La gestion du risque de sécurité numérique pour la prospérité économique et sociale

RECOMMENDATION DE L'OCDE ET DOCUMENT D'ACCOMPAGNEMENT

OCDE

Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale

Recommandation de l'OCDE et
Document d'accompagnement

OCDE
DES POLITIQUES MEILLEURES
POUR UNE VIE MEILLEURE

AVERTISSEMENT

Ce document et toute carte 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.

Merci de citer cet ouvrage comme suit :
OCDE (2015), *Gestion du risque de sécurité numérique pour la prospérité économique et sociale : Recommandation de l'OCDE et Document d'accompagnement*, Éditions OCDE, Paris.
DOI: http://dx.doi.org/10.1787/9789264246089-fr

Crédit photo :
Couverture – © Seqoya, Fotolia.com, page 19 – © Nikiforov Alexander, Shutterstock.com

Les corrigenda des publications de l'OCDE sont disponibles sur :
www.oecd.org/publishing/corrigenda.

Avant-propos

La présente *Recommandation de l'OCDE sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale* et son Document d'accompagnement posent des jalons pour l'émergence d'une nouvelle génération de stratégies nationales de gestion de ce risque, axées sur l'optimisation des retombées économiques et sociales que l'on peut attendre d'un environnement numérique ouvert.

Les menaces et incidents de sécurité numérique se font plus nombreux depuis quelques années, avec des conséquences économiques et sociales significatives pour les organisations publiques et privées ainsi que pour les individus : interruption d'activité (par exemple suite à une attaque par déni de service ou à un sabotage), pertes financières directes, actions en justice, atteinte à la notoriété, perte de compétitivité (en cas de violation d'un secret commercial, par exemple), ou encore perte de confiance des clients, pour n'en citer que quelques-unes. Les parties prenantes prennent de plus en plus conscience qu'il est nécessaire de mieux gérer le risque de sécurité numérique pour recueillir les fruits de l'économie numérique.

Depuis trois décennies, l'OCDE joue un rôle important de promotion des politiques et des instruments au service de l'innovation et de la confiance dans l'économie numérique. L'adoption de la présente Recommandation par le Conseil de l'OCDE, le 19 septembre 2015, est le couronnement d'un processus multipartite engagé en 2012 par le Groupe de travail de l'OCDE sur la sécurité et la vie privée dans l'économie numérique (GTSVPEN) en vue de réviser la *Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité* (« Lignes directrices sur la sécurité »), qui remonte à 2002.

Ce processus de révision, auquel étaient associés des représentants des pouvoirs publics, des entreprises, de la société civile et de la communauté technique de l'internet, a été conduit par Jane Hamilton (Canada), Présidente du GTSVPEN, qui a pu compter sur le soutien des autres membres du Bureau. Les délégations des pays membres de l'OCDE et des économies partenaires, ainsi que le Comité consultatif économique et industriel (BIAC), le Comité consultatif de la société

civile sur la société de l'information (CSISAC) et le Comité consultatif technique sur l'internet (ITAC) ont eux aussi pris une part active aux travaux. Le projet de Recommandation révisée a été examiné et approuvé par le Comité de la politique de l'économie numérique le 25 juin 2015 avant son adoption finale par le Conseil de l'OCDE.

Dans la Recommandation, l'OCDE appelle les décideurs au plus haut niveau du gouvernement et des organisations publiques et privées à adopter une approche de la gestion du risque de sécurité numérique de nature à instaurer la confiance et tirer parti de l'environnement numérique ouvert afin d'assurer la prospérité économique et sociale. Cette approche prend la forme d'un cadre cohérent fait de huit principes étroitement liés, interdépendants et complémentaires. Deux messages clés constituent le fil conducteur de la Recommandation.

Il s'agit premièrement de l'accent mis sur les objectifs économiques et sociaux des organisations publiques et privées et la nécessité d'adopter une approche fondée sur la gestion du risque de sécurité. Plutôt que d'être considéré comme un problème technique qui requiert des solutions de même nature, le risque numérique devrait être traité comme un risque économique et donc faire partie intégrante des cadres généraux de gestion du risque et de prise de décision en place dans les organisations. Il faut combattre l'idée selon laquelle le risque de sécurité numérique appelle une réponse de nature fondamentalement différente par rapport aux autres catégories de risque. C'est la raison pour laquelle ni le terme « cybersécurité » ni, de manière plus générale, le préfixe « cyber », qui ont contribué à répandre cette fausse idée de spécificité, ne sont employés dans la Recommandation de 2015.

En second lieu, Il est considéré qu'une gestion dynamique du risque de sécurité numérique permet de ramener celui-ci à un niveau acceptable au regard des avantages économiques attendus des activités en jeu. À cet égard, il convient que les mesures de sécurité numérique soient conçues de telle manière qu'elles tiennent compte des intérêts d'autrui, soient adaptées et proportionnées aux risques courus et ne nuisent pas à l'activité économique et sociale qu'elles sont censées protéger.

En plus du texte de la Recommandation, on trouvera dans la présente brochure un Document d'accompagnement, qui est de nature explicative et illustrative

et ne fait pas partie de la Recommandation, quand bien même l'un et l'autre ont été élaborés en lien étroit. Le document développe les concepts clés de la Recommandation, examine l'applicabilité pour les parties prenantes des huit principes qui y sont énoncés puis explique chacun de ces principes.

Il est attendu de la mise en œuvre de la Recommandation qu'elle favorise l'adoption d'une approche plus holistique de la gestion du risque de sécurité numérique et l'instauration de nouveaux mécanismes de coordination, tant au sein du gouvernement qu'avec les acteurs non gouvernementaux, et qu'elle renforce la coopération public-privé aux niveaux national, régional et international.

Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale

17 septembre 2015 – C(2015)115

LE CONSEIL,

CONSIDÉRANT la Convention relative à l'Organisation de coopération et de développement économiques en date du 14 décembre 1960, notamment ses articles 1 b), 1 c), 3 a), 3 b) et 5 b) ;

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 (« Lignes directrices de l'OCDE sur la vie privée ») [C(80)58/FINAL, telle qu'amendée] ; la Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie [C(97)62/FINAL] ; la Recommandation du Conseil sur la protection des infrastructures d'information critiques [C(2008)35] ; la Déclaration sur le futur de l'économie Internet (la Déclaration de Séoul) [C(2008)99] ; la Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet [C(2011)154] ; la Recommandation du Conseil concernant la politique et la gouvernance réglementaires [C(2012)37] ; la Recommandation du Conseil sur les stratégies numériques gouvernementales [C(2014)88] ; et la Recommandation du Conseil sur la gouvernance des risques majeurs [C/MIN(2014)8/FINAL] ;

CONSIDÉRANT la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité [C(2002)131/FINAL], que la présente Recommandation remplace ;

RECONNAISSANT que l'environnement numérique, notamment l'Internet, est essentiel au fonctionnement de nos économies et de nos sociétés et qu'il stimule la croissance, l'innovation, le bien-être et l'inclusivité ;

RECONNAISSANT que les bienfaits qu'apporte l'environnement numérique, qui s'étendent à tous les secteurs de l'économie et à tous les aspects du progrès social, tiennent à la nature mondiale, ouverte, interconnectée et dynamique des technologies et de l'infrastructure de l'information et des communications, en particulier de l'Internet ;

RECONNAISSANT que l'utilisation, la gestion et le développement de l'environnement numérique sont soumis à des incertitudes qui sont dynamiques par nature ;

RECONNAISSANT que la gestion du risque de sécurité numérique relève d'une approche souple et réactive destinée à traiter ces incertitudes et tirer pleinement parti des bienfaits économiques et sociaux attendus, fournir les services essentiels et exploiter les infrastructures critiques, préserver les droits de l'homme et les valeurs fondamentales, et protéger les individus contre les menaces de sécurité numérique ;

SOULIGNANT que la gestion du risque de sécurité numérique fournit une base solide pour la mise en œuvre du « Principe des garanties de sécurité » énoncé dans les Lignes directrices de l'OCDE sur la vie privée et, plus généralement, que la présente Recommandation et lesdites Lignes directrices se renforcent mutuellement ;

CONSCIENT que les gouvernements, les organisations publiques et privées, ainsi que les individus partagent la responsabilité, selon leurs rôles respectifs et le contexte, de la gestion du risque de sécurité et de la protection de l'environnement numérique ; et que la coopération est essentielle aux niveaux national, régional et international.

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

I. RECOMMANDE que les Membres et les non-Membres qui adhèrent à la présente Recommandation (ci-après les « Adhérents ») :

1. Mettent en pratique les principes énoncés dans la section 1 (ci-après les « Principes ») à tous les niveaux du gouvernement et au sein des organisations publiques ;

2. Adoptent une stratégie nationale pour la gestion du risque de sécurité numérique telle que décrite dans la section 2 ;

II. APPELLE les décideurs au plus haut niveau du gouvernement et des organisations publiques et privées à adopter une approche de la gestion du risque de sécurité numérique pour susciter la confiance et tirer parti de l'environnement numérique ouvert afin d'assurer la prospérité économique et sociale ;

III. ENCOURAGE les organisations privées à intégrer les Principes à leur approche de la gestion du risque de sécurité numérique ;

IV. ENCOURAGE l'ensemble des parties prenantes à mettre en œuvre les Principes dans le cadre de leurs processus décisionnels, selon leurs rôles, leur capacité à agir et le contexte ;

V. APPELLE les gouvernements et les organisations publiques et privées à travailler de concert pour permettre aux individus et aux petites et moyennes entreprises de gérer de manière collaborative le risque de sécurité numérique ;

VI. CONVIENT que les Principes sont complémentaires et doivent être pris comme un tout, et qu'ils ont vocation à être en adéquation avec les processus, les bonnes pratiques, les méthodologies et les normes en matière de gestion du risque ;

VII. CONVIENT en outre qu'aux fins de la présente Recommandation :

1. Le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Le terme « risque de sécurité numérique » désigne une catégorie de risque liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit. Ce risque peut résulter d'une combinaison de menaces et de vulnérabilités inhérentes à l'environnement numérique. Il peut compromettre la réalisation des objectifs économiques et sociaux en portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des activités et/ou de l'environnement. Dynamique par nature, le risque de sécurité numérique se compose d'éléments liés à l'environnement numérique, à l'environnement physique, aux personnes impliquées dans l'activité et aux processus organisationnels qui la structurent.
2. La « gestion du risque de sécurité numérique » est l'ensemble des mesures coordonnées, intra et/ou interorganisations, prises pour maîtriser le risque de sécurité numérique tout en maximisant les opportunités. Elle fait partie intégrante du processus décisionnel et s'inscrit dans un cadre global de gestion du risque qui pèse sur les activités économiques et sociales. Elle s'appuie sur un ensemble holistique, systématique et flexible de processus cycliques, aussi transparent et explicite que possible. Cet ensemble de processus contribue à la mise en œuvre de mesures de gestion du risque de sécurité numérique (« mesures de sécurité ») adaptées et proportionnées au risque et aux objectifs économiques et sociaux en jeu.

3. Les « parties prenantes » sont les gouvernements, les organisations publiques et privées et les individus qui dépendent de l'environnement numérique pour tout ou partie de leurs activités économiques et sociales. Elles peuvent endosser plusieurs rôles. « Les dirigeants et les décideurs » sont les acteurs opérant au plus haut niveau au sein du gouvernement et des organisations publiques et privées.

SECTION 1. PRINCIPES

Principes généraux

1. *Sensibilisation, compétences et autonomisation*

Toutes les parties prenantes devraient comprendre le risque de sécurité numérique et les moyens de le gérer.

Elles devraient être conscientes que le risque de sécurité numérique peut compromettre la réalisation de leurs objectifs économiques et sociaux, et que la gestion de ce risque peut avoir des incidences sur autrui. Elles devraient bénéficier de l'éducation et des compétences nécessaires pour comprendre ce risque, pour aider à le maîtriser et pour évaluer l'impact que pourraient avoir leurs décisions en matière de gestion du risque de sécurité numérique, tant sur leurs activités que sur l'ensemble de l'environnement numérique.

2. *Responsabilité*

Toutes les parties prenantes devraient assumer la responsabilité de la gestion du risque de sécurité numérique.

