Recommandation du Conseil sur la sécurité numérique des activités critiques

Instruments juridiques de l'OCDE

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Ce document est publié sous la responsabilité du Secrétaire général de l'OCDE. Il reproduit un instrument juridique de l'OCDE et peut contenir des informations complémentaires. Les opinions ou arguments exprimés dans ces informations complémentaires ne reflètent pas nécessairement les vues officielles des pays Membres de l'OCDE.

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

Pour accéder aux textes officiels à jour des instruments juridiques de l'OCDE, ainsi qu'aux informations s'y rapportant, veuillez consulter le Recueil des instruments juridiques de l'OCDE http://legalinstruments.oecd.org.

Merci de citer cet ouvrage comme suit :
OCDE, *Recommandation du Conseil sur la sécurité numérique des activités critiques*, OECD/LEGAL/0456

Collection : Instruments juridiques de l'OCDE

Crédits photo : © Adobe Stock/mumemories

Informations Générales

La Recommandation sur la sécurité numérique des activités critiques a été adoptée par le Conseil de l'OCDE le 11 décembre 2019 sur proposition du Comité de la politique du numérique (CPN). Elle remplace la Recommandation de 2008 sur la protection des infrastructures d'information critiques (ci-après « Recommandation PIIC ») [OECD/LEGAL/0361].

Les activités critiques sont de plus en plus exposées au risque de sécurité numérique

La plupart des activités économiques et sociales dépendent du numérique. Parmi ces activités, certaines sont critiques car leur interruption ou leur perturbation pourrait avoir de graves conséquences sur la santé, la sûreté et la sécurité des citoyens ; ou sur le fonctionnement efficace des services essentiels à l'économie et à la société, ainsi que sur celui des pouvoirs publics ; ou plus largement, sur la prospérité économique et sociale.

La Recommandation PIIC de 2008 fut une norme internationale novatrice qui a joué un rôle clé pour sensibiliser quant à la nécessité d'élaborer des politiques pour mieux protéger les systèmes d'information et les réseaux qui soutiennent les activités critiques (les « infrastructures d'information critiques » ou IIC).

Cependant, depuis 2008, la dépendance numérique des activités critiques a augmenté et accélère aujourd'hui avec la transformation numérique et la généralisation de technologies telles que le « big data », l'intelligence artificielle et l'internet des objets. On constate également la croissance du nombre et de la sophistication des menaces de sécurité numérique. Beaucoup de gouvernements prévoient une augmentation de la fréquence et de la sévérité des incidents de sécurité numérique affectant les activités critiques dans les prochaines années, conduisant potentiellement à des désastres à grande échelle.

Face à la dépendance numérique croissante des activités critiques et à l'augmentation des menaces qui les visent poussent les gouvernements à adopter des politiques pour renforcer la sécurité numérique des activités critiques. Cependant, de telles politiques ne devraient pas réduire les bénéfices de la transformation numérique dans les secteurs critiques via des contraintes qui pourraient inhiber l'innovation ou restreindre inutilement l'usage des technologies numériques, leur caractère dynamique et leur ouverture.

Un cadre de travail modernisé pour augmenter la sécurité numérique des activités critiques

Le Groupe de Travail sur la Sécurité et la Vie Privée dans l'Économie Numérique (GTSVPEN) du CPEN a suivi la mise en œuvre de la Recommandation PIIC de 2008 et convenu de la nécessité de mettre à jour la Recommandation et de la remplacer afin de tenir compte des changements survenus depuis 2008 ainsi que de l'expérience acquise par les Adhérents.

La Recommandation de 2019:

- se concentre sur les activités économiques et sociales critiques reposant sur des infrastructures d'information plutôt que sur lesdites infrastructures. Cette évolution promeut une approche économique et sociale –plutôt que purement technique– de la gestion du risque de sécurité numérique. Ce faisant, elle assure la cohérence avec la Recommandation de 2015 sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale [OECD/LEGAL/0415].
- aide à clarifier le positionnement de ce domaine de l'action publique dans le paysage plus large des politiques pour la gestion du risque national et pour la protection des infrastructures critiques.
- expose un ensemble de recommandations pour s'assurer que les politiques visant les opérateurs d'activités critiques se concentrent sur ce qui est critique pour l'économie et la société sans leur imposer de fardeau injustifié. Ces recommandations soutiennent également les Adhérents dans : (i) l'adaptation de leur cadre de politique publique d'ensemble ; (ii) la promotion et la construction de partenariats fondés sur la confiance ; et (iii) l'amélioration de la coopération au niveau international.

Deux ans d'élaboration de la Recommandation de 2019

Le processus d'examen de la Recommandation PIIC de 2008 a duré plus de deux ans avec des contributions en provenance de plus de dix-huit pays, de la société civile, et des représentants de l'industrie sur la base d'un questionnaire. L'analyse des réponses a souligné le besoin de mettre à jour la Recommandation PIIC et a fourni des informations pour guider l'élaboration de la Recommandation de 2019.

En 2018, un groupe informel composé d'experts des gouvernements, des entreprises, de la société civile et de la communauté technique de l'Internet a été créé pour guider le Secrétariat dans l'élaboration de la Recommandation de 2019.

Mise en œuvre et outils de dissémination

Pour soutenir la mise en œuvre de la Recommandation, le CPEN tiendra lieu de forum pour (a) l'échange d'informations sur la sécurité numérique des activités critiques afin d'identifier les bonnes pratiques en coordination avec d'autres instances internationales, ainsi que pour (b) la réalisation de travaux analytiques à l'appui de la mise en œuvre de la Recommandation.

Pour plus d'information, consultez: www.oecd.org/sti/ieconomy/security.htm.
Contact: digitalsecurity@oecd.org.

Mise en œuvre

La transformation numérique des activités critiques telles que la fourniture d'eau, d'énergie, de télécommunications et de services bancaires expose de plus en plus ces activités à des menaces de cybersécurité qui peuvent affecter la santé, la sûreté et la sécurité des citoyens, le fonctionnement des services essentiels, ou plus largement, la prospérité économique et sociale.

Approuvée par le Comité de la politique de l'économie numérique le 31 août 2021, la note est basée sur la Recommandation et soutient sa mise en oeuvre. Elle présente les concepts clé, tels que « activités critiques », « infrastructure critique d'information », « cybersécurité », et « gestion du risque de sécurité numérique ». Elle vise à aider les décideurs de politiques publiques à identifier ce qui devrait être protégé et quels types de mesures les opérateurs d'activités critiques devraient adopter. Elle discute également le cadre institutionnel nécessaire pour développer et superviser les politiques pour améliorer la sécurité numérique des activités critiques, y compris les partenariats basés sur la confiance, et fournit en annexe une sélection d'approches de politiques publiques adoptées dans plusieurs pays.

