le niveau de granularité de l'analyse peut varier : service métier, macro-activité, activité ou processus. Le choix doit se faire de sorte que l'organe de direction puisse prendre des décisions. L'entreprise peut s'appuyer sur un certain nombre de standards et de méthodologies existants de gestion des risques et de la continuité d'activité existants (ISO 27005, ISO 22301, EBIOS RM, etc.).

À partir des activités critiques, via une approche top-down, l'entreprise déduit le périmètre des applications et des infrastructures à rendre résilientes. L'approche par les risques permet de déterminer les maillons de la chaîne qui sont absolument nécessaires au maintien ou à la reprise d'activité. Cela nécessite de challenger et d'affiner les résultats des Bilans d'Impact sur l'Activité (BIA) produits par les métiers. La traduction des actifs métiers en actifs IT nécessite une CMDB (Configuration Management Database) à jour et suffisamment précise à commencer par les assets IT critiques. Cette cartographie est par ailleurs clé pour répondre au reste des exigences de DORA, pour la classification des incidents comme pour les plans de tests, par exemple.

Les dépendances d'activités critiques vis-à-vis de prestataires ou de partenaires externes doivent aussi être prises en compte. L'approche par les risques permet de classer les tiers par niveau de criticité. L'analyse de risque prend ainsi en compte la substituabilité d'un tiers ou encore le risque de surconcentration d'actifs.

Enfin, les actifs dont il faut renforcer la résilience doivent être priorisés dans la perspective du processus de reconstruction. Les délais de reprise d'activité ainsi que les niveaux acceptables de pertes de données sont aussi à challenger en prenant en compte, par exemple, les alternatives métiers. Cette priorisation entre les assets permettra de faire face à un cas de black-out mais aussi à une perturbation partielle.

En introduisant une approche par les risques, DORA invite à se concentrer sur ce qui est le plus critique et définit un standard de résilience opérationnelle, applicable au-delà du secteur financier.

Lucie Shen
Consultante Digital Trust & Security, Capgemini Invent

Samuel Zanin
Consultant Digital Trust & Security, Capgemini Invent

NIS 2, DORA : la gouvernance au cœur des exigences

NIS 2 et DORA partagent un même objectif : sécuriser davantage le tissu économique de l'Union européenne face à des risques numériques grandissants. Pour cela, l'un et l'autre vont imposer aux entreprises de revoir leur gouvernance de la cybersécurité, où la direction générale sera désormais en première ligne.

Alors que la directive NIS (Network and Information Security), votée en 2016 et transposée en 2018, ne s'appliquait qu'à un nombre restreint d'acteurs stratégiques, NIS 2, qui lui succède, étend son périmètre et devrait concerner des milliers de grands groupes, ETI et PME dans une vingtaine de secteurs d'activité. Les détails de son application ne seront toutefois définitivement connus qu'au terme du processus de transposition. A ce titre, le projet de loi de transposition a été déposé au Sénat par le Gouvernement le 15 octobre 2024 et est actuellement à l'étude par les deux chambres du Parlement.

Comme NIS, NIS 2 énonce un certain nombre de mesures obligatoires – correspondant plus ou moins aux exigences de la norme ISO 27001 – que doivent mettre en œuvre les entreprises pour réduire fortement l'exposition de leurs systèmes aux risques cyber.

Également votée en 2022, DORA (Digital Operational Resilience Act) est un règlement européen, qui s'applique donc tel quel, sans transposition, depuis début 2025. Son objectif, quant à lui, est de renforcer la résilience opérationnelle des entreprises du secteur financier (banques, assureurs, gestionnaires d'actifs…) face au risque numérique (cyber, panne, erreur…). Il établit pour cela des règles contraignantes concernant la gestion de ces risques, la notification des incidents, les tests de résilience et la gestion des risques liés à la supply chain et ses parties prenantes.

Un point commun : la gouvernance

Même s'ils ont des portées et des champs d'application différents, ces deux textes partagent un point commun majeur : l'un et l'autre prévoient l'instauration de sanctions et établissent, en cas de manquement, la responsabilité pénale des dirigeants de l'entreprise.

Dans le cas de DORA, ceux-ci ont d'ailleurs l'obligation d'être formés aux risques cyber et à leurs impacts sur la continuité des opérations. Outre l'aiguillon que représente le risque juridique et financier, ceci bouleverse la gestion traditionnelle de la cybersécurité dans l'entreprise et, en particulier, sa gouvernance.

Avec des responsabilités remontées au niveau de la direction, la cybersécurité devient de fait un enjeu d'entreprise, qui sera intégré à la stratégie globale et abordé de façon systématique et transverse, au même titre que d'autres types de risques.
Ceci favorisera l'homogénéisation des dispositifs et des pratiques, l'optimisation de l'allocation des ressources, l'intégration de la sécurité dans les processus opérationnels et sa prise en compte by design dans les projets, et enfin le développement d'une culture interne de la cybersécurité.