Elles devraient faire preuve de responsabilité et être en mesure de répondre, selon leurs rôles, le contexte et leur capacité à agir, de la gestion du risque de sécurité numérique et de la prise en compte de l'impact potentiel de leurs décisions sur autrui. Elles devraient par ailleurs reconnaître qu'un certain niveau de risque de sécurité numérique doit être accepté pour atteindre les objectifs économiques et sociaux.

3. *Droits de l'homme et valeurs fondamentales*

Toutes les parties prenantes devraient gérer le risque de sécurité numérique de manière transparente, dans le respect des droits de l'homme et des valeurs fondamentales.

La gestion du risque de sécurité numérique devrait se faire dans le respect des droits de l'homme et des valeurs fondamentales reconnues par les sociétés

démocratiques, notamment la liberté d'expression, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection de la vie privée et des données à caractère personnel, l'ouverture et le droit à une procédure équitable. La gestion du risque de sécurité numérique devrait se fonder sur un comportement éthique qui respecte et reconnaisse les intérêts légitimes d'autrui et de la société dans son ensemble. Les organisations devraient se doter d'une politique générale de transparence quant à leurs pratiques et leurs procédures de gestion du risque de sécurité numérique.

4. *Coopération*

Toutes les parties prenantes devraient coopérer, y compris au-delà des frontières.

Le caractère mondialement interconnecté de l'environnement numérique se traduit par une interdépendance des parties prenantes et nécessite une coopération en matière de gestion du risque de sécurité. Cette coopération, qui est l'affaire de tous, doit se faire non seulement au sein des gouvernements et des organisations publiques et privées, mais aussi entre elles/eux, ainsi qu'avec les individus. En outre, elle devrait s'étendre au-delà des frontières, aux niveaux régional et international.

Principes opérationnels

5. *Cycle d'évaluation et de traitement du risque*

Les dirigeants et les décideurs devraient s'assurer que le traitement du risque de sécurité numérique est fondé sur une évaluation permanente du risque.

L'évaluation du risque de sécurité numérique devrait s'inscrire dans un processus systématique et cyclique permanent. Elle devrait estimer les conséquences que les menaces, conjuguées aux vulnérabilités, pourraient avoir sur les activités économiques et sociales en jeu, et éclairer le processus décisionnel afférent au traitement du risque. Ledit traitement devrait viser à réduire le risque à un niveau acceptable au regard des bienfaits économiques et sociaux que l'on attend de ces activités, tout en tenant compte des incidences potentielles sur les intérêts légitimes d'autrui. Le traitement du risque peut prendre plusieurs formes : accepter le risque, le réduire, le transférer, l'éviter, ou opter pour une combinaison de ces approches.

6. *Mesures de sécurité*

Les dirigeants et les décideurs devraient s'assurer que les mesures de sécurité sont appropriées et proportionnées au risque.

L'évaluation du risque de sécurité numérique devrait guider le choix, la mise en œuvre et l'amélioration des mesures de sécurité prises pour réduire le risque au niveau acceptable tel que défini lors de l'évaluation et du traitement de ce risque. Ces mesures devraient être appropriées et proportionnées au risque, et choisies en tenant compte des effets négatifs et positifs qu'elles pourraient avoir sur les activités économiques et sociales qu'elles visent à protéger, ainsi que sur les droits de l'homme et les valeurs fondamentales, et sur les intérêts légitimes d'autrui. Tous les types de mesures devraient être envisagés, que ces mesures soient physiques ou numériques, ou qu'elles s'appliquent aux personnes, aux processus ou aux technologies concernés par les activités. Les organisations devraient rechercher les vulnérabilités et y apporter une réponse appropriée dans les plus brefs délais.

7. *Innovation*

Les dirigeants et les décideurs devraient s'assurer que l'innovation est prise en considération.

L'innovation devrait faire partie intégrante de la réduction du risque de sécurité numérique au niveau acceptable fixé lors de l'évaluation et du traitement de ce risque. Elle devrait jouer un rôle à la fois dans la conception et la conduite des activités économiques et sociales qui dépendent de l'environnement numérique, et dans l'élaboration et la mise en place des mesures de sécurité.

8. *Préparation et continuité*

Les dirigeants et les décideurs devraient s'assurer de l'adoption d'un plan de préparation et de continuité.

À partir de l'évaluation du risque de sécurité numérique, un plan de préparation et de continuité devrait être adopté pour atténuer les effets préjudiciables des incidents de sécurité et favoriser la continuité et la résilience des activités économiques et sociales. Il devrait recenser les mesures permettant de prévenir les incidents de sécurité numérique, de les détecter, d'y répondre et d'assurer la reprise des activités. Il devrait en outre prévoir des mécanismes attribuant des niveaux d'escalade clairs en fonction de l'ampleur et de la gravité des effets

de ces incidents, ainsi que de leur potentiel de propagation aux autres acteurs de l'environnement numérique. Des procédures de notification appropriées devraient être envisagées dans le cadre de la mise en œuvre du plan.

SECTION 2. STRATÉGIES NATIONALES

A. Les stratégies nationales de gestion du risque de sécurité numérique devraient être cohérentes avec les Principes et créer les conditions nécessaires à la gestion, par l'ensemble des parties prenantes, du risque de sécurité numérique qui pèse sur les activités économiques et sociales, et à l'instauration d'un climat de confiance dans l'environnement numérique. Pour ce faire, elles devraient :

1. Bénéficier du soutien des plus hautes instances du gouvernement et définir une approche claire et intergouvernementale qui soit souple, neutre sur le plan technologique et cohérente avec les autres stratégies en faveur de la prospérité économique et sociale ;

2. Énoncer clairement qu'elles visent à : tirer parti de l'environnement numérique ouvert pour favoriser la prospérité économique et sociale, en réduisant le niveau général de risque de sécurité numérique à l'échelle nationale et internationale, sans imposer de restrictions superflues à la circulation des technologies, des communications et des données ; et garantir la fourniture des services essentiels et le fonctionnement des infrastructures critiques, protéger les individus contre les menaces de sécurité numérique sans perdre de vue la nécessité de préserver la sécurité nationale et internationale, et protéger les droits de l'homme et les valeurs fondamentales ;

3. S'adresser à toutes les parties prenantes, être adaptées, s'il y a lieu, aux petites et moyennes entreprises et aux individus, et énoncer la responsabilité des parties prenantes et leur obligation de rendre des comptes, selon leurs rôles, leur capacité à agir et le contexte dans lequel elles opèrent ;

4. Être le fruit d'une approche intragouvernementale coordonnée et d'un processus de consultation ouvert et transparent associant toutes les parties prenantes, être régulièrement révisées et améliorées à la lumière des expériences et des bonnes pratiques en utilisant, si possible, des mesures comparables à l'échelle internationale.

B. Les stratégies nationales devraient comprendre des mesures aux termes desquelles les gouvernements :

*1. **Donnent l'exemple,** et notamment :*

i) Adoptent un cadre complet pour gérer le risque de sécurité numérique qui pèse sur leurs propres activités. Ce cadre et les politiques de mise en œuvre devraient être transparents afin de susciter la confiance dans les activités et le comportement du gouvernement, y compris pour ce qui est de la divulgation responsable des vulnérabilités qu'ils ont détectées et des mesures d'atténuation des risques prises en conséquence ;

ii) Mettent en place des mécanismes de coordination associant tous les acteurs concernés au sein du gouvernement, afin de s'assurer que leur gestion du risque de sécurité numérique est compatible et concourt à faire progresser la prospérité économique et sociale ;

iii) S'assurent de la création, au niveau national, d'au moins une équipe de réponse aux incidents de sécurité informatique (CSIRT), également appelée équipe d'intervention en cas d'urgence informatique (CERT) et, s'il y a lieu, encourager l'émergence de CSIRT publiques et privées travaillant en collaboration, y compris avec celles d'autres pays ;

iv) Utilisent leur position sur le marché pour promouvoir la gestion du risque de sécurité numérique dans l'ensemble de l'économie et de la société, notamment au travers des politiques de passation de marchés publics et du recrutement de spécialistes possédant les qualifications nécessaires en matière de gestion du risque ;

v) Encouragent l'utilisation de normes et de bonnes pratiques internationales de gestion du risque de sécurité numérique et en favorisent le développement et l'examen par le biais de processus ouverts, transparents et multi-partites ;

vi) Adoptent des techniques de sécurité innovantes pour gérer le risque de sécurité numérique, afin de garantir une protection adéquate des informations stockées et en transit, en tenant compte de l'intérêt d'imposer des restrictions appropriées à la collecte et la conservation des données ;

vii) Coordonnent et promeuvent la recherche et le développement publics en matière de gestion du risque de sécurité numérique afin de stimuler l'innovation ;

viii) Favorisent le développement d'une main-d'œuvre qualifiée capable de gérer le risque de sécurité numérique, en particulier en intégrant cette discipline dans les stratégies globales sur les compétences. Pour ce faire, les pouvoirs publics pourraient miser sur la formation continue et la certification dans le domaine de la gestion du risque, et soutenir le développement des compétences numériques au sein de la population, par le biais des programmes nationaux d'éducation, notamment dans l'enseignement supérieur ;

ix) Adoptent et mettent en œuvre un cadre global de lutte contre la cybercriminalité, en s'appuyant sur les instruments internationaux existants ;

x) Allouent des ressources suffisantes pour une mise en œuvre efficace des stratégies.

2. Renforcent la coopération internationale et l'assistance mutuelle, *et notamment :*

i) Prennent part à des forums régionaux et internationaux dans le domaine, et nouent des relations bilatérales et multilatérales pour favoriser le partage d'expériences et de bonnes pratiques ; et promeuvent une approche de la gestion du risque de sécurité numérique à l'échelle nationale qui ne fasse pas peser un risque accru sur les autres pays ;

ii) Dispensent, à titre volontaire, assistance et soutien à d'autres pays qui en auraient besoin et établissent des points de contact nationaux pour que les demandes de pays étrangers liées aux questions de gestion du risque de sécurité numérique puissent être traitées en temps utile ;

iii) S'efforcent d'améliorer la réponse aux menaces d'origine nationale ou étrangère, par le biais, notamment, de la coopération entre les CSIRT, d'exercices coordonnés et d'autres instruments de collaboration.

3. Collaborent avec d'autres parties prenantes, *et notamment :*

i) Réfléchissent à la manière dont les gouvernements et les autres parties prenantes peuvent s'entraider afin de mieux gérer le risque de sécurité numérique pesant sur leurs activités ;

ii) Recensent et atténuent de possibles effets négatifs que les politiques menées par les pouvoirs publics pourraient avoir sur les activités des autres parties prenantes ou sur la prospérité économique et sociale du pays ;

iii) Établissent des pratiques et des procédures de gestion du risque de sécurité numérique et les font connaître publiquement ;

iv) Encouragent la détection, le signalement et/ou la correction des vulnérabilités de sécurité numérique par toutes les parties prenantes, dans un esprit de responsabilité ;

v) Renforcent la sensibilisation, les compétences et l'autonomisation à l'échelle de la société, afin de favoriser la gestion du risque de sécurité numérique au moyen d'initiatives neutres du point de vue technologique et adaptées aux besoins particuliers des différentes catégories de parties prenantes.

4. ***Créent les conditions propices à une collaboration de toutes les parties prenantes à la gestion du risque de sécurité numérique,*** *et notamment :*

i) Favorisent la participation active des parties prenantes concernées, dans un climat de confiance mutuelle, à des initiatives et des partenariats, qu'ils soient privés ou public-privé, formels ou informels, de niveau national, régional ou international, afin :
   - De partager des connaissances, des compétences, des expériences réussies et des pratiques éprouvées en matière de gestion du risque de sécurité numérique tant au niveau des politiques qu'au niveau opérationnel ;
   - D'échanger des informations concernant la gestion du risque de sécurité numérique ;
   - D'anticiper les enjeux et les opportunités à venir et de s'y préparer.

ii) Renforcent la coordination entre les parties prenantes afin d'améliorer, d'une part, la détection des vulnérabilités et des menaces et les mesures prises pour y remédier et, d'autre part, l'atténuation du risque de sécurité numérique ;

iii) Incitent l'ensemble des parties prenantes à travailler de concert pour aider à protéger les individus et les petites et moyennes entreprises contre les menaces, et renforcer leur capacité à gérer le risque de sécurité numérique qui pèse sur leurs activités économiques et sociales ;

iv) Créent, s'il y a lieu, des dispositifs pour inciter les parties prenantes à gérer le risque de sécurité numérique, et améliorer la transparence et l'efficience du marché ;

v) Encouragent l'innovation en matière de gestion du risque de sécurité numérique et de développement d'outils utilisables par les individus et les organisations pour protéger leurs activités dans l'environnement numérique ;

vi) Encouragent le développement d'indicateurs du risque permettant les comparaisons internationales, fondés sur des méthodologies, des normes et des bonnes pratiques communes, le cas échéant, afin d'améliorer l'efficacité, l'efficience et la transparence de la gestion du risque de sécurité numérique.