LE CONSEIL,

CONSIDÉRANT l'Article 5 b) de la Convention relative à l'Organisation de Coopération et de Développement Économiques en date du 14 décembre 1960 ;

CONSIDÉRANT la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel [OECD/LEGAL/0188] ; la Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet [OECD/LEGAL/0387] ; la Recommandation du Conseil sur la gouvernance des risques majeurs [OECD/LEGAL/0405] ; la Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale [OECD/LEGAL/0415] (ci-après dénommée « Recommandation sur le risque de sécurité numérique ») et la Déclaration sur l'économie numérique : innovation, croissance et prospérité sociale (Déclaration de Cancún) [OECD/LEGAL/0426] ;

CONSIDÉRANT l'expérience et les meilleures pratiques acquises au titre de la mise en œuvre de la Recommandation du Conseil sur la protection des infrastructures d'information critiques [OECD/LEGAL/0361], que la présente Recommandation vient remplacer ;

RECONNAISSANT que

- la transformation numérique touche l'ensemble des activités économiques et sociales, et, ce faisant, stimule l'innovation et induit des avantages significatifs, mais expose également ces activités à un risque de sécurité numérique croissant ;
- le risque de sécurité numérique émane de menaces, intentionnelles ou non, qui se jouent par nature des frontières, exploitent les vulnérabilités et produisent des incidents affectant à la disponibilité, l'intégrité et la confidentialité des données, du matériel, des logiciels et des réseaux sur lesquelles ces activités dépendent;

RECONNAISSANT que la multiplicité et la complexité des dépendances numériques par-delà les frontières sectorielles et géographiques et tout au long des chaînes de valeur des activités critiques génèrent un risque de sécurité numérique partagé qui ne saurait être réduit significativement par un seul et unique acteur pour tous les autres; et que, par conséquent, chaque acteur est à la fois dépendant de tous les autres acteurs et responsable envers eux pour gérer le risque de sécurité numérique ;

RECONNAISSANT l'importance de mettre en place des partenariats entre les secteurs public et privé et en leur sein afin d'aborder le risque de sécurité numérique inhérent aux activités critiques selon une approche cohérente et globale ;

RECONNAISSANT que la Recommandation sur le risque de sécurité numérique fournit un cadre robuste pour renforcer la sécurité numérique des activités économiques et sociales sans restreindre les opportunités qu'offre la transformation numérique ;

RECONNAISSANT que les activités critiques conduites par divers opérateurs dans différents secteurs et pays dépendent des mêmes technologies numériques et peuvent par conséquent être perturbées simultanément par des menaces exploitant des vulnérabilités communes ; que les incidents de sécurité numérique peuvent se propager extrêmement rapidement d'un opérateur, d'un secteur et d'un pays à l'autre ; et que les perturbations de l'exécution des activités critiques occasionnées par les incidents de sécurité numérique à un endroit peuvent provoquer des effets en cascade sur d'autres opérateurs, secteurs et pays, voire toucher des régions et mettre à mal la stabilité internationale ;

RECONNAISSANT que les conséquences des incidents de sécurité numérique affectant les activités critiques conduites par des opérateurs publics et privés peuvent dépasser les seuls intérêts desdits opérateurs et toucher une société tout entière et d'autres à l'étranger ; et que, de ce fait, tout risque résiduel pris par ces opérateurs pourrait avoir des répercussions sur tous ceux qui dépendent de ces activités et sur la société dans son ensemble ;

RECONNAISSANT que le renforcement de la sécurité numérique des activités critiques est une priorité d'action nationale ; que les disparités entre les politiques publiques des différents pays ajoutent à la complexité de la gestion de la sécurité numérique d'activités critiques interdépendantes à l'échelle transfrontière ; et que la coopération internationale s'avère par conséquent essentielle pour réduire ces disparités et maximiser l'efficacité, au plan mondial, des politiques nationales ;

CONSCIENT que la gestion du risque de sécurité numérique inhérent aux activités critiques devrait se faire dans le respect des règles de protection de la vie privée et des données à caractère personnel ;

CONSCIENT de la diversité des cultures ainsi que des cadres juridiques et institutionnels dans les pays Membres et non Membres adhérant à la présente Recommandation (ci-après dénommés les « Adhérents ») et de la possible utilisation de terminologies distinctes dans les politiques mises en œuvre par les Adhérents pour renforcer la sécurité numérique des activités critiques ;

Sur proposition du Comité de la politique de l'économie numérique :

I. **CONVIENT** que la présente Recommandation a pour objet de fournir des orientations sur les modalités de mise en œuvre de la Recommandation sur le risque de sécurité numérique en vue de maintenir la continuité, la résilience et la sécurité des activités critiques sans diminuer les avantages de la transformation numérique.

II. **CONVIENT** qu'aux fins de la présente Recommandation :

- **Les activités critiques** désignent les activités économiques et sociales dont l'interruption ou la perturbation aurait de graves conséquences :
  - sur la santé, la sûreté et la sécurité des citoyens ; ou
  - sur le fonctionnement efficace des services essentiels à l'économie et à la société, ainsi que sur celui des pouvoirs publics ; ou
  - plus largement, sur la prospérité économique et sociale.

  Les activités critiques sont identifiées sur la base d'une évaluation nationale du risque.
- **Les opérateurs** sont les entités publiques et privées qui mènent à bien des activités critiques.
- **Les fonctions critiques** désignent les processus sans lesquels les opérateurs ne pourraient mener à bien efficacement leurs activités critiques.
- **L'écosystème numérique** désigne l'environnement numérique qui soutiennent les fonctions critiques d'un opérateur tout au long de la chaîne de valeur des activités critiques. Il couvre les actifs numériques, tels que le matériel, les logiciels, les réseaux et les données, les technologies opérationnelles qui détectent ou entraînent des modifications des processus physiques, ainsi que les entités, personnes et processus internes et externes qui les conçoivent, en assurent la maintenance, et les exploitent, ainsi que les relations qu'ils entretiennent.

CADRE D'ACTION GÉNÉRAL

III. **RECOMMANDE** que les Adhérents mettent au point une **approche stratégique** de la gestion du risque de sécurité numérique inhérent aux activités critiques en :

1. Adoptant, au plus haut niveau de l'administration et dans le cadre d'une stratégie nationale de sécurité numérique, des **objectifs clairs** en vue de renforcer la sécurité numérique et la résilience des activités critiques, et d'assurer la cohérence avec l'évaluation nationale du risque et les stratégies propres à certains risques et secteurs.
2. Adoptant et mettant à la disposition du public un mécanisme de **gouvernance nationale** qui confère à des organismes publics spécifiques l'autorité et la responsabilité de concevoir et mettre en œuvre avec les parties prenantes concernées des politiques visant à renforcer la sécurité

numérique des activités critiques entre les différents secteurs et en leur sein. Le mécanisme de gouvernance nationale devrait en outre identifier, en tant que de besoin, tout rôle d'appui que pourraient jouer les organismes publics chargés de la sécurité et de la défense nationales.

3. Assurant une **coordination nationale**, à l'échelle de l'ensemble de l'administration, en vue de :

   a. Nouer une coopération intragouvernementale, en tenant pleinement compte de l'importance d'un dialogue entre les spécialistes de la sécurité numérique et les experts sectoriels ;

   b. Veiller à la cohérence des mesures adoptées dans les différents secteurs, le cas échéant, et résoudre les éventuels conflits entre les objectifs d'action ;

   c. Procéder à une allocation efficace des ressources entre les organismes publics compétents et créer une masse critique d'expertise et de compétences ; et

   d. Faciliter la coopération transfrontière.