Comme le demande d'ailleurs explicitement DORA, cette transversalité nécessitera une gouvernance renforcée, impliquant régulièrement les acteurs métiers. Étant donné la technicité du sujet, le CISO/RSSI en restera l'acteur clé, mais il gagnera en visibilité et en poids politique, bénéficiant de réponses plus rapides et de moyens accrus.

Deux volets pour la mise en œuvre

Les mises en œuvre de NIS 2 comme de DORA auront donc deux volets. Le premier concernera les mesures de sécurité proprement dites, conformément à ce que réclament les textes.

Très précises et détaillées pour DORA, ces exigences doivent encore être précisées par chaque Etat membre pour NIS 2. En France, en l'état de sa transposition menée avec l'ANSSI, il s'agirait plutôt d'une liste d'objectifs à atteindre, les entreprises bénéficiant d'une grande latitude sur les moyens d'y parvenir et sur le choix de leurs priorités. Le point de départ consistera donc à déterminer à quel régime d'obligations exactement est soumise l'entreprise, puis à mesurer l'écart entre ces exigences et l'existant, et enfin à établir une feuille de route (désormais sous l'œil de la direction générale !).

Le second volet de la mise en œuvre concernera justement le dispositif organisationnel et de gouvernance transverse et à haut niveau qui permettra de suivre, piloter et coordonner cette mise en conformité, puis le respect dans la durée des exigences réglementaires en fonction de l'évolution des technologies et des risques.

Bien plus que des nouvelles contraintes réglementaires, NIS 2 et DORA visent ainsi à faire prendre conscience aux entreprises et à leurs dirigeants de l'importance cruciale de la cybersécurité dans l'environnement actuel. Elles aident à passer d'un traitement cloisonné et à haut niveau des risques et de la sécurité numériques, à un traitement transverse et stratégique, inscrit comme tel dans la gouvernance de l'entreprise.

Pierre Tournier
Consultant gouvernance et stratégie de cybersécurité,
Capgemini France

Lina Ouaras
Consultante Digital Trust & Security,
Capgemini Invent

Supply chain : quelle cybersécurité pour les composants connectés ?

Les composants connectés que l'on trouve désormais dans toutes sortes de produits sont une source de risques grandissante. Pour les adresser, la réglementation engage les fabricants à renforcer leur contrôle sur leur chaîne d'approvisionnement.

Entre les soupçons pesant sur la sécurité des équipements 5G produits hors de l'Union européenne et le piratage spectaculaire de véhicules autonomes, de nombreuses affaires ont attiré ces dernières années l'attention sur la vulnérabilité des objets connectés.

Qu'il s'agisse d'un train, d'un automate industriel ou d'une caméra de vidéosurveillance, sitôt qu'un appareil ou un système est capable d'échanger des données avec l'extérieur, il se trouve en effet exposé à des actes de malveillance. On peut chercher à soutirer les données qu'il contient, à bloquer ou détourner son fonctionnement, ou encore à s'en servir comme d'une porte d'entrée vers d'autres systèmes. Pour cela, on exploite le plus souvent les vulnérabilités de l'un de ses composants matériel ou logiciel, vulnérabilités qui peuvent avoir été introduites par son fabriquant délibérément ou en raison de son manque de vigilance.

Le fabricant du produit final reste tributaire du niveau de sécurité des composants qu'il utilise. Or, bien que leur responsabilité puisse être engagée en cas d'incident, peu d'industriels se soucient aujourd'hui de demander à leurs fournisseurs des garanties en matière de cybersécurité, sinon dans de rares activités sensibles. Dans le secteur de la défense, par exemple, l'Armée française a ainsi élaboré un référentiel de maturité cyber pour les entreprises de la Base Industrielle et Technologique de Défense (BITD). Malgré ces initiatives, l'approche reste souvent désordonnée et cloisonnée, chaque département évaluant les risques aux limites de son périmètre et selon ses critères.

Une pression réglementaire grandissante

La multiplication des composants connectés exacerbe aussi les tensions économiques et géopolitiques en raison de l'accès qu'ils pourraient potentiellement donner à des informations critiques. Face à ces enjeux qu'il n'est plus possible d'ignorer, la réglementation se renforce. En Europe, le Cyber Resilience Act et et la directive NIS 2 vont ainsi accroître la pression sur les entreprises en leur imposant de faire preuve de davantage de vigilance. En parallèle, émergent des normes sectorielles, comme l'UNR 155 et l'ISO 21434 pour l'automobile, ou l'ED 202 pour l'aéronautique, qui renforcent elles aussi les exigences de sécurisation et de contrôle.