VIII. RECOMMANDE que les Adhérents travaillent de concert à la mise en œuvre de la présente Recommandation et en assurent la promotion et la diffusion dans les secteurs public et privé, auprès des non-Adhérents et dans les forums internationaux ;

IX. INVITE les non-Membres à adhérer à la présente Recommandation ;

X. CHARGE le Comité de la politique de l'économie numérique d'examiner la mise en œuvre de la présente Recommandation et d'en faire rapport au Conseil dans les trois ans suivant son adoption, puis ultérieurement en fonction des besoins.

***

Document d'accompagnement de la Recommandation du Conseil de l'OCDE sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale

Le Document d'accompagnement est de nature explicative et illustrative. Il ne fait pas partie de la *Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*.

Table des matières

Graphiques

Encadrés

Introduction

Au cours des dix dernières années, les technologies de l'information et de la communication (TIC), y compris l'Internet, sont devenues un maillon essentiel du fonctionnement de l'économie et un véritable levier de développement dans tous les secteurs. De fait, les principales activités des gouvernements, des organisations publiques et privées et des individus dépendent désormais de l'environnement numérique. Cependant, les incertitudes liées à l'utilisation de cet environnement vont croissant. Les menaces et les incidents de sécurité numérique se sont multipliés, avec, à la clé, des préjudices importants sur les plans financier, de la vie privée et de la réputation, voire, dans certains cas, des dommages corporels. Bien que les parties prenantes prennent de plus en plus conscience du risque de sécurité numérique, elles l'approchent souvent d'un point de vue seulement technique, et d'une manière séparée de la prise de décision économique et sociale. Il est devenu urgent d'expliquer que la gestion du risque de sécurité numérique doit, avant tout, faire partie de la prise de décision économique et sociale, afin de permettre aux parties prenantes de tirer pleinement parti des opportunités qu'offre l'environnement numérique.

Le terme générique de « cybersécurité » est souvent utilisé pour regrouper les différents aspects des questions de sécurité numérique – qu'ils soient technologiques, économiques, sociaux, juridiques, relatifs à la police, ainsi qu'aux droits de l'homme, à la sécurité nationale, aux opérations militaires, à la stabilité internationale, au renseignement, et bien d'autres aspects. La banalisation de ce terme fait souvent oublier l'ampleur et la complexité du sujet. En effet, la sécurité numérique peut être abordée sous au moins quatre angles différents, caractérisés par une culture, un contexte, des pratiques reconnues et des objectifs distincts :

- ***L'angle technologique***, axé sur le fonctionnement de l'environnement numérique (les experts parlent souvent de « sécurité de l'information », de « sécurité informatique » ou de « sécurité des réseaux ») ;
- ***L'application de la loi*** et, plus généralement, les aspects juridiques (par exemple, la cybercriminalité) ;

- ***La sécurité nationale et internationale***, qui couvre des considérations telles que le rôle des TIC dans le renseignement, la prévention des conflits, les opérations militaires, etc. ;
- ***La prospérité économique et sociale***, qui englobe non seulement la création de richesse, l'innovation, la croissance, la compétitivité et l'emploi dans tous les secteurs de l'économie,[1] mais aussi les libertés individuelles, la santé,[2] l'éducation,[3] la culture, la participation démocratique, la science, les loisirs et d'autres aspects liés au bien-être, que l'environnement numérique concourt à faire progresser.

Conformément à sa mission, qui consiste à promouvoir « des politiques meilleures pour une vie meilleure », l'OCDE aborde le risque de sécurité numérique dans une perspective économique et sociale.

En 2015, le Conseil[4] a adopté la *Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale* (la « Recommandation ») dans le cadre d'un ensemble plus vaste de Recommandations, d'orientations et de travaux analytiques sur la politique de l'économie numérique.[5] Fruit de plus de deux années de travaux, la Recommandation s'appuie sur 30 ans d'expérience de l'élaboration de politiques et d'instruments au service de l'innovation et de la confiance dans l'économie numérique, amorcés en 1980 avec la *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (« Lignes directrices de l'OCDE sur la vie privée », révisées en 2013) (OCDE, 2013b) et jalonnés par la mise au point d'instruments juridiques liés, entre autres, à la politique de cryptographie, à l'authentification électronique et à la protection des infrastructures d'information critiques (OCDE, 2008). La Recommandation remplace la *Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* (« Lignes directrices sur la sécurité de 2002 ») (OCDE, 2002), qui, elle-même, succédait à la *Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes d'information* (« premières Lignes directrices sur la sécurité ») de 1992. Il s'agit donc de la troisième étape d'un processus de maturation reflétant l'évolution de l'économie numérique et en particulier son rôle essentiel pour le bon fonctionnement et développement de l'ensemble des secteurs économiques et de la vie sociale.

Si les Recommandations ne sont pas des Actes de l'Organisation juridiquement contraignants, la pratique leur reconnaît une force morale importante, dans la mesure où elles représentent la volonté politique des pays Membres. On attend de ces derniers et des non-Membres y ayant adhéré (les « Adhérents ») qu'ils fassent tout ce qui est en leur pouvoir pour les mettre en œuvre intégralement.[6] La présente Recommandation a été approuvée par consensus à l'issue d'un processus multipartite associant les pouvoirs publics, des représentants des entreprises et de l'industrie, de la société civile et de la communauté technique.[7] Les non-Membres sont encouragés à s'en inspirer pour l'élaboration de leurs stratégies nationales, qu'ils choisissent d'adhérer formellement ou non à la Recommandation. En outre, l'OCDE engage toutes les organisations publiques et privées à intégrer à leurs cadres de gestion du risque les Principes qui y sont énoncés. Enfin, les autres organisations internationales et régionales sont encouragées à en tenir compte dans le cadre de leurs propres travaux et activités.[8]

La Recommandation reconnaît que les diverses perspectives mentionnées ci-dessus (économique, sociale, technique, criminelle, de sécurité nationale, de sécurité internationale) sont autant liées entre elles au sein de l'environnement numérique qu'en dehors. Par conséquent, les pouvoirs publics devraient aborder les différents aspects du risque de sécurité numérique dans une démarche associant l'ensemble du gouvernement et axée sur la cohérence, la complémentarité et le renforcement mutuel.

À cet égard, la Recommandation exhorte les pouvoirs publics à adopter une stratégie nationale de gestion du risque de sécurité numérique (I. 2) avec le soutien des plus hautes instances du gouvernement (Section 2. A. 1) afin de garantir un équilibre approprié entre des objectifs concurrents de l'action publique. La mise en œuvre de la Recommandation devrait favoriser la coopération entre les experts traitant des différents aspects de la sécurité numérique aux niveaux national, régional et international.

Il convient de souligner que la Recommandation et, plus généralement, les travaux de l'OCDE dans ce domaine, s'inscrivent dans le cadre d'un dialogue international impliquant plusieurs organisations qui poursuivent des axes de travail complémentaires, reflets de leurs mandats respectifs. Ainsi, le Conseil de l'Europe traite des questions liées à la cybercriminalité (avec, notamment,

la Convention de Budapest sur la cybercriminalité, adoptée en 2001) ;[9] Interpol favorise la coopération opérationnelle en matière d'application de la loi ;[10] les Nations Unies[11] et l'Organisation pour la sécurité et la coopération en Europe (OSCE)[12] examinent le comportement des États au sein de l'environnement numérique et les mesures de confiance destinées à préserver la stabilité internationale ; enfin, plusieurs organismes développent des normes techniques, de l'Organisation internationale de normalisation (ISO) à l'Internet Engineering Task Force (IETF), en passant par le World Wide Web Consortium (W3C), l'Organization for the Advancement of Structured Information Standards (OASIS), etc. Les organisations régionales telles que l'APEC (Asia-Pacific Economic Cooperation)[13] jouent également un rôle important pour promouvoir les bonnes pratiques.

La Recommandation s'ouvre par un préambule (« Considérant », « Reconnaissant », etc.), suivi de recommandations numérotées du Conseil (ci-après « l'OCDE ») aux gouvernements et aux autres parties prenantes (« I. Recommande », « II. Appelle », etc.), ainsi que des informations relatives aux Principes (« VI. Convient ») et des précisions d'ordre terminologique (« VII. Convient en outre »). Dans cette partie, l'OCDE appelle les décideurs au plus haut niveau des gouvernements et des organisations publiques et privées à adopter une approche de la gestion du risque de sécurité numérique de nature à susciter la confiance et tirer parti de l'environnement numérique ouvert pour assurer la prospérité économique et sociale (II).

La Section 1 pose un cadre cohérent fait de huit grands Principes étroitement liés, interdépendants et complémentaires concernant la gestion du risque de sécurité numérique (ci-après « les Principes »). L'OCDE recommande aux Adhérents de mettre en pratique ces Principes à tous les niveaux du gouvernement[14] et au sein des organisations publiques (I.1). Elle encourage par ailleurs les organisations privées – entreprises et organismes sans but lucratif – à intégrer les Principes à leur approche de la gestion du risque de sécurité numérique (III) et à mettre en œuvre les Principes dans le cadre de leurs processus décisionnels, selon leurs rôles, leur capacité à agir et le contexte[15] (IV).

Les Principes peuvent ainsi être appliqués directement par les organisations publiques ou privées pour faciliter l'élaboration de leurs politiques de gestion du risque, ou indirectement, pour inspirer la formulation des stratégies

nationales et des politiques publiques correspondantes. La Recommandation recommande justement que les Adhérents adoptent une stratégie nationale de gestion du risque de sécurité numérique en suivant les orientations proposées dans la Section 2 de la Recommandation, laquelle, quoique structurée de manière différente, a été élaborée à la lumière des Principes.

Dans l'ensemble, la Recommandation s'adresse avant tout aux décideurs au plus haut niveau (« les dirigeants et les décideurs ») qui sont en tant que tels les mieux placés pour amener, d'une part, les organisations à adopter un cadre approprié de gouvernance de la gestion du risque de sécurité numérique et, d'autre part, les gouvernements à se doter d'une stratégie nationale favorisant la prospérité économique et sociale.

Dès les premières étapes du processus de rédaction de la Recommandation, les délégations de l'OCDE ont reconnu la complexité du sujet et la nécessité de fournir, dans un document séparé, des informations et des explications contextuelles, afin d'en faciliter la mise en oeuvre. Elles se sont également accordées sur le fait que le « Document d'accompagnement » devait être succinct et traiter exclusivement des aspects fondamentaux de la gestion du risque de sécurité numérique et ainsi ne porter que sur la Section 1 de la Recommandation. Les travaux futurs permettront d'approfondir certaines des thématiques abordées ici et d'apporter les orientations nécessaires pour l'action des pouvoirs publics visée dans la Section 2 de la Recommandation. L'Annexe fournit une liste de sujet pour d'éventuels travaux futurs identifiés dans ce Document d'accompagnement ainsi que pendant le processus de consultation et de rédaction.

Après une brève description du contexte, le présent document examine les concepts clés de la Recommandation, examine l'applicabilité des Principes pour les parties prenantes, puis explique chacun des huit Principes.

Contexte

De nombreux dirigeants et décideurs des organisations publiques et privées prennent peu à peu conscience que l'environnement numérique n'est pas seulement un moteur d'innovation, de productivité et de croissance, mais aussi un vecteur d'incertitudes susceptibles de compromettre la prospérité économique et sociale. Les incidents de sécurité numérique peuvent avoir des conséquences économiques considérables pour les organisations – interruption d'activité (par exemple suite à une attaque par déni de service ou à un sabotage), pertes financières directes, actions en justice, atteinte à la notoriété, perte de compétitivité (en cas de violation d'un secret commercial, par exemple), ou encore perte de confiance des clients, des collaborateurs, des parties prenantes et des partenaires. Dans certains cas, qui restent à ce jour exceptionnels, les incidents peuvent aller jusqu'à causer des dommages physiques, y compris avec perte de vie humaine du fait de la dépendance croissante des installations industrielles, des systèmes de transport et des hôpitaux vis-à-vis des TIC.