IV. RECOMMANDE que les Adhérents **développent les capacités** nécessaires pour soutenir la gestion du risque de sécurité numérique et la résilience des activités critiques en s'attelant à :

1. Mettre en place ou renforcer leurs **capacités de réponse aux incidents**, avec par exemple l'établissement d'une ou plusieurs équipes de réponse aux incidents de sécurité informatique (CSIRT ou CERT) et/ou centres d'opérations de sécurité (SOC), assurant une mission de surveillance, de veille, d'alerte et de mise en œuvre de mesures de rétablissement, ainsi que des mécanismes visant à renforcer la coopération et la communication entre les acteurs intervenant dans la réponse aux incidents ;

2. Faciliter la **coopération entre les équipes CERT/CSIRT/SOC et les opérateurs**, y compris pour ce qui est du signalement et de l'analyse des incidents, afin de favoriser une coopération opérationnelle prompte et efficace ;

3. Appliquer les meilleures pratiques pour la gestion du risque de sécurité numérique relative aux **activités numériques critiques assurées par les pouvoirs publics**.

4. Promouvoir la mise en œuvre des **normes internationales en matière de sécurité numérique**, ainsi que des méthodologies, manuels de référence sur la sécurité, meilleures pratiques et outils connexes ;

5. Fournir un **appui aux opérateurs**, en tant que de besoin, notamment en:

   a. partageant les informations sur les menaces et les vulnérabilités ;

   b. aidant les opérateurs à évaluer les risques et définir des mesures de traitement appropriées ;

   c. fournissant une assistance et/ou des directives en cas d'incident ou de crise ; et

   d. mettant à disposition des boîtes à outils, des méthodologies, des pratiques optimales et des outils ;

6. Favoriser le **développement du marché mondial** des services et produits de sécurité de confiance, notamment des services d'infogérance, d'audit et de réponse aux incidents, y compris, le cas échéant, par divers mécanismes indiquant la nature et le degré de sécurité de façon fiable;

7. Soutenir le développement d'une **main-d'œuvre qualifiée**, capable de gérer le risque de sécurité numérique sectoriel et intersectoriel ;

8. Adopter et encourager l'adoption de processus de **divulgation et de gestion responsables et coordonnées des vulnérabilités**, et encourager et protéger les chercheurs en sécurité ; et

9. Partager, en tant que de besoin, avec les opérateurs et d'autres acteurs, les **données statistiques, agrégées** comme il se doit, issues du signalement des incidents ;

V. RECOMMANDE que les Adhérents mettent en place des cycles de **suivi** et de **surveillance** fondés sur des données probantes dans le but *i)* d'évaluer et d'apprécier la mise en œuvre des exigences

par les opérateurs, et *ii)* de favoriser l'amélioration continue des politiques, des cadres juridiques et des dispositifs d'autoréglementation afin de parvenir au niveau de protection attendu.

VI. RECOMMANDE que les Adhérents **intègrent le risque de sécurité numérique inhérent aux activités critiques dans leur gestion nationale du risque**, de sorte que :

1. Les évaluations nationales du risque permettent l'identification des activités critiques et de leurs opérateurs, en prenant en considération la chaîne de valeur des activités critiques ; et
2. Les opérateurs soient incités à réaliser une évaluation cyclique du risque d'entreprise afin de repérer les fonctions critiques nécessaires à l'exécution des activités critiques.

MESURES À L'INTENTION DES OPÉRATEURS

VII. RECOMMANDE que les Adhérents s'assurent que les opérateurs :

1. soient responsables de la gestion du risque de sécurité numérique inhérent aux fonctions critiques en vue d'assurer la continuité, la résilience et la sécurité des activités critiques qu'elles rendent possible ; et
2. réduisent de manière effective le risque de sécurité numérique inhérent aux fonctions critiques à un niveau qui soit acceptable pour la société, en conformité avec l'évaluation nationale du risque, en les incitant ou en les obligeant, le cas échéant, à prendre des mesures de gouvernance, de protection, de détection, de réponse aux incidents et de résilience. Ces mesures devraient notamment porter sur les éléments suivants :

   a. Gouvernance – établir un cadre organisationnel pour l'évaluation et le traitement cycliques du risque de sécurité numérique

   i. Attribuer la responsabilité de la gestion du risque de sécurité numérique au plus haut niveau de direction ;

   ii. Intégrer la gestion du risque de sécurité numérique et la gouvernance de la sécurité numérique au cadre général de gestion cyclique du risque d'entreprise ;

   iii. Adopter une politique interne de gestion du risque de sécurité numérique qui définisse :

      a) les responsabilités et les modalités de redevabilité pour ce qui est de la propriété, de l'évaluation et du traitement du risque de sécurité numérique, de l'acceptation du risque résiduel, et des processus d'examen des décisions liées au risque de sécurité numérique ;

      b) les moyens de garantir que la gestion du risque de sécurité numérique fasse systématiquement partie intégrante des décisions stratégiques et opérationnelles liées à l'utilisation des technologies numériques ; et que les dirigeants et décideurs soient informés et accompagnés par des experts de la sécurité numérique ;

   iv. Cartographier l'écosystème numérique des opérateurs, notamment les dépendances internes et externes en vue d'identifier les composantes essentielles aux fonctions critiques ;

   v. Mener à bien des évaluations cycliques du risque de sécurité numérique pour les fonctions critiques, en tenant compte de l'écosystème numérique des opérateurs et des conséquences potentielles que les incidents de sécurité numérique pourraient avoir sur les activités critiques des opérateurs eux-mêmes, sur les tierces parties, en particulier sur les autres opérateurs intervenant dans le même secteur et dans d'autres secteurs, ainsi que sur l'ensemble de l'économie et de la société ;

vi. Déterminer, à la lumière de l'évaluation du risque de sécurité numérique, le niveau de risque à réduire, transférer, éviter et accepter (traitement du risque) ;

vii. Réaliser des audits périodiques de la sécurité numérique ;

viii. Investir dans la formation et le développement des compétences dans le domaine de la sécurité numérique ;

ix. Favoriser la mise en œuvre des meilleures pratiques de gestion du risque de sécurité numérique tout au long de la chaîne logistique ;

b. Protection – mettre en œuvre des mesures de sécurité appropriées pour réduire le risque de sécurité numérique inhérent aux fonctions critiques

i. Déterminer les mesures liées à l'architecture numérique, à l'administration du système, à la formation du personnel, à la maintenance de la sécurité numérique et à la sécurité physique de l'opérateur ;

ii. Maintenir des mesures appropriées en matière de gestion des identités, d'authentification et de contrôle d'accès ;

iii. Déterminer les mesures liées à la sécurité des données, y compris à la protection des données stockées et en transit ;

iv. Partager avec les pouvoirs publics et les experts, le cas échéant, les informations relatives aux répercussions économiques et sociales des incidents, dans l'optique de l'amélioration des cadres d'action publique en matière de sécurité numérique.