Pour toutes les industries connectées et/ou qui fabriquent des produits connectés, il va donc falloir très vite s'organiser pour pouvoir garantir la sécurité, l'authenticité et l'intégrité des composants tiers. Pour mettre en place cette « supply chain de confiance », il faudra toutefois surmonter quatre écueils majeurs :

- la faible maturité en matière de cybersécurité des fournisseurs, dont peu ont la taille et les ressources pour s'en être sérieusement préoccupé jusqu'ici ;
- la faible substituabilité des composants, en général très spécialisés et sur lesquels on ne peut donc pas imposer trop d'exigences ;
- la difficulté pour les donneurs d'ordre de mettre en place un dispositif global et systématique d'évaluation et de contrôle ;
- et enfin la règlementation jusqu'ici insuffisante pour contraindre les fabricants à se pencher sur le niveau de sécurité des composants utilisés.

Dans ce contexte, nous recommandons une approche en trois temps :

1 Sensibiliser et convaincre pour embarquer

La priorité est d'abord de prendre conscience et de faire prendre conscience de la réalité des risques, de leur ampleur, et donc de la nécessité de s'en prémunir. L'objectif est de construire une vision stratégique globale tant au niveau des produits (du chipset au cloud) que de la production (processus et outils de l'industrie intelligente), et de faire en sorte que tous les acteurs internes concernés (études, achats, IT, juridique, production…) adhèrent et participent. La gestion des risques cyber liés aux tiers doit être décloisonnée, coordonnée de bout en bout, et fondée sur une perception et une visibilité commune des risques. Ce travail pour sensibiliser, convaincre et embarquer devra également être mené avec les fournisseurs eux-mêmes.

2 Se donner les moyens de ses ambitions

La deuxième étape consiste à doter cette stratégie de moyens organisationnels et techniques. Étant donné les enjeux, des procédures déclaratives ne suffisent plus : il faut formaliser les pratiques, objectiver les évaluations, systématiser les contrôles. Pour cela, après avoir cartographié l'existant, on pourra s'appuyer sur un référentiel (NIST, ISO, IEC…) pour remettre à plat les processus et les mesures de sécurité, notamment en ce qui concerne l'évaluation et la sélection des fournisseurs. Il faudra aussi collaborer avec ces derniers pour les accompagner dans la mise en place de leurs nouvelles obligations.

Il faudra par ailleurs se doter de l'outillage adéquat : d'une part, pour vérifier et contrôler le niveau de sécurisation intrinsèque des composants tiers (évaluation des risques, tests, validation des certifications et homologations…) ; d'autre part, pour s'assurer qu'ils respectent les principes de l'architecture de sécurité de type zero-trust (auto-contrôle des équipements, gestion des identités et des accès, stockage des informations sensibles…).

3 Inscrire cette politique dans la durée

Enfin, la troisième étape va consister à mettre en place un suivi de cette politique dans la durée. En effet, les cycles de vie des produits industriels sont parfois longs, et les technologies comme le contexte sécuritaire évolueront probablement. Ainsi, il faut prévoir un dispositif opérationnel qui permettra de superviser les risques et leur évolution tout au long de l'exploitation des produits, en intégrant ces derniers au SOC (Security Operations Center) et à un processus de gestion des vulnérabilités et des incidents. Celui-ci viendra s'ajouter aux stratégies de défense en profondeur et de conception robuste qui évitent de faire reposer toute la sécurité sur des composants au futur incertain.

Depuis la cyberattaque qui, en 2020, a emprunté des mises à jour de l'éditeur SolarWinds, les risques associés à la supply chain logicielle sont désormais bien identifiés (sinon adressés). Il ne faudrait pas attendre un incident similaire, aux conséquences potentiellement catastrophiques, pour que les entreprises prennent conscience que les menaces sont identiques sur leur supply chain matérielle. La sécuriser de bout en bout sur le plan cyber sera un travail de longue haleine, mais il est capital de débuter dès aujourd'hui en se posant une simple question : que sais-je exactement de la sécurité des composants avec lesquels je fabrique mes produits ?

Laurent Mahieux
Responsable Cybersécurité pour l'Industrie Intelligente, Capgemini France

Ali Bekkali
Head of Intelligent Product & 5G Security, Capgemini Engineering

Samuel Zanin
Consultant Digital Trust & Security, Capgemini Invent

DORA, un modèle de maturité pour les tests de cybersécurité

Pierre angulaire de la cybersécurité, le test était jusqu'ici laissé à la discrétion des organisations. Les règles que fixe désormais DORA pour le secteur financier marquent une montée en maturité et pourraient servir de modèle à d'autres acteurs.

En matière de politiques de sécurité informatique, les tests constituent l'un des piliers fondamentaux, autant pour valider l'efficacité des dispositifs mis en place pour protéger les systèmes que pour révéler des brèches restant à colmater.

Cependant, qu'il s'agisse de tests d'intrusion, d'analyse de code, de configuration ou encore d'infrastructure, ces tests sont le plus souvent conçus, et parfois réalisés, en interne par les équipes de la DSI et du RSSI. Il peut donc arriver que les enjeux soient couverts de façon incomplète, morcelée, voire partiale, donnant ainsi lieu à diverses zones d'ombre et angles morts.