Les gouvernements sont exposés aux mêmes conséquences potentielles que les organisations, mais pas seulement. En tant que concepteurs des politiques publiques, leurs préoccupations portent également sur les conséquences macroéconomiques des incidents, excédant en cela par certains côtés la sphère économique et sociale pour s'étendre à la sécurité nationale et internationale, comme évoqué précédemment.

Encadré 1. 2007-14: exemples d'incidents à grande échelle

S'il est difficile, dans ce domaine, de mettre au point des mesures quantitatives fiables et comparables à l'échelle internationale (OCDE, 2012c), les données empiriques dont on dispose montrent que les incidents de sécurité numérique se multiplient et qu'ils n'épargnent personne, des organisations publiques et privées aux individus, en passant par les gouvernements. Elles comprennent les exemples suivants.

En 2007, l'Estonie a ainsi été victime de « cyberattaques » massives visant le parlement, les ministères, les banques et les médias.

Encadré 1. 2007-14: exemples d'incidents à grande échelle (suite)

En 2010, le ver informatique Stuxnet a détruit physiquement des centaines de centrifugeuses d'enrichissement d'uranium en Iran. En 2011, des pirates se sont introduits dans le réseau Sony PlayStation Network, exposant les données personnelles de plus de 77 millions de comptes et coûtant, officiellement, à l'entreprise 171 millions USD – un chiffre qui, selon certaines estimations, pourrait en réalité atteindre 250 millions USD (Gaudiosi, 2014).

En 2012, il a fallu plus de deux semaines à la compagnie pétrolière Saudi Aramco pour se remettre du piratage au cours duquel a été effacé le contenu de plus de 30 000 disques durs connectés à son réseau interne.

En 2013, une attaque massive par déni de service (DdS) a été lancée contre l'organisation de lutte contre les courriels non sollicités Spamhaus, avec des pointes de débit record à 300 gigabits par seconde (Gbit/s), soit six fois plus que le débit moyens des attaques par DdS, et trois fois plus que ceux atteints lors de l'attaque par déni de service de la plus grande envergure jamais détectée (Leyden, 2013). La même année, l'enseigne de grande distribution américaine Target a été victime, à quelques jours de Noël, d'une attaque sophistiquée qui a infecté les caisses de ses points de vente, aboutissant au vol de 40 millions de numéros de cartes de crédit et de débit et de plus de 110 millions de données personnelles de ses clients. Le coût pour le groupe se situerait, selon les estimations, entre 148 millions et plus d'un milliard USD. Quelques semaines plus tard, son PDG a démissionné (O'Connor, 2014).

En 2014, l'entreprise américaine Home Depot a, à son tour, été victime du vol de 56 millions de données de cartes de crédit et de débit. En Corée, un homme a dérobé les données personnelles associées à 104 millions de cartes de crédit émises par trois grandes banques, faisant 20 millions de victimes, soit 40 % de la population du pays. Des dizaines de cadres supérieurs ont perdu leur emploi suite à ce piratage (Choe, 2014 ; Kim, 2014). Plus tard, au cours de la même année, les données de comptes que 76 millions de foyers américains et 7 millions de petites entreprises détenaient auprès de la banque américaine JP Morgan Chase ont été compromises ; suite à cet incident, le PDG a annoncé son intention de doubler le budget alloué à la sécurité numérique, de 250 à 500 millions USD (Kitten, 2014). Toujours en 2014, le réseau interne de Sony Pictures Entertainment a été la cible d'une intrusion en profondeur qui a conduit à la divulgation de courriels internes, de données personnelles de collaborateurs et de partenaires, et de films qui n'étaient pas encore à l'affiche ; par ailleurs, une opération de cyberespionnage à grande échelle (« Dragonfly ») ciblant principalement des entreprises européennes et américaines de l'industrie pharmaceutique et, potentiellement, du secteur de l'énergie, a été détectée (Peters, 2014). Enfin, une intrusion dans le réseau d'une usine sidérurgique en Allemagne a entraîné des « dommages physiques considérables » (Lee, Assante, Conway, 2014).

Enfin, les individus sont de plus en plus conscients que les nombreux avantages qu'ils tirent de l'utilisation de l'environnement numérique peuvent avoir un revers. Ainsi, la divulgation des données à caractère personnel ou l'accès non autorisé à ces données sont autant d'atteintes à la vie privée susceptibles d'induire des dommages corporels, matériels et moraux.[16] Les individus peuvent également être victimes de fraudes financières consécutives à une usurpation d'identité, en cas de vol de leurs données personnelles ou de leurs informations d'authentification numériques, perpétré à partir soit de leurs propres équipements, soit des systèmes d'information d'entreprises ou d'administrations compromises.

La multiplication et la sophistication accrue des incidents résultent de nombreux facteurs. L'un d'eux tient au déplacement des activités criminelles vers l'environnement numérique, entraînant une professionnalisation des attaques et une élévation du niveau général de la menace de sécurité numérique. Du simple pirate occasionnel aux groupes transnationaux parfaitement organisés, les criminels déploient des capacités d'innovation technique considérables pour extorquer des fonds, usurper des informations et des identités, et faire du chantage aux individus, aux entreprises et aux gouvernements. À cela s'ajoutent les terroristes et leurs soutiens, qui ont également étendu leur champ d'action à l'environnement numérique, en complétant les attaques physiques par des attaques de sites Internet, ou en les menant de front. Bien que peu de cas aient été documentés en détail, l'espionnage industriel numérique semble également gagner du terrain.[17] Les « hacktivistes » attaquent régulièrement des cibles sélectionnées dans le but d'accroître la visibilité de la cause politique qu'ils défendent. Enfin, de nombreux gouvernements mènent des opérations offensives et de renseignement dans ce qu'ils appellent le « cyberespace ». L'époque où la principale incertitude en termes de sécurité numérique était incarnée par des adolescents lançant des attaques aléatoires à l'aide d'outils prêts à l'emploi disponibles en ligne (les script-kiddies) est bel et bien révolue.

La professionnalisation des auteurs des menaces s'est traduite par une sophistication des outils techniques d'attaque, avec, pour certains, un déploiement automatisé à grande échelle pour un impact maximal, tandis que d'autres sont conçus spécifiquement pour des cibles sélectionnées avec soin et pour échapper à la détection et à l'attribution. Une économie souterraine de la cybercriminalité s'est également développée. Les programmes de type « jour

zéro », qui exécutent du code malveillant capable de déjouer la plupart des solutions de protection, sont disponibles à l'achat sur des sites de commerce électronique. Ils permettent de pénétrer furtivement les systèmes informatiques, de les surveiller et d'en exfiltrer des données confidentielles, telles que des secrets commerciaux ou politiques, et ce sur des périodes prolongées (on parle de « menaces persistantes avancées », ou APT).[18] Les botnets, qui peuvent infecter des milliers, voire des millions[19] d'ordinateurs et d'équipements, peuvent être loués pour lancer des attaques par déni de service, dans le but de faire du chantage à leurs propriétaires ou d'exprimer un mécontentement. En outre, les méthodes d'ingénierie sociale se sont généralisées ; elles peuvent prendre la forme de courriels qui, tout en paraissant légitimes, permettent à l'attaquant de dérober des identifiants ou de pénétrer le système de l'utilisateur (« hameçonnage »). L'encadré 1 recense des exemples d'incidents à grande échelle qui ont révélé l'étendue et l'importance de ces attaques.

À partir de 2009, les enjeux de la sécurité numérique sont peu à peu devenus une priorité de l'action publique dans les pays de l'OCDE. Un certain nombre de gouvernements ont entrepris d'adopter des « stratégies nationales de cybersécurité », avec le soutien des plus hauts niveaux de l'Etat. Ces stratégies visent à promouvoir une approche plus holistique et à instaurer de nouveaux mécanismes de coordination, tant au sein du gouvernements qu'avec les acteurs non gouvernementaux.[20]

Les organisations des secteurs public et privé mesurent peu à peu[21] l'ampleur du défi et ajustent leurs pratiques. En particulier, un nombre croissant de dirigeants de grandes entreprises a désormais conscience que la gestion du risque de sécurité numérique ne doit plus être abordée sous un angle exclusivement technique. En revanche, bon nombre d'organisations publiques et privées, à commencer par les Petites et Moyennes Entreprises (PME), ne sont pas encore prêtes à gérer le risque de sécurité numérique comme un enjeu économique et continuent de privilégier une approche principalement technique. Enfin, la multiplication des cas de violations massives de données impliquant l'accès à des données personnelles et donnant lieu, dans certains cas, à des fraudes financières et des usurpations d'identité, suscite l'inquiétude des individus[22] qui, souvent, ne disposent pas des moyens, des connaissances ni des compétences pour gérer efficacement le risque de sécurité numérique.

Encadré 2. De la « sécurité des systèmes d'information » à la « gestion du risque de sécurité numérique » (2002-15)

La Recommandation de 2015 s'inscrit, certes, dans la continuité des Lignes directrices de 2002 sur la sécurité, mais elle marque également un changement profond.

Les deux Recommandations partent d'une même analyse : i) la nature mondiale, interconnectée, ouverte et dynamique de l'environnement numérique est indispensable pour favoriser la prospérité économique et sociale, ii) il est impossible de parvenir à un environnement numérique « sûr et sécurisé », d'où le risque serait complètement écarté, sans renoncer, ce faisant, au caractère ouvert, interconnecté et dynamique, et aux bienfaits économiques et sociaux qui en découlent. Par conséquent, les deux Recommandations confirment l'abandon de la « sécurité périmétrique », statique et rigide, qui était de mise avant l'ère de l'Internet, au profit d'une approche cyclique et flexible, basée sur le risque, où ce dernier est géré, à savoir réduit à un niveau acceptable au regard du contexte et des objectifs en jeu.

Le principal changement tient au fait que les Principes ne sont plus axés sur la « sécurité des systèmes et réseaux d'information », mais sur le risque de sécurité qui pèse sur les activités économiques et sociales dépendant de l'environnement numérique. La Recommandation part du principe que les dirigeants et les décideurs chargés, en définitive, de mener à bien une activité, sont les mieux placés pour en définir le niveau de risque acceptable et s'assurer que les mesures de sécurité numérique sont adaptées et proportionnées au risque, et ne compromettent pas l'activité qu'elles visent à protéger. Néanmoins, elle met en exergue la nécessité d'une coopération avec les experts en charge de la conception et de la gestion de l'environnement numérique (à savoir les professionnels des TIC), qui sont susceptibles d'avoir une meilleure connaissance des facteurs de risque et des mesures de sécurité envisageables.

En conséquence, la terminologie a été clarifiée. Il est apparu, au cours du processus de rédaction, que la définition que le dictionnaire donne du terme « sécurité » – situation, état résultant de l'absence de danger ou de dommage – implique un objectif binaire et statique, intrinsèquement en contradiction avec le concept de gestion du risque. Pour certaines parties prenantes, le terme « sécurité » est lié à la « sécurité nationale », un domaine souvent associé, à tort ou à raison, à une culture où la sécurité prime sur toute autre considération. C'est pourquoi, contrairement aux Lignes directrices de 2002, la Recommandation utilise le terme « sécurité » comme un adjectif caractérisant le risque, les facteurs de risque, et l'approche de la gestion du risque, et ne l'utilise pas comme un substantif, afin qu'il ne puisse être interprété comme un objectif. De même, la Recommandation n'utilise pas le terme « cybersécurité » ni le préfixe « cyber » (comme dans « cyberespace »), sources potentielles de confusion car compris différemment selon les audiences. De plus, ils peuvent donner la fausse impression que le risque de sécurité numérique est, d'une manière ou d'une autre, fondamentalement différent des autres catégories de risque.

Concepts clés

Cette section présente les principaux concepts abordés dans la Recommandation.

Parties prenantes et rôles respectifs

Aux fins de la Recommandation, le terme « parties prenantes » désigne « les gouvernements, les organisations des secteurs public et privé et les individus qui dépendent de l'environnement numérique pour tout ou partie de leurs activités économiques et sociales. Elles peuvent endosser plusieurs rôles. » (voir VII, 3.)