c. Détection et réponse – mettre en place des processus et des mesures afin de se défendre contre les incidents et d'y répondre

i. Mettre en place la gestion des informations et des événements de sécurité, la détection des incidents et les opérations de veille, et réaliser les analyses appropriées ;

ii. Mettre en place des processus et des mesures de gestion des incidents, des capacités de réponse aux incidents (des CERTs, par exemple), ainsi que des procédures à jour pour le traitement et l'analyse des incidents ;

iii. Signaler, le cas échéant, les incidents, y compris les quasi-incidents selon leur degré de criticité, à un organisme public compétent et/ou à d'autres entités ou instances pertinentes (telles que des forums de coopération sectorielle, par exemple) ;

iv. Communiquer, le cas échéant, les incidents au public dès que possible.

d. Résilience – adopter des mesures de préparation et de reprise appropriées afin d'assurer la continuité des fonctions critiques

i. Fixer des objectifs stratégiques et des plans tenant compte de la sûreté afin d'assurer la continuité des opérations, la gestion de crise et la reprise après sinistre ;

ii. Tester et améliorer à intervalles réguliers les plans de continuité des opérations, de gestion de crise et de reprise après sinistre, y compris en organisant et co-organisant des exercices internes, multi-opérateurs, intersectoriels et transfrontières et en prenant part à de tels exercices ; et

iii. Veiller à ce que les décideurs métiers des opérateurs soient chargés de la planification et de la mise en œuvre de la gestion de crise, avec le soutien d'experts techniques en sécurité numérique.

PARTENARIATS FONDÉS SUR LA CONFIANCE

VIII. RECOMMANDE que les Adhérents promeuvent et renforcent la confiance dans des partenariats durables afin de veiller à ce que la gestion du risque de sécurité numérique inhérent aux activités critiques

tienne dûment compte des dépendances par-delà les frontières sectorielles et géographiques. À cette fin, les Adhérents devraient :

1. Nouer des **partenariats en vue de l'élaboration et de la mise en œuvre de politiques** en favorisant :
    a. Un dialogue ouvert, au niveau national, entre les opérateurs et les organismes publics compétents afin de définir et d'appliquer les mesures que les opérateurs devraient entreprendre, en tenant compte des spécificités de chaque secteur, ainsi que des contraintes des opérateurs en termes de métiers, de ressources, de réglementation et de marché, notamment celles des petites et moyennes entreprises ;
    b. La coopération privé-privé et un dialogue structuré entre les opérateurs à l'échelle tant intrasectorielle qu'intersectorielle, et avec d'autres acteurs privés concernés (des fournisseurs, par exemple), afin de favoriser les échanges sur l'expertise en matière de sécurité numérique, les menaces et la gestion du risque ;
    c. Un dialogue permanent entre les spécialistes de la sécurité numérique et les experts sectoriels afin d'améliorer la compréhension mutuelle de leurs spécificités et contraintes respectives ; et
    d. La coopération bilatérale et multilatérale à l'appui du partage de connaissances et d'expérience quant aux politiques, pratiques et modèles de coordination nationaux avec les opérateurs, de même que l'action collective afin de :
        i. gérer le risque de sécurité numérique inhérent aux activités critiques en tenant compte des dépendances et interdépendances transfrontières ;
        ii. traiter les vulnérabilités, les menaces et les incidents de sécurité numérique intersectoriels et propres aux secteurs, ainsi que les répercussions sur les activités critiques.
2. Renforcer la **coopération opérationnelle** en prenant les mesures suivantes :
    a. Favoriser les partenariats à l'appui de la coopération entre les opérateurs, à l'intérieur et par-delà les secteurs et les pays, sur la prévention et la détection des incidents et la réponse qui y est apportée, en vue d'encourager le partage d'informations et les échanges sur les menaces, les vulnérabilités, les incidents, les impacts et les pratiques de gestion du risque ;
    b. Instaurer des conditions propices à une coopération formelle et informelle entre les opérateurs lorsqu'elle n'existe pas encore, y compris sans la participation des pouvoirs publics si cela peut nuire aux relations de confiance entre les parties aux partenariats ;
    c. Instaurer des conditions propices à la réalisation d'exercices de sécurité numérique avec les opérateurs concernés, au sein des secteurs et des pays et au-delà, afin de renforcer la préparation en matière de sécurité numérique, et de tester et d'améliorer les mécanismes de prise de décisions stratégiques et de coordination ;
    d. Inciter les opérateurs à participer aux réseaux internationaux ou régionaux de veille, d'alerte et de réponse aux incidents, en vue de favoriser l'échange d'informations et la coordination au niveau opérationnel, et d'améliorer la gestion de crise en cas d'incident dépassant le cadre des frontières ;
    e. Soutenir la collaboration transfrontière et l'échange d'informations dans le domaine de la recherche et du développement public-privé sur la sécurité numérique des activités critiques, notamment sur les méthodologies en matière d'évaluation d'impact des incidents de sécurité numérique ; et
    f. Soutenir la recherche avancée, stimuler l'innovation et collaborer au développement des compétences et des connaissances en matière de gestion du risque de sécurité numérique afin de disposer à l'avenir d'une main-d'œuvre qualifiée.

3. Instaurer des **conditions propices à la confiance** en vue de l'établissement de partenariats durables, en s'assurant que :

   a. les objectifs et les valeurs sur lesquels sont fondés les partenariats soient partagés par les partenaires et transparents pour le public ;

   b. les rôles et responsabilités des diverses parties prenantes soient clairement établis ;

   c. les partenariats soient fondés sur des règles claires acceptées par l'ensemble des partenaires, de sorte que leurs actions soient fiables, prévisibles et cohérentes dans le temps ;

   d. les partenaires tirent un bénéfice mutuel du partenariat au fil du temps, notamment en instaurant des conditions pour que les opérateurs partagent les informations avec les pouvoirs publics et reçoivent des informations de leur part ; et

   e. les informations partagées par les opérateurs et les pouvoirs publics :

      i. soient divulguées de manière volontaire, uniquement à destination des publics appropriés, dans le cadre de protocoles de partage d'informations ;

      ii. soient gérées de manière responsable, selon un ensemble de règles régissant leur réception, leur conservation, leur utilisation et leur diffusion, dans le respect des réglementations en matière de protection de la vie privée et des données à caractère personnel et d'autres réglementations protégeant la confidentialité des informations (telles que les secrets commerciaux, par exemple). De telles règles devraient en particulier garantir que les données à caractère personnel non liées à une menace relative à la sécurité numérique soient retirées avant tout échange d'informations ; et

      iii. soient utilisées exclusivement à des fins de protection.

   f. la confidentialité des informations liées au risque et à la gestion du risque que les opérateurs partagent avec les pouvoirs publics soient protégées de manière à éviter de compromettre inutilement la réputation et les intérêts commerciaux des opérateurs.