Consciente des menaces qui peuvent en résulter, la Commission européenne a souhaité encadrer et systématiser la pratique des tests dits de « résilience opérationnelle numérique » dans le cadre du règlement DORA.

Le test comme aboutissement d'une approche par les risques

DORA constitue un changement important de paradigme : d'une pratique purement technologique à la discrétion de l'organisation et de son RSSI, le test de cybersécurité devient l'aboutissement obligatoire et formalisé d'une approche par les risques.

Ainsi, ces tests devront désormais être définis au regard de scénarios d'attaque, lesquels devront eux-mêmes découler d'une analyse des risques. La philosophie de DORA est donc de lier systématiquement et explicitement les tests à une analyse de risques en amont.

La clé de voûte de son application résidera par conséquent dans la mise en place d'une collaboration entre les équipes cyber et les équipes risques afin de bâtir un cadre validé et promu par le plus haut niveau de l'organisation, explicitant et expliquant :

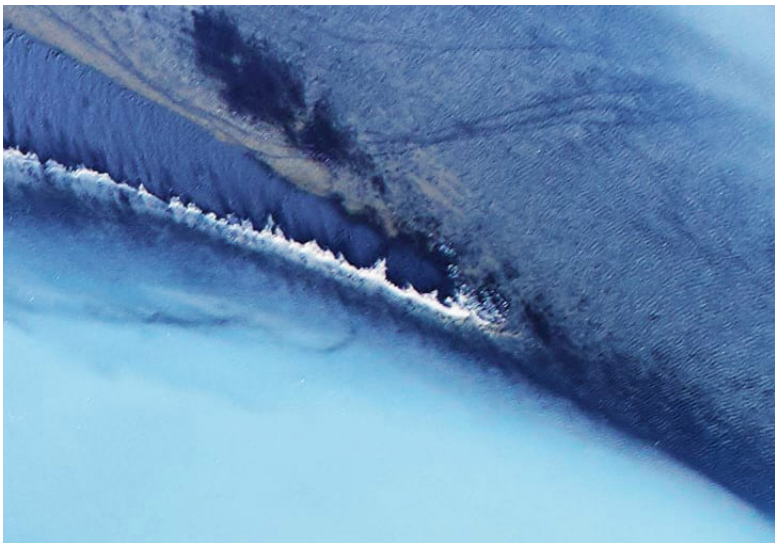
- les objectifs de sécurité ;
- les scénarios envisagés ;
- le programme de tests correspondant.

Si leur statut d'Opérateurs d'Importance Vitale (OIV) imposait déjà aux plus grandes banques et compagnies d'assurance un certain nombre d'obligations, avec DORA, c'est tout le secteur financier, au sens large, qui va devoir mettre en place une politique systématique, standard et rigoureuse en matière de tests de cybersécurité. Même pour les établissements les plus avancés, cela nécessitera au minimum quelques ajustements.

Des dispositions pratiques pour encadrer la mise en œuvre

DORA encadre la mise en œuvre des tests par des dispositions pratiques et rigoureuses :

- Les tests devront être directement réalisés sur les environnements de production, et ce, au moins une fois par an pour les fonctions dites critiques ou importantes ;
- Les entités les plus sensibles devront procéder à des tests avancés d'intrusion tous les trois ans au moins, l'autorité compétente pouvant, selon les circonstances, demander à augmenter ou réduire cette fréquence ;
- Afin d'éviter les conflits d'intérêt, les tests devront toujours être réalisés par des testeurs externes pour les établissements de crédit sensibles, et au minimum tous les trois tests pour les autres établissements. Pour réaliser leur inspection ou leur audit dans les règles de l'art, ces testeurs devront avoir le niveau requis et présenter un certain nombre de garanties de compétences et d'indépendance, en particulier via une certification (ISO 19011). Idéalement, on s'efforcera aussi de varier les approches et les méthodes ;
- Étant donné l'importance croissante de la supply chain comme vecteur de menace, DORA précise aussi les conditions de mise en œuvre des tests chez les fournisseurs IT. Ceux-ci ne pourront s'y opposer et les contrats passés avec les prestataires de fonctions critiques ou importantes devront faire apparaître des contraintes telles que l'obligation de coopérer pleinement aux pentests et un accès illimité au donneur d'ordre ou à l'autorité pour leurs audits ;
- En revanche, pour alléger les coûts et le fardeau pour les donneurs d'ordre comme pour leurs fournisseurs, le texte autorise la réalisation de tests groupés de ces derniers. Dans cette perspective, les organismes de place (Office de Coordination Bancaire et Financière, Fédération Bancaire Française, Fédération Française des Sociétés d'Assurance…) pourraient jouer un rôle pour favoriser et organiser cette mutualisation ;
- Enfin, les organisations devront documenter la démarche et produire un rapport structuré, lequel débouchera sur d'éventuelles mesures correctives. Ces éléments devront être communiqués aux autorités, qui pourront surveiller la mise en œuvre et les résultats de ce plan d'action.