L'emploi de ce terme vise à couvrir l'ensemble des entités qui, à des degrés divers, utilisent l'environnement numérique pour mener à bien des activités économiques et/ou sociales afin d'accomplir leur mission. Cette acception, plus sociologique que juridique, sous-entend une utilisation directe et/ou indirecte de l'environnement numérique. Le terme « gouvernement » couvre l'ensemble des autorités, à quelque niveau que ce soit (central/fédéral, international/régional/national/provincial/local, etc.). « Organisations publiques » désigne toutes les autres entités de droit public ou administratif, à l'instar des administrations financées par l'impôt (hôpitaux, établissements scolaires, bibliothèques publiques, etc.), ainsi que les entreprises publiques. Enfin, les « organisations privées » relèvent du droit privé et comprennent les entreprises et les organisations à but non lucratif.

Toutes les parties prenantes peuvent endosser des rôles différents et les cumuler. Par exemple, selon l'activité considérée, un particulier peut être un citoyen, un consommateur, un parent, un étudiant, un travailleur, etc. La plupart des organisations sont des utilisatrices de l'environnement numérique. Dans le cadre de leurs activités principales, certaines peuvent également intervenir dans son fonctionnement, sa gestion ou sa conception (tel est le cas des éditeurs de logiciels ou des fabricants de matériel, des opérateurs de télécommunications, ou des fournisseurs de service Internet). Par ailleurs, au-delà d'une certaine taille, les organisations disposent généralement d'une division informatique chargée de fournir l'infrastructure numérique qui sous-tend leurs activités. Certains individus participent également au fonctionnement de l'environnement numérique, sans pour autant appartenir à une organisation ; tel est le cas de certains développeurs d'applications ou de logiciels. Enfin, les gouvernements peuvent eux aussi

endosser différents rôles : d'une part, ils utilisent l'environnement numérique, dont ils dépendent dans une large mesure (dans le cadre de l'administration électronique et pour exécuter la plupart des autres fonctions publiques, telles que la rémunération des fonctionnaires) ; d'autre part, ils adoptent des politiques pour favoriser de la prospérité économique et sociale, y compris en lien avec l'environnement numérique.

Risque de sécurité numérique

Extrait de la Recommandation (VII. 1) :

« Le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Le terme « risque de sécurité numérique » désigne une catégorie de risque liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit.
Ce risque peut résulter d'une combinaison de menaces et de vulnérabilités inhérentes à l'environnement numérique. Il peut compromettre la réalisation des objectifs économiques et sociaux en portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des activités et/ou de l'environnement. Dynamique par nature, le risque de sécurité numérique se compose d'éléments liés à l'environnement numérique, à l'environnement physique, aux personnes qui participent à l'activité et aux processus organisationnels qui la structurent. »

Les activités menées par les parties prenantes dans le cadre de la réalisation de leurs objectifs sont tributaires de facteurs susceptibles d'influer sur leurs chances de réussite. L'incertitude fait partie de la vie : la connaissance et la compréhension de ces facteurs et de l'incidence qu'ils peuvent avoir sur la réalisation des objectifs sont limitées. Le « risque » est l'effet, ou la conséquence, de l'incertitude sur les objectifs que les parties prenantes cherchent à atteindre, à savoir l'inflexion que la réalité peut imposer par rapport à la voie qui a été tracée. Cette approche du risque s'appuie sur la norme ISO/CEI 31000:2009, la série ISO/CEI 27000 et le Guide ISO 73 (voir encadré 3). Le risque se mesure souvent en termes de probabilité et de conséquences, les niveaux de risque étant généralement représentés sur un axe X-Y, ce qui permet d'examiner les diverses combinaisons de ces deux dimensions.

Le risque de sécurité numérique tel que défini aux fins de la Recommandation (voir encadré 3) est l'une des nombreuses catégories de risques auxquelles sont confrontées les parties prenantes. Il présente les caractéristiques suivantes :

Encadré 3. Définitions, terminologie et normes

Les définitions et la terminologie utilisées dans la Recommandation ne revêtent pas un caractère normatif ou rigide, pas plus qu'elles ne reflètent une préférence particulière pour une terminologie du risque ou des termes techniques plutôt que d'autres. Elles ont été choisies pour soutenir la formulation d'orientations de haut niveau à destination de dirigeants et décideurs de pays Membres et non Membres de l'OCDE dont la culture, le cadre juridique et la situation économique, sociale et politique varient.

Dans la mesure du possible, la terminologie du risque employée dans la Recommandation est basée sur les normes et guides internationaux ISO/CEI afférents à la gestion du risque, en particulier la norme ISO/CEI 31000:2009 et le Guide ISO 73 – dont il est également tenu compte dans la série ISO/CEI 27000 – sachant que de nombreuses autres normes existent dans ce domaine, avec, parfois, une terminologie différente.[23] En règle générale, les termes et les définitions ont été adaptés au public ciblé, aux objectifs et au champ d'application de la Recommandation. Comme précisé dans cette dernière, les Principes ont vocation à être en adéquation avec les processus, les bonnes pratiques, les méthodologies et les normes existants en matière de gestion du risque. La Recommandation devrait contribuer à jeter un pont entre, d'une part, les dirigeants et décideurs de haut niveau et, d'autre part, les experts chargés de l'application de ces normes, au service de la prospérité économique et sociale.

La gestion du risque est une discipline complexe couvrant de nombreux secteurs – de la santé à la finance, en passant par l'ingénierie, l'assurance et les processus industriels –, qui se caractérisent par une culture, une terminologie et des normes en matière de risque qui leur sont propres. La Recommandation ne prétend pas représenter la une connaissance figée et globale du risque et de sa gestion. Le risque est un concept ancien qui n'a cessé d'évoluer au fil de l'histoire et continue de le faire. Il n'en existe aucune définition ou terminologie universellement admise : un chercheur a analysé récemment pas moins de 27 définitions du risque, regroupées en 9 catégories, tout en reconnaissant que cette liste n'est probablement pas exhaustive (Aven, 2012).

- *Il est lié à « l'incertitude numérique », mais pas seulement*. Toute dépendance vis-à-vis des TIC s'accompagne d'un certain degré d'incertitude liée à l'utilisation de l'environnement numérique (« incertitude numérique »). Toutefois, le risque de sécurité numérique ne concerne pas seulement des zéros et des uns : la dépendance à l'égard de l'environnement numérique implique le recours à du logiciel, du matériel, et à des interventions ou interactions humaines directes ou indirectes, toutes ces composantes pouvant être exposées à des menaces, des vulnérabilités et des incidents. Par exemple, une catastrophe

naturelle qui affecterait l'alimentation en énergie d'un centre de données ou endommagerait des câbles aériens pourrait entraîner la perturbation de la disponibilité d'un service ou le fonctionnement d'une chaîne de production ; de même, des criminels peuvent s'emparer de secrets commerciaux en ayant recours à des méthodes d'ingénierie sociale au moyen desquelles, par manipulation et imposture, ils amènent des personnes à effectuer des opérations leur permettant d'accéder aux systèmes d'information de façon illégitime. Les menaces, les vulnérabilités et les incidents peuvent donc avoir une dimension non seulement numérique, mais aussi physique ou humaine.

- *Il est de nature économique et sociale.* Les effets ou les conséquences de l'incertitude numérique sont économiques et sociaux, et peuvent affecter des actifs tangibles ou intangibles. Le risque doit donc être formulé en termes économiques et sociaux : perte financière, perte de compétitivité, occasions manquées, atteinte à la notoriété ou à l'image, perte de confiance, etc. À cela peuvent s'ajouter, selon le contexte, d'autres effets – c'est-à-dire catégories de risques – qui, certes, dépassent le champ d'application de la Recommandation, mais doivent toutefois être traités. Par exemple, les organisations peuvent envisager les conséquences purement techniques (à savoir liées aux TIC), et les gouvernements les conséquences relatives à la sécurité nationale et internationale.

- *Il affecte la Disponibilité, l'Intégrité et la Confidentialité* (i.e. la « sécurité »). Les événements susceptibles d'induire des effets sont la violation de confidentialité et d'intégrité, et la perturbation de disponibilité des activités ou de l'environnement numérique dans lequel elles ont lieu ou sur lequel elles reposent directement ou indirectement. Cette triade, dite « DIC », représente les propriétés ou attributs de sécurité traditionnels utilisés pour définir le périmètre de la gestion du risque de sécurité numérique en tant que domaine d'expertise spécifique. Le risque de sécurité numérique ne couvre donc pas les incertitudes liées à la violation des droits de propriété intellectuelle ou à la diffusion d'informations (contenu) inappropriées dans l'environnement numérique.[24]

- *Il a un effet négatif.* Dans le langage courant, le terme « risque » a généralement une connotation exclusivement négative et, par conséquent, la Recommandation est axée sur les incertitudes susceptibles de compromettre la réalisation des objectifs économiques et sociaux. La gestion du risque de

sécurité numérique y est conçue comme un moyen de protéger la valeur afin d'atteindre les objectifs économiques et sociaux de façon optimale. Toutefois, les incertitudes peuvent également avoir des effets positifs et profiter à une activité. On parle alors d'« opportunité » plutôt que de « risque », pour désigner ces effets bénéfiques. La relation entre risque et opportunité est importante car la gestion du risque de sécurité numérique peut aussi servir à créer de la valeur si l'on s'attache à déceler systématiquement les incertitudes dont on pourrait tirer servir pour innover. On reviendra sur ce point dans la section consacrée au Principe « Innovation ».

Facteurs de risque : menaces, vulnérabilités et incidents

Le risque peut résulter d'événements où une combinaison de menaces et de vulnérabilités produit des conséquences économiques. Les événements susceptibles d'altérer le déroulement attendu des activités et d'influer sur la réalisation des objectifs sont généralement appelés incidents. Il ne peut y avoir de conséquences sur l'activité sans la présence concomitante de menaces et de vulnérabilités. De fait, l'existence de menaces sans vulnérabilités ou, inversement, de vulnérabilités sans menaces, n'augmente pas le risque.

Dans le langage courant, le terme « risque » est employé au sens large. Il peut désigner une menace, une vulnérabilité, un incident, une probabilité, une chance, un danger.[25] En revanche, la gestion du risque requiert d'opérer une distinction claire entre les causes et les conséquences, et examine les premières (menaces, vulnérabilités et incidents) pour gérer les secondes (risque). Pour souligner cette différence, nous parlerons, dans le présent document, de « facteurs de risques » pour désigner les menaces, vulnérabilités et incidents, à savoir les causes du risque ou éléments qui y contribuent.

Les menaces sont généralement extérieures à l'activité, tandis que les vulnérabilités correspondent en principe à des faiblesses qui lui sont inhérentes. Par conséquent, les parties prenantes n'ont souvent que peu de prise sur les menaces ; elles peuvent en revanche agir plus directement sur les vulnérabilités. Il arrive toutefois que les deux éléments soient internes – par exemple lorsqu'un collaborateur mécontent se sert de ses privilèges pour réaliser des actions non autorisées aux conséquences néfastes pour l'employeur.

Il existe de nombreuses catégories et taxonomies des menaces, vulnérabilités et incidents. Ainsi, une menace peut être intentionnelle (à l'instar d'une attaque perpétrée par des criminels tentant de dérober quelque chose) ou non intentionnelle (par exemple, suite à un accident au cours duquel des travaux sur la voie publique endommagent un câble à fibre optique). Un incident peut également être le résultat d'une action humaine –comme lorsqu'une personne commet une erreur involontaire ou est manipulée par des méthodes d'ingénierie sociale (par exemple de type hameçonnage) –, ou d'événements naturels tels que des tempêtes, inondations, ou tremblements de terre. Par ailleurs, le degré de sophistication des menaces intentionnelles peut varier de la grande simplicité à l'extrême complexité, à l'image de leurs auteurs, qui vont des jeunes adolescents aux groupes soutenus par des États. Enfin, la durée des incidents peut être variable : certains sont extrêmement brefs, comme dans le cas d'attaques par déni de services perturbant les communications avec la clientèle au moment d'un pic d'activité annuel, quand d'autres au contraire peuvent se prolonger fort longtemps (jusqu'à plusieurs années), par exemple une intrusion furtive dans un système informatique pour dérober les secrets commerciaux d'une entreprise que l'on souhaite évincer du marché.