COOPÉRATION INTERNATIONALE

IX. **RECOMMANDE** que les Adhérents coopèrent activement au niveau international :

1. En partageant :

   a. des informations sur les rôles et responsabilités des organismes publics et autres parties prenantes chargées de la gestion du risque de sécurité numérique inhérent aux activités critiques avec les autres contreparties des pays Adhérents afin d'accélérer la mise en place de la coopération transfrontière ;

   b. les expériences d'élaboration et de mise en œuvre des politiques afin d'identifier les bonnes pratiques et, autant que faire se peut, de minimiser les différences entre les pays ; et

   c. des données statistiques agrégées issues, le cas échéant, des signalements d'incidents, et en travaillant de concert pour assurer la comparabilité internationale desdites statistiques.

2. En soutenant les efforts de développement de capacités afin d'aider les autres pays à élaborer et mettre en œuvre leurs politiques en matière de sécurité numérique des activités critiques, en tant que de besoin .

X. **INVITE** le Secrétaire général et les Adhérents à diffuser la présente Recommandation.

XI. **INVITE** les Adhérents à la Recommandation sur le risque de sécurité numérique à tenir dûment compte de la présente Recommandation et à y adhérer.

XII. **CHARGE** le Comité de la politique de l'économie numérique :

a) de tenir lieu de forum pour :

   i. l'échange d'informations sur la sécurité numérique des activités critiques afin d'identifier les bonnes pratiques en coordination avec d'autres instances internationales, ainsi que pour

   ii. la réalisation de travaux analytiques à l'appui de la mise en œuvre de la Recommandation ;

b) d'assurer le suivi de la mise en œuvre de la présente Recommandation et d'en faire rapport au Conseil dans les cinq ans suivant son adoption, puis au moins tous les dix ans.

Documents associés

NOTE EXPLICATIVE[1]

Les technologies numériques stimulent l'innovation et la productivité, et améliorent l'efficacité des produits et des services, entre autres avantages. Leur diffusion à l'échelle des chaînes de valeur et d'approvisionnement et leur intégration aux appareils physiques industriels et grand public, ainsi qu'à tous les stades de la prestation de services, sont telles que **la plupart des activités économiques et sociales sont aujourd'hui dépendantes du numérique**.

Parmi ces activités, certaines revêtent un caractère critique car leur interruption ou leur perturbation pourrait avoir des répercussions majeures sur la santé, la sûreté et la sécurité des citoyens, sur le fonctionnement efficace des services essentiels à l'économie et à la société, ainsi que celui des administrations ; ou, plus largement, sur la prospérité économique et sociale. Au nombre de ces activités critiques figurent par exemple la distribution d'énergie, l'offre de soins de santé et la prestation de services bancaires clés. À cela s'ajoutent les activités des grandes sociétés ou chaînes de valeur dont dépend une part non négligeable du PIB des pays, sans être nécessairement indispensables au fonctionnement de l'économie.

La **dépendance des activités critiques à l'égard du numérique date de plusieurs décennies** et s'est progressivement accentuée, à mesure que les opérateurs publics et privés se sont tournés vers les technologies numériques pour automatiser leurs processus opérationnels. Cette évolution a franchi une première étape après le passage au nouveau millénaire, avec l'adoption généralisée des technologies de l'internet, lorsque les systèmes et les réseaux d'information jusque-là isolés et fermés sont devenus interconnectés à l'échelle mondiale et ouverts par défaut. Si l'ouverture et la connectivité numérique ont décuplé les avantages liés à l'utilisation des technologies numériques, elles ont également exposé les activités critiques à de nouvelles menaces. Les incidents de sécurité numérique sont alors devenus pour les activités critiques une nouvelle source potentielle de catastrophes aux niveaux national, régional et international.

Au cours des dix dernières années, la dépendance des activités critiques à l'égard du numérique a continué d'augmenter. Dans les environnements industriels, les technologies opérationnelles et les systèmes de contrôle industriel (SCI) détectant ou entraînant des modifications des processus physiques ne sont désormais plus isolés des technologies de l'information. La transformation numérique accélère encore davantage la dépendance des activités critiques à l'égard du numérique, sous l'effet de la généralisation des données massives, de l'intelligence artificielle, de l'internet des objets et d'autres technologies à l'appui de villes, de réseaux électriques et de systèmes de santé « plus intelligents ». Les opérateurs d'activités critiques gèrent des volumes de plus en plus colossaux de données, de matériel, de logiciels et d'infrastructures réseau qu'il est impossible de sécuriser entièrement. Ces écosystèmes numériques complexes et dynamiques augmentent la surface d'attaque des opérateurs et leur exposition aux menaces de sécurité numérique.

Parallèlement, **les menaces numériques ont progressé à la fois en nombre et en sophistication.** Si l'on manque de données quantitatives robustes dans ce domaine, les données qualitatives empiriques sont claires. Les acteurs malveillants font preuve d'une inventivité croissante et ont accès à des outils plus perfectionnés qu'il y a dix ans. Qui plus est, les tensions géopolitiques s'étendent à l'environnement numérique, de sorte qu'aujourd'hui les États viennent grossir la liste des sources potentielles de menaces sur la sécurité numérique. Les chercheurs en sécurité détectent sans cesse de nouveaux programmes malveillants (*malware*) sophistiqués spécialement conçus pour cibler des activités critiques, tels Havex, DragonFly, Black Energy, Grey Energy, Triton ou encore

[1] Cette note explicative a été préparée par le Secrétariat. Les opinions exprimées et les arguments employées dans cette note explicative ne reflètent pas nécessairement les vues officielles des Membres de l'OCDE.

Industroyer[2], pour ne citer que quelques exemples. Le risque que des incidents de sécurité numérique occasionnent des dommages physiques est désormais bien réel : en témoignent le virus Stuxnet, découvert en 2010, qui a détruit des centrifugeuses de centrales nucléaires en Iran, ou les attaques qui ont causé des dégâts matériels considérables dans une aciérie allemande en 2014[3], ou des pannes d'électricité en Ukraine en 2015 et 2017. Sans compter l'attaque par le virus NotPetya, en 2017, qui a prouvé que des incidents de sécurité numérique pouvaient fortement perturber les opérations et les chaînes logistiques pendant plusieurs jours dans des domaines comme la logistique mondiale de conteneurs (Maersk) et la production pharmaceutique (Merck)[4].

Les effets conjugués de cette dépendance croissante à l'égard du numérique et des menaces accrues qui pèsent sur les activités critiques mettent les gouvernements au défi d'adopter des **politiques renforçant la sécurité numérique des activités critiques sans compromettre les avantages** de la transformation numérique dans les secteurs vitaux en imposant des contraintes susceptibles de restreindre inutilement l'utilisation et l'ouverture des technologies numériques.

En 2008, l'OCDE a adopté le premier instrument juridique international sur cette question : la *Recommandation sur la protection des infrastructures d'information critiques* (« Recommandation PIIC ») [OECD/LEGAL/0361]. Elle complétait la *Recommandation de l'OCDE de 2002 concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information* (« Lignes directrices sur la sécurité ») [OECD/LEGAL/0312] qui a été remplacée en 2015 par la *Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale* (« Recommandation sur le risque de sécurité numérique ») [OECD/LEGAL/0415].