Une voie à suivre

Analyse des risques en amont, indépendance des testeurs, transparence, amélioration continue : en définitive, DORA apparaît moins comme une nouvelle contrainte réglementaire que comme la marche à suivre pour hisser les tests de cybersécurité au niveau de maturité qu'exige le grand virage numérique actuel du secteur financier.

De bonnes pratiques dont les organisations des autres secteurs d'activité auraient sans doute grand intérêt à s'inspirer elles aussi, puisque la directive NIS 2 impose des exigences plus limitées en matière de tests…

Erwan Michel
Consultant en Sécurité de l'Information,
Capgemini France

DORA : pour une gestion de crise plus structurée

En dépit des meilleurs efforts, des incidents de cybersécurité sont inévitables. Aussi, DORA impose une préparation rigoureuse de la gestion de crise, insistant tout particulièrement sur le partage d'information, la communication et l'entraînement.

Conscientes qu'en matière d'IT le risque zéro n'existe pas, de plus en plus d'organisations ont mis en place des dispositifs et des procédures afin de réagir efficacement en cas d'incident de sécurité. Si ces plans de surveillance, de continuité et de reprise d'activité, et de gestion de crise se fondent en général sur de bonnes pratiques reconnues, ils ne sont ni systématiques ni homogènes à l'échelle sectorielle. En cas d'incident, les clients, les collaborateurs et les partenaires peuvent rester dans le flou concernant sa nature, ses impacts et la durée de sa résolution comme l'ont encore montré dernièrement des dysfonctionnements affectant les systèmes de paiement d'acteurs majeurs.

Avec le règlement européen DORA, la capacité de gestion de crise devient une obligation, poussant le secteur financier à se structurer sur les plans opérationnels et organisationnels. L'objectif est à la fois de :

- renforcer la protection des parties prenantes au niveau de chaque établissement ;
- renforcer la sécurité collective en ayant une visibilité accrue et plus précoce sur des incidents qui pourraient affecter tout le secteur ;
- répondre à un besoin d'harmonisation, rendu fondamental par le caractère transfrontalier et interdépendant des risques. Ce qui a notamment fait défaut lors de cyberattaques de grande envergure, tels que les rançongiciels NotPetya et WannaCry qui ont touché plusieurs milliers de sociétés dans le monde.

DORA entend donc faire progresser les établissements financiers en matière de gestion de crise en ce qui concerne le partage d'information, la communication et la nécessité absolue de s'entraîner.

Une remontée d'information formalisée

DORA formalise la notification aux régulateurs nationaux en cas d'incident (en France l'ACPR, l'Autorité de Contrôle Prudentiel et de Résolution et l'AMF, l'Autorité des Marchés Financiers), en demandant à ce qu'un certain nombre d'éléments techniques standards soient systématiquement rapportés aux autorités européennes de surveillance. De cette manière, chaque acteur devient un capteur d'indicateurs de compromission (IoC), contribuant à accroître la connaissance des menaces (threat intelligence) et permettant de prévenir au plus tôt le reste de la place financière.

Cette grille, dont le contenu sera précisé par les textes d'application, fait évoluer les rapports d'incidents que les entreprises produisaient jusqu'ici, souvent avec un prisme essentiellement technique et interne. Outre les caractéristiques et les impacts techniques de l'incident, il faudra en effet être capable d'évaluer tout ce qu'il entraîne pour l'organisation et ses parties prenantes : coûts, impacts sur les opérations et les affaires, conséquences pour les clients et les collaborateurs… La DSI et la direction des risques ne pouvant apprécier seules l'étendue de ces répercussions, le règlement DORA pousse donc à ce que le risque numérique soit désormais pris en compte de façon globale et transverse au sein de toute l'organisation, sous l'œil et le patronage de la direction générale.

L'importance clé de la communication

DORA met également l'accent sur l'importance de la communication en cas de crise. Le texte impose notamment de définir une stratégie dédiée et de désigner un responsable pour communiquer en cas de crise.

Avec cette obligation, l'établissement qui ne communiquera pas, ou mal, en cas d'incident sera décrédibilisé auprès de ses pairs, des autorités de régulation et, surtout, du public. Pour ne pas se retrouver dans cette situation, il est fondamental d'anticiper divers scénarios de crise et de préparer pour chacun d'eux des éléments de langage adéquats, de prérédiger des contenus et d'identifier les destinataires (clients, autorités, médias, collaborateurs…) de la communication. On veillera aussi à adapter les messages à ces cibles tout en restant cohérent avec le positionnement et le discours usuel de la marque (à l'inverse, on sera aussi attentif à éviter dans la communication ordinaire de l'entreprise tout élément qui pourrait se retourner contre elle en cas de crise).