La nature dynamique du risque de sécurité numérique tient au caractère évolutif de chacune de ses composantes : activités économiques et sociales, facteurs de risque et environnement numérique.

Gestion du risque de sécurité numérique

Extrait de la Recommandation (VII. 2) :

« La « gestion du risque de sécurité numérique » est l'ensemble des mesures coordonnées, intra et/ou interorganisations, prises pour maîtriser le risque de sécurité numérique tout en maximisant les opportunités. Elle fait partie intégrante du processus décisionnel et s'inscrit dans un cadre global de gestion du risque qui pèse sur les activités économiques et sociales. Elle s'appuie sur un ensemble holistique, systématique et flexible de processus cycliques, aussi transparent et explicite que possible. Cet ensemble de processus contribue à la mise en œuvre de mesures de gestion du risque de sécurité numérique (« mesures de sécurité ») adaptées et proportionnées au risque et aux objectifs économiques et sociaux en jeu. »

Si le risque de sécurité numérique ne peut être éliminé (comme on l'a vu dans l'encadré 2), il peut en revanche être géré de façon à promouvoir et protéger les activités économiques et sociales. La gestion du risque a par conséquent pour finalité de favoriser la réalisation des objectifs économiques et sociaux. Plus spécifiquement :

- *Elle joue un rôle stratégique dans la prise de décisions économiques et sociales.* La gestion du risque est le processus par lequel les décideurs tiennent compte, dans le cadre de la conception et de la conduite de leurs activités, de facteurs susceptibles d'influer sur la réalisation de leurs objectifs. Dans la mesure où leurs activités économique et sociale dépendent, directement ou indirectement, de l'environnement numérique, la gestion du risque de sécurité numérique doit faire partie intégrante du processus décisionnel et aller de pair avec la maximisation des opportunités (voir le Principe « Innovation » ci-après). Les dirigeants devraient l'envisager comme un enjeu économique et social et non comme une question d'ordre purement technique. Cela passe nécessairement par une coopération avec les autres parties prenantes, en particulier celles chargées du fonctionnement et de la gestion de l'environnement numérique, afin de mieux appréhender les principaux facteurs de risque, tels que la probabilité de certaines menaces de sécurité informatique, la prédominance de vulnérabilités informatiques particulières et les caractéristiques d'éventuels incidents de sécurité informatique (par exemple, leur potentiel de propagation et d'intensification), ainsi que les mesures techniques susceptibles, entre autres, de faciliter le traitement du risque. Si les experts des TIC sont à même de déceler les incidents et de les traiter d'un point de vue technique, il n'est pas en leur pouvoir d'analyser les répercussions économiques sur l'organisation de ces incidents ni des mesures techniques prises pour les traiter. De la même manière, seuls les dirigeants et les décideurs sont en mesure de tenir compte du risque de sécurité numérique dans les plans et objectifs stratégiques généraux de leur organisation.
- *Elle garantit que les « mesures de sécurité » soutiennent pleinement les activités économiques et sociales en jeu et ne les compromettent pas.* Il est impossible de protéger une activité contre l'ensemble des menaces, vulnérabilités et incidents potentiels. Des décisions doivent donc être prises quant au choix et à la mise en œuvre des mesures de gestion du risque de sécurité numérique (« mesures de sécurité »). Qui plus est, ces mesures ne sont généralement pas neutres pour l'activité qu'elles protègent. Elles peuvent induire différents types d'obstacles

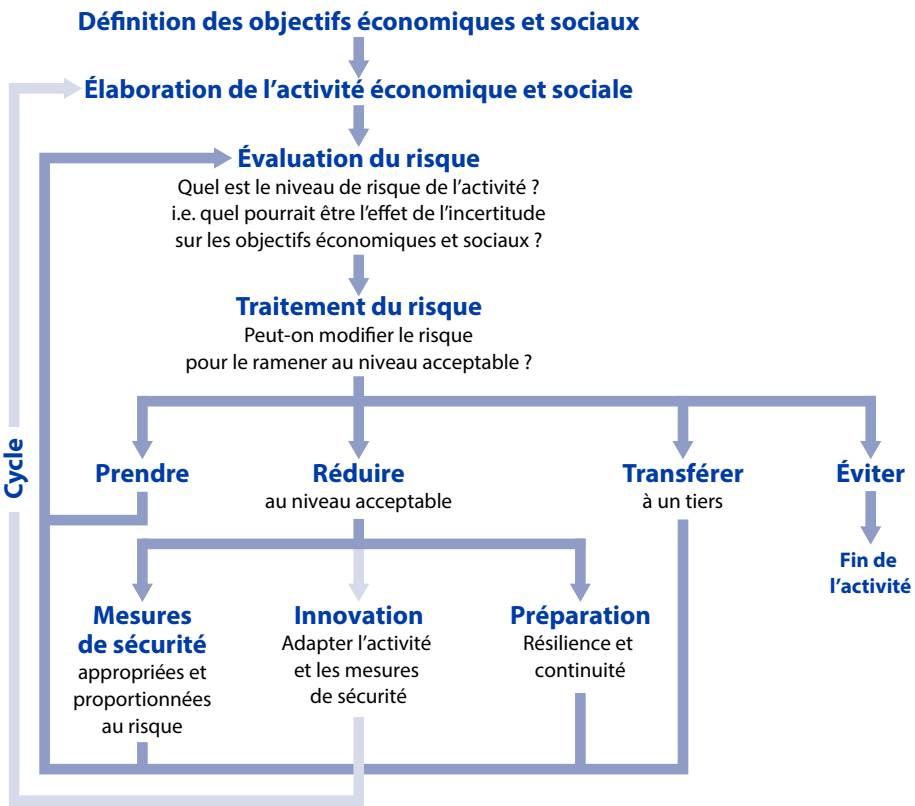
et de contraintes pour cette activité. Par exemple, accroître le coût financier et la complexité du système, limiter les performances, l'utilisation, l'évolutivité, l'innovation et la convivialité, ou encore allonger les délais de lancement sur le marché. Elles peuvent également donner lieu à des menaces sur la vie privée (voir Encadré 4) et avoir d'autres conséquences sociales préjudiciables. Ces contraintes et effets néfastes peuvent être traités et atténués, mais pas sans un coût. La gestion du risque de sécurité numérique permet d'ancrer les décisions de sécurité dans la réalité économique et sociale de l'activité concernée. Elle permet d'éviter la prise de décision isolée, en se basant uniquement sur des critères techniques ou de sécurité. Elle permet de choisir des « mesures de sécurité » appropriées et proportionnées au risque et à l'activité concernée. Ce faisant, elle permet de s'assurer qu'elles soutiennent pleinement les activités économiques et sociales qui sont menées, et ne viennent pas les compromettre, par exemple, en fermant de manière inappropriée l'environnement ou en limitant les fonctionnalités d'une manière qui réduise la possibilité de tirer parti des TIC pour innover et accroître la productivité.

- *Elle s'inscrit dans le cadre global de gestion du risque* et ne constitue pas une discipline cloisonnée et isolée. Le risque de sécurité numérique constitue l'un des nombreux types de risques qui pèsent sur les activités économiques et sociales. L'intégrer dans le cadre plus général de la gestion des risques à l'échelle de l'organisation confère aux dirigeants et décideurs de plus haut niveau une vue d'ensemble de la situation, garante d'une direction et d'une prise de décisions plus stratégiques et efficaces. De fait, il serait contre-productif de mettre en place un cadre de gestion dédié au seul risque de sécurité numérique en dehors du cadre existant.

Un cycle de gestion du risque devrait normalement être intégré au processus décisionnel relatif à la conduite d'activités, et concerner l'ensemble du cycle de vie de ces activités. On trouvera dans le graphique 1 une représentation schématique de la gestion du risque, sur laquelle figurent les Principes opérationnels établis par la Recommandation. L'étape première est celle de la définition des objectifs et de la conception des activités. Le risque est ensuite évalué puis traité en fonction des résultats de son évaluation, d'une manière conforme aux objectifs poursuivis et propre à en faciliter la réalisation. Le traitement du risque permet de déterminer si et comment il faut agir sur le risque pour accroître les chances de succès des activités, c'est-à-dire de

décider quelle partie du risque il convient d'accepter, de réduire, de transférer ou d'éviter (Principe 1). Pour réduire le risque, on peut alors sélectionner et appliquer des mesures de sécurité (Principe 2), songer à l'innovation à l'égard de ces mesures ou des activités en jeu (Principe 3) et définir des mesures de préparation à mettre en œuvre en cas d'incident (Principe 4). Le sujet est traité plus en détails dans la section consacrée aux Principes opérationnels.

Graphique 1: Aperçu du cycle de gestion du risque de sécurité numérique



Note : ce graphique, qui n'est qu'une possible représentation du cycle de gestion du risque de sécurité, est centré sur les Principes opérationnels énoncés dans la Section 1 de la Recommandation. Il convient de considérer les Principes généraux comme les éléments sous-jacents sur lesquels ce cycle repose.

Source: OCDE.

Encadré 4. Gestion du risque de sécurité numérique et protection de la vie privée

La relation entre gestion du risque de sécurité numérique et protection de la vie privée comporte au moins trois volets.

Tout d'abord, la gestion du risque de sécurité numérique fournit une base solide sur laquelle les contrôleurs de données (partie qui décide de la teneur et de l'utilisation des données de caractère personnel) peuvent s'appuyer pour mettre en œuvre le Principe des mesures de sécurité énoncé dans les Lignes directrices de l'OCDE sur la vie privée, selon lequel il « conviendrait de protéger les données de caractère personnel, grâce à des mesures de sécurité raisonnables, contre des risques tels que la perte des données ou l'accès aux données, leur destruction, utilisation, modification ou divulgation non autorisés ».

En particulier, la gestion du risque de sécurité numérique permet de s'assurer que les mesures de sécurité sont adaptées et proportionnées au risque, ce qui constitue une approche efficace de la formulation de mesures de sécurité « raisonnables ». Néanmoins, en matière de données personnelles, le niveau de risque acceptable pour contrôleur de données peut être supérieur à celui de la personne concernée. Ce possible décalage entre les intérêts respectifs de ces deux parties constitue l'une des principales problématiques de la protection de la vie privée. Plus généralement, le fait que la partie chargée d'évaluer le risque (le contrôleur de données) n'est pas celle qui y est exposée (la personne concernée) représente une différence de taille entre l'évaluation du risque de sécurité et du risque d'atteinte à la vie privée.

En outre, la gestion du risque de sécurité numérique peut compromettre le respect de la vie privée ; tel est le cas, par exemple, lorsque les mesures instaurées – surveillance des réseaux, partage d'informations avec des tierces parties, etc. – augmentent le risque qui pèse sur la vie privée. C'est pourquoi la protection de la vie privée est incluse dans le troisième Principe de la Section 1 de la Recommandation, afférent aux droits de l'homme et aux valeurs fondamentales, lequel appelle au respect et à la reconnaissance des intérêts légitimes d'autrui.

Enfin, la gestion du risque apparaît de plus en plus comme une méthodologie potentiellement utile pour améliorer la mise en œuvre des principes énoncés dans les Lignes directrices sur la vie privée. Toutefois, des travaux complémentaires sont nécessaires afin d'en appréhender les applications concrètes et les implications.

Dans les organisations relativement grandes, la complexité de la gestion du risque de sécurité numérique nécessite souvent l'adoption d'un cadre formel, garant d'une solution complète et cohérente à l'échelle de l'organisation. Généralement transcrit dans un document de politique ou de gouvernance

organisationnelle, un tel cadre peut prendre autant de formes qu'il existe de cultures organisationnelles et de styles de gestion. Il reflète les Principes de la Recommandation et est cohérent avec le cadre général de gestion du risque de l'organisation – s'il en existe déjà un– et dont il fait partie intégrante.

Le cadre de gestion du risque de sécurité numérique est généralement élaboré avec le concours de tous les acteurs concernés et adopté au plus haut niveau, afin de garantir un maximum de cohérence et de visibilité. Cela peut soulever des questions de gouvernance complexes qui ne sont pas abordées ici, mais qu'il conviendrait d'analyser plus avant. En règle générale, il énonce clairement la responsabilité et l'imputabilité des acteurs chargés de le mettre en œuvre. Parmi les aspects clés à couvrir, il importe d'établir les modalités de coopération en matière de gestion du risque de sécurité numérique entre les responsables « métier » et ceux en charge des TIC au sein de l'organisation.