La *Recommandation sur la sécurité numérique des activités critiques* (« la Recommandation ») actualise et **remplace la Recommandation PIIC de 2008**. Elle a été élaborée dans le but de : *i)* moderniser les concepts fondamentaux afin d'assurer la cohérence avec la Recommandation de 2015 sur le risque de sécurité numérique ; *ii)* clarifier le champ de ce domaine d'action, notamment sa place dans le paysage plus large des politiques en matière de sécurité numérique et des politiques de gestion nationale du risque ou de protection des infrastructures critiques[5] ; et *iii)* tenir compte des évolutions intervenues depuis 2008, ainsi que de l'expérience acquise par les pays quant à la mise en œuvre des politiques dans ce domaine.

Champ d'application

La Recommandation fournit des orientations sur les modalités de mise en œuvre de la Recommandation de 2015 sur le risque de sécurité numérique en vue d'assurer la continuité, la résilience et la sécurité des activités critiques sans compromettre les avantages de la transformation numérique. Elle précise en outre la place qu'occupe ce domaine d'action publique dans le paysage plus large des politiques de gestion nationale du risque ou de protection des infrastructures critiques.

Le champ d'application de la Recommandation marque une évolution des « infrastructures d'information critiques » (ou IIC) vers les « activités critiques ». La notion d'infrastructure d'information critique était fondée sur le concept, à l'époque relativement récent, d'infrastructure critique, expression utilisée depuis la fin des années 90 par les gouvernements pour désigner les actifs essentiels au fonctionnement d'une société et d'une économie. Les politiques en matière de protection des infrastructures critiques considèrent généralement l'énergie, la finance ou la santé publique comme des

2 www.techrepublic.com/article/how-the-triton-malware-shut-down-critical-infrastructure-in-the-middle-east/ et www.welivesecurity.com/fr/2017/06/15/industroyer-plus-grande-menace/.

3 www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/ et ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

4 www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ et www.fiercepharma.com/manufacturing/merck-has-hardened-its-defenses-against-cyber-attacks-like-one-last-year-cost-it.

5 Les pays n'ont pas tous la même approche de la protection des activités critiques ; on retrouve souvent des appellations de type « politique de protection des infrastructures critiques » ou « politique nationale de gestion du risque ».

secteurs d'infrastructures critiques. En 2008, l'un des principaux objectifs était de sensibiliser à la nécessité d'élaborer des politiques en vue de protéger les systèmes et réseaux d'information qui sous-tendent ces secteurs d'infrastructures critiques. Il avait alors semblé naturel de qualifier ces actifs TIC d'« infrastructure d'information critique », comme s'il s'agissait d'un secteur d'infrastructure critique supplémentaire. La Recommandation PIIC de 2008 a parfaitement rempli cette mission.

Toutefois, l'examen de la Recommandation de 2008 PIIC lancé en 2016 a montré que, bien qu'elle soit utile au niveau international et reconnue par les experts compétents, la notion d'infrastructure d'information critique a rarement été utilisée pour l'élaboration de cadres d'action nationaux. Cela pourrait s'expliquer par la difficulté à délimiter les infrastructures d'information critiques dans la pratique. Par exemple, l'internet peut être considéré comme faisant partie des IIC, puisque la plupart des opérateurs d'autres infrastructures critiques (banques, hôpitaux, distributeurs d'énergie, etc.) en dépendent. Or ces opérateurs dépendent également de leurs propres systèmes et réseaux d'information internes, qui font par conséquent aussi partie des IIC. Ces systèmes et réseaux d'information peuvent tantôt être détenus et gérés par les opérateurs des infrastructures critiques eux-mêmes, tantôt intégrer des composantes résidant « dans le nuage », à savoir sur l'internet, composantes alors détenues et gérées par des tierces parties, parfois dans d'autres pays et territoires. Cette combinaison de composantes techniques partagées et isolées, internes et externes, rend l'infrastructure d'information critique difficile à représenter et plus complexe que les secteurs d'« infrastructure critique » plus traditionnels dont s'inspirait la notion d'IIC.

Qui plus est, la notion d'IIC donne la fausse impression que la protection de ce type d'infrastructure est séparée de la protection des infrastructures critiques. Surtout, elle ne correspond plus à l'approche de l'OCDE en matière de sécurité numérique, qui a évolué de la sécurité des actifs techniques (à savoir des systèmes et réseaux d'information) vers la sécurité des activités économiques et sociales qui en dépendent (à savoir la fourniture d'énergie ou la prestation des services médicaux d'urgence, par exemple). Cette évolution a été l'une des principales nouveautés de la Recommandation de 2015 sur le risque de sécurité numérique, qui a remplacé les Lignes directrices de 2002 sur la sécurité. Le passage des IIC aux activités critiques permet donc de rétablir la cohérence entre les orientations de l'OCDE dans ce domaine et la Recommandation de 2015 sur le risque de sécurité numérique.

On entend par « activités critiques » les activités économiques et sociales dont l'interruption ou la perturbation aurait des conséquences graves sur la santé, la sûreté et la sécurité des citoyens ; sur le fonctionnement efficace des services essentiels à l'économie et à la société, ainsi que sur celui des pouvoirs publics ; ou, plus largement, sur la prospérité économique et sociale. Ce dernier type d'activité critique marque une évolution importante par rapport à la notion d'IIC telle qu'appréhendée en 2008. De fait, il couvre les activités économiques et sociales qui sont essentielles à la prospérité sans nécessairement jouer un rôle critique dans le fonctionnement de l'économie et de la société ni nuire à la santé, la sûreté ou la sécurité des citoyens. Tel est le cas par exemple de la production automobile ou de l'exploitation minière dans les pays où ces activités représentent une part importante du PIB.

Terminologie

La Recommandation fournit un cadre sémantique cohérent afin d'aider à comprendre comment aborder la sécurité numérique des activités critiques. L'usage de cette terminologie dans les politiques nationales pourrait faciliter la coopération internationale. La Recommandation reconnaît toutefois que les Adhérents peuvent employer des termes différents dans les politiques qu'ils mettent en place pour renforcer la sécurité numérique des activités critiques. On observe en effet que les termes utilisés par les pays dans ce domaine sont souvent hérités des cadres plus larges de gestion nationale du risque ou de protection des infrastructures critiques, qui couvrent l'ensemble des risques qui pèsent sur les activités critiques. Certains pays préfèrent par exemple à « activité » le terme « fonction », et à « critique » l'adjectif « vital » ou « essentiel ». Préconiser l'utilisation de la terminologie proposée dans la Recommandation pourrait dans ce cas nuire à la cohérence entre, d'un côté, les politiques nationales visant à renforcer la sécurité numérique des activités critiques et, de l'autre, les cadres nationaux de gestion du risque ou de protection des infrastructures critiques. Ce qui pourrait être source de confusion et contrevenir à l'objectif même de la Recommandation, qui est de renforcer la cohérence entre ces domaines d'action étroitement corrélés. De même, il se peut que le champ des « activités critiques »