Les organisations devront aussi veiller à disposer d'un outillage approprié et particulièrement robuste. Celui-ci doit en effet être imperméable à la crise pour que les acteurs clés puissent quoi qu'il arrive collaborer et diffuser leurs messages en interne et en externe.

S'entraîner, une nécessité

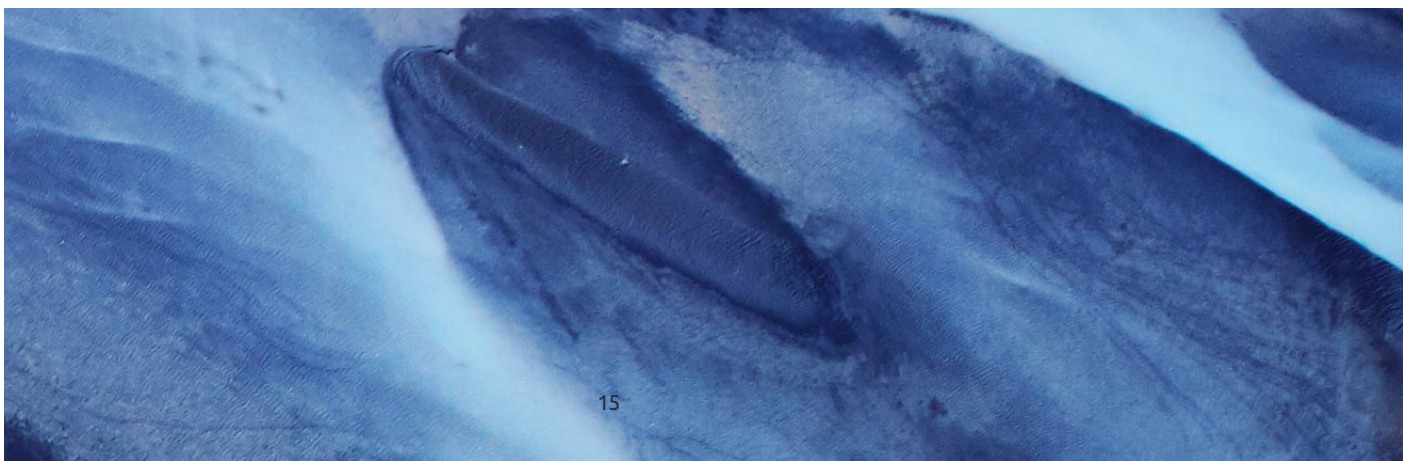
Aucune préparation n'est toutefois complète sans entraînement ni confrontation avec la réalité.

L'ensemble de la procédure de gestion de crise devra donc être testée dans des conditions les plus proches possibles d'un véritable incident, et les acteurs devront s'exercer pour tenir efficacement leur rôle le moment venu. Des enseignements devront être tirés de ces entraînements pour compléter et ajuster le dispositif afin d'éviter les mauvaises surprises. Enfin, l'implication et le sponsorship de la direction sont particulièrement importants pour que chacun soit mobilisé et contribue à ces efforts de préparation avec le sérieux qui s'impose.

Comme sur les autres aspects de la résilience face au risque numérique, le règlement européen DORA, réservé au secteur financier, pourrait préfigurer en matière de gestion de crise ce que NIS 2 demandera à l'ensemble des entreprises. Et, ici aussi, cela doit être moins perçu comme une contrainte que comme l'opportunité de structurer, renforcer et harmoniser les pratiques pour mettre en résonance protections individuelle et collective.

Olivier Gellez
Consultant Gouvernance et Stratégie de Sécurité, Capgemini

Lucie Shen
Consultante Digital Trust & Security, Capgemini Invent



NIS 2, DORA : une incitation à la modernisation ?

Pour beaucoup d'organisations, la mise en conformité avec DORA et NIS 2 s'annonce comme un chantier conséquent. Pour l'alléger tout en renforçant sa sécurité, le plus efficace pourrait être de moderniser préalablement ses systèmes.

Bien que les règlementations européennes DORA et NIS 2 n'aient ni le même périmètre ni tout à fait le même objectif, ces deux textes partagent de nombreux points communs, parmi lesquels l'attention toute particulière portée à la gestion des incidents. Celle-ci doit désormais faire l'objet d'une démarche structurée, prévoyant la mise en place de processus et outillages appropriés. De quoi poser la question plus globale du renouvellement complet du système d'information (SI) des organisations.

Une gestion de crise plus structurée

Jusqu'à présent, si l'on exclut les Opérateurs d'Importance Vitale (OIV) et les organisations déjà soumises à NIS 1, chacun gérait ses incidents de cybersécurité à sa manière, en interne, avec ses prestataires et, si possible, en toute discrétion.

Avec NIS 2 et DORA, la grande nouveauté est qu'il faut désormais systématiquement alerter les autorités, en respectant des grilles de reporting standards, et dans des délais très brefs (4h pour la notification initiale de l'incident au titre de DORA).