Le cadre de gestion couvre l'ensemble des aspects des activités économiques et sociales qui dépendent de l'environnement numérique, tout au long de leur cycle de vie. Il clarifie les processus organisationnels afin de garantir une approche systématique et continue du risque. Il est suffisamment souple pour permettre d'apporter des réponses flexibles et prospectives aux risques de sécurité numérique qui se font jour. Comme expliqué plus loin (Principes opérationnels), il s'appuie sur un ensemble holistique, systématique et flexible de processus cycliques dont la mise en œuvre doit prendre en charge la nature intrinsèquement dynamique du risque. Il tient compte des bonnes pratiques et des normes applicables, tout en intégrant les éléments contextuels qu'elles ne couvriraient pas. Un certain degré de transparence contribue à renforcer la crédibilité et la confiance au sein et en dehors de l'organisation, témoignant de son engagement en matière de gestion du risque de sécurité numérique. Un tel cadre doit être vérifiable aisément et objectivement, via, par exemple, l'application d'une règle simple : « écrire ce que l'on fait, faire ce que l'on écrit ». Un cycle continu d'évaluation et d'amélioration du cadre est indispensable pour assurer une gestion efficace du risque et renforcer la confiance. Il est généralement assorti de processus visant à tester, auditer et optimiser les mesures instaurées.

La section consacrée aux Principes opérationnels apporte d'autres informations concernant la gestion du risque de sécurité numérique, et en particulier son caractère cyclique.

Applicabilité des principes

Les Principes devraient être mis en œuvre par les parties prenantes selon « leurs rôles, leur capacité à agir et le contexte » (voir IV). Si ce point s'applique d'une manière générale à l'ensemble des Principes, il revêt une importance particulière dans le cadre du Principe « Responsabilité » et a des incidences sur l'applicabilité des Principes opérationnels.

Rôles : distinguer les utilisateurs des acteurs responsables de l'environnement numérique

Comme évoqué dans la définition, les rôles des parties prenantes peuvent varier et être cumulés. Il importe d'opérer une distinction entre les parties prenantes au sens général, et celles chargées de mettre au point et de diffuser les biens et services numériques. Toutes les parties prenantes sont des utilisatrices de l'environnement numérique et, en tant que telles, devraient gérer le risque de sécurité numérique qui pèse sur leurs propres activités. Toutefois, celles qui, parmi elles, sont chargées du développement et de la gestion de l'environnement numérique (notamment les professionnels des TIC)[26] devraient en outre intégrer à leurs biens et services des mesures de sécurité appropriées lorsque cela est possible,[27] afin de permettre aux utilisateurs de gérer le risque de sécurité numérique. Par conséquent, elles se doivent de développer une double culture de la gestion du risque : l'une pour le risque qui pèse sur leurs propres activités dépendantes de l'environnement numérique, l'autre dans le but d'optimiser leurs biens et services afin donner aux clients et utilisateurs les moyens de gérer le risque découlant de leur utilisation de l'environnement numérique. Elles peuvent, par exemple, concevoir les produits et services d'une façon qui permette aux consommateurs de comprendre et d'utiliser des fonctionnalités de sécurité intégrées, faciles à utiliser et faisant un usage approprié des options par défaut.

Ces deux aspects sont étroitement liés : si le risque de sécurité relatif au développement des biens et services TIC n'est pas géré de manière appropriée, l'efficacité des mesures de sécurité qu'ils intègrent peut être altérée, avec, à la clé, un risque accru pour les utilisateurs. Par exemple, les systèmes d'information de l'autorité de certification néerlandaise DigiNotar ont été compromis en 2011 ; A la suite de ce piratage, 300 000 comptes Gmail ont été attaqués, les clients de DigiNotar ont été exposés à un risque accru et la confiance dans l'infrastructure de l'administration électronique néerlandaise, qui reposait indirectement sur cette entreprise (laquelle a finalement fait faillite) a été altérée. Autre exemple: l'attaque dont a été victime l'éditeur de solutions de sécurité RSA en 2011, qui a compromis quelque 40 millions de dispositifs de sécurité et donné lieu à l'utilisation des informations dérobées pour lancer des attaques contre certains de ses clients du secteur de la défense.[28] Les acteurs du secteur des TIC et, a fortiori, de la sécurité informatique, devraient être exemplaires dans leur gestion du risque de sécurité numérique.

Capacité à agir : distinguer les PME et les individus des autres parties prenantes

La capacité à agir des parties prenantes peut également varier considérablement en fonction d'autres facteurs, notamment i) de leur compréhension générale du risque de sécurité numérique, ii) de l'attention qu'elles portent à cette problématique et des ressources qu'elles y consacrent, iii) de leur capacité juridique – on parle parfois d'« habilitation» ou d'« autorité» à agir, et iv) du niveau de contrôle qu'elles peuvent avoir sur l'environnement numérique et de la facilité avec laquelle elles peuvent exercer ce contrôle. Pour ces quatre facteurs, il convient d'opérer une distinction entre, d'une part, les gouvernements et les grandes organisations et, d'autre part, les PME et les individus, dont la capacité à agir est généralement considérée comme plus limitée – surtout pour ces derniers. Le niveau de contrôle que les PME et les individus peuvent exercer dépend notamment de la disponibilité, du coût, de la facilité d'utilisation et de la pertinence des mesures de sécurité intégrées aux biens et services numériques proposés sur le marché.[29]

Compte tenu de ces contraintes, la Recommandation invite les gouvernements et les organisations publiques et privées à travailler de concert pour permettre aux individus et aux PME de gérer le risque de sécurité numérique (point V). Qui plus est, s'ils sont pertinents pour toutes les parties prenantes au plan

conceptuel, les Principes opérationnels énoncés dans la Section 1 visent avant tout à guider les organisations au-delà d'une certaine taille dans la définition de leur politique/cadre de gestion du risque de sécurité numérique. Des travaux complémentaires devraient être menés après l'adoption de la Recommandation, afin de mieux appréhender ce que ces Principes impliquent, tant sur le plan pratique qu'en termes d'action publique, pour les individus et les PME, et, éventuellement, de formuler des orientations en la matière.

Contexte : distinguer les situations particulières

Le contexte joue un rôle important dans l'interprétation des Principes énoncés. Par exemple, les exigences légales et réglementaires peuvent influencer les modalités de mise en œuvre de la gestion du risque de sécurité numérique, en obligeant par exemple les prestataires de services critiques à procéder à une évaluation formelle du risque et à démontrer que les mesures appropriées ont été mises en place. En outre, si une interprétation spécifique des Principes opérationnels est nécessaire pour les PME et les individus, compte tenu de leur capacité à agir limitée, certains d'entre-eux opèrent dans des contextes dans lesquels la gestion du risque revêt une importance accrue. Tel est le cas des PME intervenant dans des secteurs critiques, ou des individus manipulant des données ultrasensibles, à l'instar des médecins ou des journalistes.

Il convient par ailleurs de souligner que des individus peuvent agir comme des acteurs prenant part au développement et à la gestion de certaines parties de l'environnement numérique en dehors des structures organisationnelles. Entrent dans cette catégorie les personnes assurant la maintenance de composants de sécurité essentiels exploités par des millions d'utilisateurs (OpenSSL ou GNU Privacy Guard (GPG)), qui travaillent parfois sur ces outils à titre bénévole ou avec un budget et un soutien très limités. Tel est également le cas de la grande majorité des développeurs d'applications mobiles, qui, selon une enquête, tirent de leurs logiciels un revenu inférieur à 500 USD par mois.

Principes

Structure générale des Principes

Les huit Principes « doivent être pris comme un tout » :[32] ils sont tous indispensables et seront inefficaces s'ils sont interprétés ou mis en œuvre individuellement, ou si l'un d'entre eux est laissé de côté. L'ordre dans lequel ils sont cités et la numérotation utilisée suivent une logique narrative et ne reflètent pas nécessairement leur degré d'importance. Les Principes sont organisés en deux parties :

- *Les Principes généraux (1 à 4)* concernent « toutes les parties prenantes », à savoir les gouvernements, les organisations publiques et privées et les individus, qui, de manière directe ou indirecte, dépendent de l'environnement numérique pour tout ou partie de leurs activités économiques et sociales.
- *Les Principes opérationnels (5 à 8)* s'adressent plus particulièrement aux « dirigeants et décideurs » qui, parce qu'ils se situent au plus haut niveau du gouvernement et des organisations publiques et privées, sont les mieux placés pour amener leur entité à adopter un cadre approprié de gouvernance de la gestion du risque de sécurité numérique.

Principes généraux

Quatre Principes forment le socle sur lequel peut être établi un cycle de gestion du risque de sécurité numérique.

1. Sensibilisation, compétences et autonomisation

Gérer le risque de sécurité numérique requiert, au préalable, d'avoir conscience de son existence et d'acquérir les compétences appropriées – par l'éducation, la formation, l'expérience ou la pratique –, afin d'être en mesure de prendre des décisions responsables (autonomisation). La première étape d'une approche de la gestion du risque de sécurité numérique est donc la sensibilisation et l'acquisition des compétences nécessaires pour permettre aux parties prenantes de gérer le risque.

Toutes les parties prenantes étant interdépendantes au sein de l'environnement numérique, le fait d'ignorer le risque auquel l'une d'elles est exposée ou de ne pas être capable de le gérer peut accroître le risque qui pèse sur les autres.[33] Par conséquent, toute mesure de sensibilisation et de développement des compétences destinée à autonomiser un public ciblé a également un effet collectif positif sur la réduction globale du niveau de risque pour autant qu'elle se traduise par la mise en œuvre effective des compétences inculquées.

La sensibilisation au risque n'est pas la sensibilisation aux facteurs de risque – menaces, vulnérabilités et incidents. Si les conséquences possibles d'un accident de voiture sont intuitives – dommages corporels, voire décès –, la complexité de l'environnement numérique brouille le lien entre l'incident et ses conséquences. Par exemple, bien que de nombreuses personnes soient conscientes que leurs équipements peuvent être infectés par un virus, elles n'en mesurent pas nécessairement les conséquences potentielles telles que l'usurpation d'identité, la fraude financière, ou le vol de secret commercial. Les conséquences pour autrui sont encore moins visibles, par exemple lorsqu'un équipement infecté vient à faire partie d'un botnet utilisé pour lancer des attaques par déni de service. Ainsi, la sensibilisation devrait mettre l'accent sur les possibles effets économiques et sociaux (risque) des menaces, vulnérabilités et incidents, et non pas se limiter aux seuls facteurs de risque. Elle devrait par ailleurs encourager les parties prenantes à acquérir les compétences appropriées pour gérer le risque de manière à tirer le meilleur parti des bienfaits économiques et sociaux de l'environnement numérique, plutôt que de les dissuader d'y avoir recours.

De même, il convient de faire la distinction entre, d'une part, le développement d'une culture générale de la gestion du risque de sécurité numérique et, d'autre part, les connaissances et les compétences que chaque participant devrait posséder pour être à même d'évaluer et de gérer le risque selon son rôle, sa capacité à agir et le contexte. Dans les deux cas, il importe de tenir compte de la nature dynamique du risque, des facteurs de risque, de l'utilisation de l'environnement numérique, ainsi que des activités économiques et sociales en jeu. La sensibilisation et le développement des compétences relèvent d'un processus continu qui doit être intégré au cycle de gestion du risque.

Ce Principe s'applique à l'ensemble des parties prenantes : les gouvernements, les organisations publiques et privées, et les individus eux-mêmes, ont un rôle à jouer dans la sensibilisation à la gestion du risque de sécurité numérique et l'amélioration des compétences. Les organisations publiques et privées mettent au point des initiatives ciblant leur public, à l'appui de leurs propres cadres de gestion du risque. Certaines d'entre elles, en particulier les entreprises du secteur des TIC et les ONG, jouent un rôle important en soutenant des programmes de sensibilisation à l'intention du grand public ou de catégories de population particulières – enfants, adolescents, étudiants, personnes âgées, etc. Les initiatives peuvent prendre diverses formes et s'appuyer sur tous types de supports et de formules (cours, formations sur site, etc.). L'un des publics visés – cible privilégiée de la Recommandation – est celui des dirigeants et décideurs eux-mêmes, qui sont les mieux placés pour impulser des changements culturels et organisationnels au sein de leur organisation. En termes d'action publique, des efforts considérables ont été déployés au cours des dix dernières années tant par les gouvernements que par les acteurs du secteur privé, pour accroître la sensibilisation générale.[34] Ces efforts doivent se poursuivre afin d'atteindre toutes les catégories d'acteurs de l'économie et de la société, et de favoriser l'acquisition des compétences adéquates.