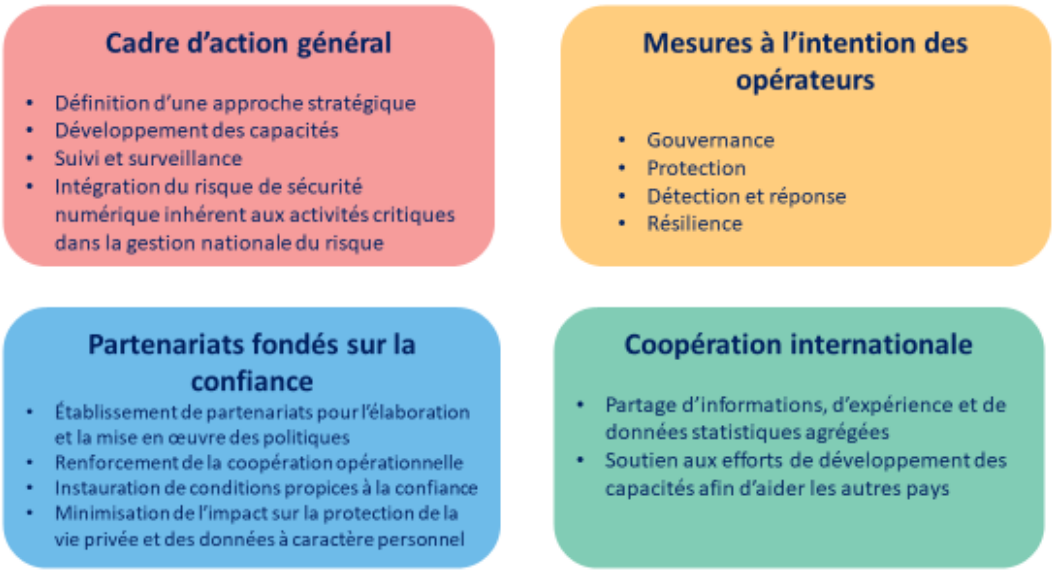
défini dans les politiques nationales soit hérité d'un cadre plus large de gestion nationale du risque ou de protection des infrastructures critiques et formulé différemment de celui exposé dans la Recommandation. Il peut en effet y être plus large ou plus restreint, inclure des références à la sécurité nationale et être utilisé à des fins autres que la sécurité numérique[6].

Conformément à la Recommandation de 2015 sur le risque de sécurité numérique, la Recommandation privilégie l'expression « sécurité numérique » à celle de « cybersécurité » afin de souligner le fait que la sécurité numérique est un enjeu de gestion du risque économique et social et d'assurer la cohérence avec d'autres expressions comme les technologies numériques, l'économie numérique et la transformation numérique.

Principes fondamentaux

La Recommandation fournit des orientations sur le cadre d'action général en faveur du renforcement de la sécurité numérique des activités critiques, les mesures que les pouvoirs publics pourraient encourager les opérateurs à prendre, la constitution de partenariats et le resserrement de la coopération internationale (voir Graphique 1).

Graphique 1. Principes fondamentaux du projet de Recommandation sur la sécurité numérique des activités critiques



Source : OCDE

Le **cadre d'action général** devrait puiser ses racines à la fois dans une stratégie nationale de sécurité numérique et dans une évaluation nationale du risque, et intégrer un mécanisme de gouvernance national. La coordination à l'échelle nationale s'avère particulièrement importante pour assurer la cohérence entre les politiques en matière de sécurité numérique et les réglementations existantes dans les secteurs critiques (de l'énergie au secteur bancaire, en passant par la santé). Au titre de ce cadre général, les pouvoirs publics devraient développer les capacités à l'appui de la gestion du risque de sécurité numérique et de la résilience des activités critiques. Cela passera notamment par la mise en place ou le renforcement des capacités de réponse aux incidents, en mettant sur pied une

6 Par exemple, aux États-Unis, les « activités critiques » sont actuellement dénommées « fonctions critiques » et désignent « les fonctions de l'administration et du secteur privé si essentielles aux États-Unis que toute perturbation, toute corruption ou tout dysfonctionnement aurait un effet préjudiciable sur la sécurité, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou une quelconque combinaison de ces éléments » (traduction libre), *Executive Order on Coordinating National Resilience to Electromagnetic Pulses*, 26 mars 2019, www.whitehouse.gov/presidential-actions/executive-order-coordinating-national-resilience-electromagnetic-pulses/. Voir également www.dhs.gov/cisa/national-critical-functions.

équipe de réponse aux incidents de sécurité informatique (CSIRT ou CERT) ou un centre d'opérations de sécurité (SOC), ou plusieurs dispositifs de ce type opérant par exemple à l'échelle sectorielle. Il s'agira en outre de renforcer la sécurité des services numériques critiques des administrations, en promouvant l'adoption de normes internationales (y compris de normes régionales, à l'instar de celles mises en œuvre au niveau de l'Union européenne), et de soutenir les opérateurs en tant que de besoin.

Les opérateurs devraient quant à eux être responsables de la gestion du risque de sécurité numérique inhérent aux activités critiques qu'ils exploitent.

Un **processus en entonnoir**, fondé sur une évaluation nationale du risque menée au titre du cadre de protection des infrastructures critiques ou de gestion nationale du risque, permet de faire en sorte que les politiques visant les opérateurs d'activités critiques soient centrées sur les composantes vitales pour l'économie et la société, sans imposer de contraintes indues sur le reste.

Ce processus devrait être mis en œuvre comme suit. Sur la base d'une évaluation nationale du risque couvrant l'ensemble des activités économiques et sociales :

- Les pouvoirs publics, en coopération avec les acteurs concernés des secteurs public et privé, identifient :
    1. Les *activités critiques* ;
    2. Les *opérateurs* de ces activités critiques ;
- Les opérateurs d'activités critiques :
    3. Assurent une gestion cyclique du risque d'entreprise en vue de repérer les fonctions sans lesquelles ils ne pourraient mener à bien efficacement leurs activités critiques (« *fonctions critiques* ») ;
    4. Cartographient l'« *écosystème numérique* », à savoir l'environnement numérique qui sous-tend leurs fonctions critiques tout au long de la chaîne de valeur des activités critiques ;
    5. Réalisent des *évaluations du risque de sécurité numérique inhérent aux fonctions critiques*, sur une base cyclique, en tenant compte de leur écosystème numérique, et en déduisent le niveau du risque de sécurité numérique à réduire, transférer, éviter et accepter (« *traitement du risque* »), ainsi que les mesures de gouvernance de la sécurité numérique et celles visant à protéger les activités, détecter les incidents et y répondre, et mettre en place la résilience.

Les trois premières étapes de ce processus, qui font partie d'un cadre d'action plus large de gestion nationale du risque ou de protection des infrastructures critiques, ne sont pas couvertes par la Recommandation, centrée sur la sécurité numérique. Il importe toutefois de les mentionner afin de s'assurer que les étapes quatre et cinq soient alignées sur l'évaluation nationale du risque et ne représentent pas pour les opérateurs une charge inutile.