Les organisations sont par conséquent dans l'obligation d'avoir mis en place des processus efficients et un outillage approprié pour pouvoir détecter au plus tôt les incidents, en évaluer rapidement la gravité et les impacts, notamment business, et enfin structurer ces informations pour les communiquer aux autorités.

- **Un outillage approprié**

  Nombre d'organisations ne disposent pas pour le moment de l'outillage adéquat pour gérer correctement un incident de sécurité. Même pour celles ayant déjà un Security Operations Center ou SOC (ce qui est loin d'être toujours le cas !), celui-ci donne surtout une vision technique des incidents et ne dit rien, le plus souvent, de ses conséquences pour les clients. Quant aux organisations qui possèdent déjà des grilles d'impacts, il est peu probable qu'elles coïncident avec ce qui sera demandé et la question se posera de savoir s'il vaudra mieux avoir deux reportings distincts en parallèle ou les fusionner.

- **Des processus efficients**

  Après la détection et la notification de l'incident vient son traitement proprement dit, pour lequel NIS 2 exige là aussi que des processus adéquats aient été prévus. C'est bien sûr très utile, mais aussi extrêmement contraignant, surtout pour les plus petites entités concernées. En effet, beaucoup, comme les collectivités locales, sont aujourd'hui très en retard en matière de cybersécurité, non qu'elles ne prennent pas le sujet au sérieux mais parce qu'elles n'ont ni les ressources – financières et humaines – ni la taille critique pour s'équiper.

Souvent d'ailleurs pour les mêmes raisons, ces organisations s'appuient encore largement sur des systèmes anciens, hétérogènes, mal entretenus, peu surveillés et qui sont précisément les plus vulnérables et les plus difficiles à protéger. Pour elles, aussi bien en termes financiers que de compétences, de culture et, bien sûr, de technologies, la marche de la mise en conformité sera donc assez haute.

Et s'il valait mieux moderniser ?

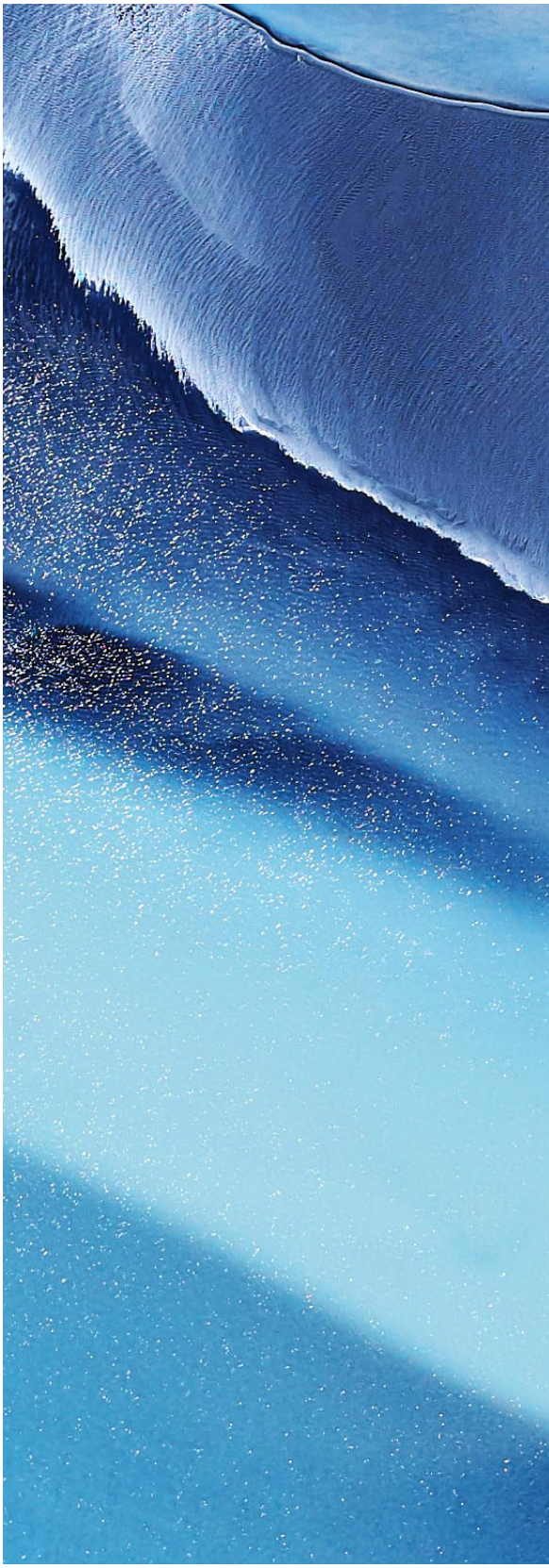
Dans ces conditions, cela peut être l'opportunité d'adopter une démarche radicale et de considérer que la meilleure façon de traiter des incidents est encore de ne pas en avoir ! En modernisant son IT, en se dotant d'un SI à l'état de l'art des technologies, nativement sécurisé, surveillé et administré par des experts (dans le cloud ou en infogérance), et compatible avec des outils de sécurité modernes, les risques sont considérablement diminués et la mise en conformité grandement facilitée.

Tout bien pesé, il pourrait donc être plus efficace, et pas forcément plus compliqué ni plus coûteux, de migrer ses anciens systèmes vers de nouvelles solutions que de chercher à les sécuriser. Et cela sans même tenir compte des bénéfices métiers induits par cette modernisation : innovation, expérience utilisateur, coûts de possession…

Que ce soit intentionnel ou non de la part du législateur, NIS 2 apparaît donc comme un accélérateur indirect du renouvellement des SI des organisations, de la même manière que le renforcement des normes de sécurité a pu l'être pour le parc automobile. Avec des exigences proches, DORA pourrait jouer un rôle similaire dans le secteur financier, même si l'équipement et la culture en matière de cybersécurité y sont souvent déjà plus développés qu'ailleurs.

Reste que les délais sont courts, même si, en ce qui concerne NIS 2, les autorités semblent disposées à accorder un peu plus de temps aux organisations pour se préparer. Ce répit n'est néanmoins pas destiné à différer le chantier, mais bien à y consacrer toute l'attention nécessaire. Pour bâtir une stratégie de mise en conformité (passant ou non par la modernisation), réunir les budgets, choisir les solutions, les mettre en œuvre et accompagner le changement, ce sursis ne sera pas de trop.

Olivier Gellez
Consultant Gouvernance et Stratégie de Sécurité, Capgemini



Conclusion

Les réglementations DORA et NIS 2 prennent acte de la place fondamentale qu'occupe désormais le numérique dans nos sociétés et du risque systémique induit et amplifié par la forte interconnexion des systèmes. Comme la vaccination, elles font passer la sécurité collective par des mesures de protection individuelles, en l'occurrence exigées des acteurs du secteur financier et des entreprises de secteurs jugés sensibles.

Responsables désignés, les dirigeants ne doivent surtout pas voir dans ces textes une nouvelle série de contraintes techniques. Ils leur donnent au contraire l'opportunité de prendre enfin toute la mesure du risque cyber pour leur organisation et ses parties prenantes, et d'engager les travaux qui s'imposent.

Une originalité et une qualité communes à DORA et NIS 2 est de présenter une approche par les risques. C'est un gage de pragmatisme et d'efficacité, mais cela nécessite aussi d'avoir une vision globale, orientée business, et de prendre le temps de l'analyse et de la réflexion, ce qui peut allonger d'autant la mise en conformité.

C'est pourquoi il est impératif de se lancer sans attendre. Pas seulement pour satisfaire les autorités de contrôle, qui ont déjà commencé leurs vérifications, mais pour ne pas devoir agir dans l'urgence d'ici quelques mois. Dans la précipitation, on risquerait en effet de créer des doublons, de passer à côté de certaines obligations, de bâcler ses solutions, et, au final, de payer cher une sécurité et une conformité incertaines. Surtout, attendre, c'est retarder le renforcement de sa sécurité numérique. Et dans le contexte actuel, qui peut se le permettre ?

Aperçu du cadre réglementaire de l'UE en matière de cybersécurité

	Digital Operational Resilience Act	Network and Information Systems 2
Objectifs	• Améliorer la **résilience opérationnelle numérique des entités financières européennes**	• Harmoniser et garantir un niveau élevé d'exigences en matière de **cybersécurité pour les entités fournissant des services importants ou critiques dans toute l'UE**
Cibles	• Autorités européennes et nationales de surveillance financière • Entités financières (y compris les fournisseurs informatiques critiques)	• États membres de l'UE et autorités compétentes • **Entités essentielles et importantes** (champ d'application plus large que NIS-1)
Calendrier de mise en œuvre	• Application complète : **à partir du 17 janvier 2025**	• Transposition en droit national : **d'ici le 14 octobre 2024** • Application des mesures par les États membres : **à partir du 18 octobre 2024** • Liste des entités essentielles et importantes par les États membres de l'UE : **d'ici le 17 avril 2025**

Exigences essentielles	• Gestion des risques liés aux TIC
	• Gestion et reporting d'incidents
	• Tests de résilience opérationnelle numérique
	• Gestion des risques liés aux tiers
	• Partage d'informations
		• (Auto-) enregistrement des entités
		• Mesures organisationnelles et techniques de cybersécurité, y compris :
		  • Gouvernance et gestion des risques
		  • Reporting d'incidents et de menaces
		  • Sécurité de la chaîne d'approvisionnement

À propos de Capgemini

Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle et IA générative, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,1 milliards d'euros en 2024.

Get the future you want* | www.capgemini.com

*Capgemini, le futur que vous voulez