Considérer une activité comme critique aux termes de la Recommandation créera des contraintes supplémentaires pour les opérateurs et pourrait peser sur leur compétitivité sur le marché mondial. C'est pourquoi il n'est pas rare que les pouvoirs publics coopèrent avec ces opérateurs et les autres parties prenantes dans le cadre de la première et de la deuxième étape, et, plus généralement, du processus d'élaboration des politiques, afin d'équilibrer au mieux les progrès en matière de sécurité numérique et les résultats économiques et sociaux.

La quatrième étape introduit la notion d'« écosystème numérique », qui couvre un champ plus large que celui des systèmes et réseaux d'information considéré dans la Recommandation PIIC de 2008, puisqu'il s'étend aux actifs numériques comme le matériel, les logiciels, les réseaux et les données, aux technologies opérationnelles qui détectent ou entraînent des modifications des processus physiques, ainsi qu'aux entités, personnes et processus internes et externes qui les conçoivent, les exploitent et en assurent la maintenance, et aux relations qu'ils entretiennent. La quatrième étape est

un prérequis à la cinquième, au cours de laquelle les opérateurs gèrent le risque de sécurité numérique conformément aux préconisations énoncées dans la Recommandation de 2015 sur le risque de sécurité numérique, à savoir au titre du cadre plus large de gestion du risque d'entreprise et des processus généraux de prise de décisions économiques et sociales (voir Graphique 2). La Recommandation fournit toutefois des orientations plus détaillées sur les mesures de gouvernance, de protection, de détection et réponse, et de résilience qu'ils devraient mettre en place – une catégorisation cohérente avec à la fois le cadre de cybersécurité (*Cybersecurity Framework*) du *National Institute of Standards and Technologies* (NIST), aux États-Unis, et le *Reference Document on Security Measures for Operators of Essential Services* du Groupe de coordination chargé de la Sécurité des réseaux et de l'information (NIS) de l'UE.

Graphique 2. Processus en entonnoir à suivre pour centrer le renforcement de la sécurité numérique des activités critiques

Source : OCDE

La Recommandation reconnaît que la multiplicité et la complexité des dépendances à l'égard du numérique par-delà les frontières sectorielles et géographiques et tout au long des chaînes de valeur des activités critiques génèrent un risque de sécurité numérique partagé qui ne saurait être réduit sensiblement, dans l'intérêt de tous, par un seul et unique acteur. Chaque acteur est donc à la fois dépendant de tous les autres acteurs et responsable envers eux pour ce qui est de la gestion du risque de sécurité numérique. Pour garantir que la gestion du risque de sécurité numérique inhérent aux activités critiques tienne dûment compte de ces dépendances, la Recommandation préconise d'instaurer des **partenariats public-public, public-privé et privé-privé** durables qui transcendent les secteurs et les pays, aux termes desquels les partenaires partageraient les informations sur les risques, de même que l'expérience et les bonnes pratiques de gestion du risque de sécurité numérique.

Compte tenu du caractère sensible des informations à échanger, ces **partenariats doivent être fondés sur la confiance**. La Recommandation propose une liste générale de conditions propices pour instaurer la confiance dans l'optique de l'établissement de tels partenariats durables public-public, public-privé et privé-privé, parmi lesquelles la nécessité de définir des objectifs, des valeurs et des règles clairs, la recherche d'avantages mutuels au fil du temps, ou encore le respect des réglementations en matière de protection de la vie privée et des données à caractère personnel, ainsi que d'autres réglementations protégeant la confidentialité des informations telles que les secrets

commerciaux. En particulier, il importe que les acteurs concernés veillent à ce que les informations qu'ils reçoivent des autres partenaires soient utilisées exclusivement à des fins préventives et gérées dans le respect des réglementations régissant la protection des données à caractère personnel et des autres informations de type secrets commerciaux. Il pourrait être nécessaire d'ajouter des conditions supplémentaires, dont certaines seraient propres aux types de partenariats considérés (public-public, public-privé, privé-privé).

Enfin, la Recommandation encourage les Adhérents à renforcer la **coopération internationale** en partageant des informations sur les organismes publics et d'autres parties prenantes chargées de la gestion du risque de sécurité numérique inhérent aux activités critiques, des expériences en matière d'élaboration des politiques, et des données statistiques agrégées sur les incidents, ainsi qu'en appuyant les efforts de développement des capacités des autres pays en tant que de besoin.

À propos de l'OCDE

L'OCDE est un forum unique en son genre où les gouvernements œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux que pose la mondialisation. L'OCDE est aussi à l'avant- garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays Membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, le Chili, la Colombie, la Corée, le Costa Rica, le Danemark, l'Espagne, l'Estonie, les États Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, Israël, l'Italie, le Japon, la Lettonie, la Lituanie, le Luxembourg, le Mexique, la Norvège, la Nouvelle Zélande, les Pays Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Slovénie, la Suède, la Suisse et la Türkiye. L'Union européenne participe aux travaux de l'OCDE.

Instruments juridiques de l'OCDE

Environ 460 instruments juridiques de substance ont été développés dans le cadre de l'OCDE depuis sa création en 1961. Ces instruments comprennent les Actes de l'OCDE (les Décisions et Recommandations adoptées par le Conseil de l'OCDE conformément à la Convention relative à l'OCDE) et d'autres instruments juridiques développés dans le cadre de l'OCDE (notamment les Déclarations et les accords internationaux).

L'ensemble des instruments juridiques de substance de l'OCDE, qu'ils soient en vigueur ou abrogés, est répertorié dans le Recueil des instruments juridiques de l'OCDE. Ils sont présentés selon cinq catégories :

- Les **Décisions** sont adoptées par le Conseil et sont juridiquement contraignantes pour tous les Membres, à l'exception de ceux qui se sont abstenus au moment de leur adoption. Elles définissent des droits et des obligations spécifiques et peuvent prévoir des mécanismes de suivi de la mise en œuvre**.**
- Les **Recommandations** sont adoptées par le Conseil et n'ont pas une portée juridique obligatoire. Elles représentent un engagement politique vis-à-vis des principes qu'elles contiennent, il est attendu que les Adhérents feront tout leur possible pour les mettre en œuvre.
- Les **Documents finaux de substance** sont adoptés individuellement par les Adhérents indiqués plutôt que par un organe de l'OCDE et sont le résultat d'une réunion ministérielle, à haut niveau ou autre, tenue dans le cadre de de l'Organisation. Ils énoncent habituellement des principes généraux ou des objectifs à long terme et ont un caractère solennel.
- Les **accords internationaux** sont négociés et conclus dans le cadre de l'Organisation. Ils sont juridiquement contraignants pour les parties.
- **Arrangement, accord/arrangement et autres** : plusieurs autres types d'instruments juridiques de substance ont été développés dans le cadre de l'OCDE au fil du temps, comme l'Arrangement sur les crédits à l'exportation bénéficiant d'un soutien public, l'Arrangement international sur les Principes à suivre dans les transports maritimes et les Recommandations du Comité d'aide au développement (CAD).