Suffisamment conscientes et compétentes, les parties prenantes autonomes peuvent assumer leur responsabilité (Principe 2).

2. Responsabilité

Une règle fondamentale de la vie sociale est que toute personne doit assumer les conséquences de ses actes, tant sur elle-même que sur autrui. C'est pourquoi toutes les parties prenantes devraient assumer la responsabilité de la gestion du risque de sécurité numérique, selon leur rôle, le contexte et leur capacité à agir, comme évoqué précédemment.

Ce principe ne traite pas des conséquences juridiques de cette responsabilité, qui varient selon le système légal et le contexte. En revanche, le Principe de responsabilité fait écho au préambule de la Recommandation, qui énonce que « les gouvernements, les organisations publiques et privées, ainsi que les individus partagent la responsabilité, selon leurs rôles respectifs et le contexte, de la gestion du risque de sécurité et de la protection de l'environnement numérique ». Il est devenu impossible de dépendre d'autrui pour tous les aspects de la gestion du risque de sécurité numérique. De fait, la responsabilité

est partagée, chaque intervenant en exerçant un certain degré. Charge aux parties prenantes de réfléchir à leur rôle, au contexte et à leur capacité à agir, et de déterminer la responsabilité qui leur incombe.

Cette responsabilité montre que l'environnement numérique n'est pas différent des autres : un certain niveau de risque de sécurité numérique doit être accepté pour atteindre les objectifs économiques et sociaux.

Pour employer une analogie, toutes les parties prenantes ont une part de responsabilité en matière de sécurité routière, selon leur rôle, le contexte et leur capacité à agir. Les conducteurs devraient avoir appris à conduire et respecter les règles de sécurité de base : ne pas boire d'alcool, respecter les limitations de vitesse, attacher leur ceinture, tenir compte des autres conducteurs, etc. Les constructeurs automobiles devraient, pour leur part, concevoir des véhicules de manière à minimiser les accidents liés aux défauts de conception ou aux pannes mécaniques (à savoir éviter des vulnérabilités, telles que des freins défaillants), et intégrer des mécanismes de protection (en prévoyant des mesures de sécurité de type airbags, rétroviseurs, etc.). Les constructeurs routiers devraient, quant à eux, concevoir des routes qui soient les moins accidentogènes possible : installation de glissières de sécurité, ronds-points, feux tricolores, panneaux de signalisation, etc. Enfin, les pouvoirs publics devraient définir des règles applicables aux conducteurs, à la construction des véhicules et à la circulation routière, et veiller à leur application. Ils devraient également mettre en place des services d'urgence (mesures de préparation), etc. Toute défaillance à un niveau de responsabilité, quel qu'il soit, augmente le niveau de risque pour l'un des acteurs ou pour l'ensemble.

Les parties prenantes qui décident d'utiliser l'environnement numérique pour atteindre leurs objectifs économiques et sociaux (à l'instar des conducteurs) acceptent un certain niveau de risque de sécurité – les éventuelles conséquences négatives. Elles devraient gérer ce risque, à savoir le réduire à un niveau acceptable au regard des quatre Principes opérationnels énoncés ci-après. Elles devraient également être en mesure de rendre compte de leur action ou inaction (imputabilité).

Toutefois, tous les participants ne sont pas égaux en termes de responsabilité et d'imputabilité. Ils doivent être capables de gérer le risque – par exemple,

en termes d'informations, de connaissances, de compétences, de ressources, d'outils et de contrôle, y compris en matière de technologie. Leur capacité à identifier, évaluer et gérer le risque varie sensiblement ; ainsi, on ne peut raisonnablement escompter que certaines catégories (notamment les individus et les petites entreprises) identifient, évaluent et gèrent le risque de la même manière que d'autres acteurs ayant accès à des ressources plus conséquentes. Comme évoqué précédemment, il conviendrait de mener des travaux complémentaires sur les enjeux et les pistes envisageables pour faciliter la mise en œuvre de ce Principe par les individus et les PME.

Les parties prenantes qui mettent au point, opèrent ou gèrent des composants de l'environnement numérique, tels que les logiciels, le matériel (les constructeurs automobiles, pour poursuivre l'analogie) et les infrastructures réseau (les constructeurs routiers), devraient créer les conditions propices pour que les utilisateurs puissent prendre des décisions responsables en matière de gestion du risque. Il s'agit par exemple d'adopter des normes et des bonnes pratiques, d'intégrer aux composants techniques des mesures de sécurité appropriées, et de fournir des informations et une aide adaptées afin d'autonomiser convenablement les utilisateurs, en tenant compte de la nature dynamique du risque.

Les gouvernements quant à eux devraient définir des stratégies nationales et adopter des mesures et des initiatives d'action publique favorisant la gestion du risque de sécurité numérique par l'ensemble des parties prenantes. La plupart des Membres de l'OCDE ont d'ores et déjà mis en place les composants de base – réglementations, législation (par exemple en matière de cybercriminalité et de protection de la vie privée), capacité d'intervention (avec les équipes de réponse aux incidents de sécurité informatique, CSIRT), éducation, partenariats public-privé, etc. Depuis plusieurs années, ils ont entrepris de formuler leurs politiques dans des termes plus stratégiques[35] et veillent à renforcer la cohérence de leurs approches, par le biais, notamment, de mécanismes de coopération nouveaux ou améliorés, tels que des agences dédiées ou d'autres moyens. Comme le montre la Section 2, la politique publique en faveur de la gestion du risque de sécurité numérique est intrinsèquement horizontale et nécessite une coopération non seulement au sein du gouvernement, mais aussi avec l'ensemble des parties prenantes aux niveaux national, régional et international. Elle s'inscrit dans un effort d'action publique stratégique à long terme.

Cependant le degré d'interconnexion et d'interdépendance des parties prenantes est autrement plus important dans l'environnement numérique que sur la route.. Aussi le Principe de responsabilité énonce-t il que ces parties prenantes devraient tenir compte de l'impact potentiel de leurs décisions sur autrui. Cet impact concerne notamment : i) les tiers dont elles traitent les données à caractère personnel, ii) l'écosystème numérique global, sachant que sa protection est l'affaire de tous[36] et que l'action ou l'inaction de chacun peut contribuer à le protéger ou à le dégrader, iii) le fonctionnement de l'économie et de la société dans leur ensemble, dans la mesure où l'environnement numérique est utilisé pour les infrastructures et les services critiques. Au-delà de l'adoption de bonnes pratiques et de la prise en considération des intérêts d'autrui, l'exercice de la responsabilité collective peut se faire par plusieurs moyens : l'observation des normes et bonnes pratiques et la participation aux organisations de normalisation, la collaboration avec les autres parties prenantes, notamment au niveau transfrontalier et interdisciplinaire, etc.

Tous les acteurs ont également la responsabilité de gérer le risque de sécurité numérique dans le respect des droits de l'homme et des valeurs fondamentales (Principe 3) et de coopérer avec les autres parties prenantes (Principe 4).

3. Droits de l'homme et valeurs fondamentales

Les règles sociales de base s'appliquent à l'environnement numérique. Il les droits de l'homme et des valeurs fondamentales d'y appliquent donc également et demandent dès lors à y être protégés. Ces droits et valeurs sont énoncés dans divers instruments internationaux, parfois avec d'autres appellations – « valeurs universelles », « libertés fondamentales », etc. Les instruments internationaux applicables comprennent la Déclaration universelle des droits de l'homme, le Pacte international relatif aux droits civils et politiques, et le Pacte international relatif aux droits économiques, sociaux et culturels.[37]

Selon leurs modalités d'utilisation, les mesures de sécurité adoptées aux fins de la gestion du risque de sécurité numérique[38] peuvent avoir des effets positifs ou négatifs sur le respect des droits de l'homme et des valeurs fondamentales. Elles peuvent influer sur la liberté d'expression, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection de la vie privée et des données à caractère personnel, l'ouverture et le droit à une

procédure équitable.[39] Par exemple, les mesures de sécurité peuvent contribuer à renforcer la protection de la vie privée ou assurer l'anonymat des lanceurs d'alerte et des défenseurs des droits de l'homme. Elles peuvent en revanche permettre une surveillance illégitime des citoyens ou empêcher l'accès au contenu produit par les militants. Par ailleurs, elles peuvent avoir une influence sur d'autres droits et valeurs non mentionnés au titre du Principe. Par conséquent, une approche responsable implique que les décisions de gestion du risque de sécurité numérique soient prises à la lumière des conséquences sur ces droits et valeurs.

Ce Principe s'applique à l'ensemble des parties prenantes. Les organisations doivent être conscientes que l'adoption de mesures de sécurité numérique qui compromettent les droits de l'homme et les valeurs fondamentales peut porter atteinte à leur image et leur crédibilité, et engage leur responsabilité juridique. Elles doivent tirer parti de la nature systématique du cycle de gestion du risque de sécurité numérique pour évaluer l'impact de leurs décisions en la matière sur les droits de l'homme et les valeurs fondamentales, et les adapter en conséquence. Les programmes de gestion de la confidentialité, préconisés dans les Lignes directrices de l'OCDE sur la vie privée, gagneraient assurément à être intégrés aux cadres et aux structures de gouvernance existants en matière de gestion du risque.[40]

Les parties prenantes chargées de la conception, du fonctionnement ou de la gestion de l'environnement numérique (par exemple les professionnels des TIC) devraient se demander si les mesures de sécurité qu'elles intègrent aux biens et services informatiques sont susceptibles d'être utilisées dans le but de porter atteinte aux droits de l'homme et agir en conséquence si tel est le cas. Il arrive que les incidences potentielles sur le respect de ces droits dépendent du contexte dans lequel les biens et services sont utilisés, et il n'est pas toujours possible de l'empêcher au stade de la conception. Les professionnels de l'informatique devraient alors envisager d'avertir les utilisateurs d'effets négatifs potentiels sur les droits de l'homme et de la façon de les prévenir. Enfin, les pouvoirs publics devraient s'assurer que les politiques en faveur de la gestion du risque de sécurité numérique soutiennent et respectent les cadres légaux et réglementaires, ainsi que les obligations internationales en la matière (voir Section 2. A. 2).

Conformément à la « Règle d'or », ou l'éthique de réciprocité (« traiter autrui comme on voudrait qu'il nous traite »), les parties prenantes devraient

reconnaître que leur action ou inaction peut porter préjudice à autrui et affecter l'environnement numérique lui-même. Elles devraient faire preuve d'éthique, à savoir respecter les intérêts légitimes d'autrui et de la société dans son ensemble. Le comportement éthique est d'autant plus important que la nature ouverte, mondiale et interconnectée de l'environnement numérique peut accroître l'impact de l'action ou de l'inaction des parties prenantes.

Les organisations devraient se doter d'une politique générale de transparence sur leurs pratiques et leurs procédures de gestion du risque de sécurité numérique. Toutefois, des travaux complémentaires seraient nécessaires pour formuler des orientations quant aux modalités de mise en œuvre d'une telle politique, en particulier dans les cas où une transparence excessive pourrait nuire à la sécurité et pour ce qui est des mécanismes de surveillance envisageables.

4. Coopération

Comme souligné précédemment, l'interconnectivité mondiale de l'environnement numérique se traduit par une interdépendance des parties prenantes. Celle-ci présente des aspects positifs, tels que les bienfaits économiques et sociaux qu'elle confère à chacune des parties, fruits de l'effort collectif déployé. Mais elle a aussi des inconvénients, dans la mesure où elle renforce la complexité, facilite la propagation des menaces et des vulnérabilités, et peut accroître le risque collectif. Les parties prenantes étant à la fois interdépendantes et dépendantes de l'environnement numérique, la coopération s'avère essentielle.

La plupart des aspects de la gestion du risque de sécurité numérique nécessitent un certain degré de coopération[41] et ne peuvent être traités avec succès par une partie isolée. C'est pourquoi la coopération sous-tend tous les autres Principes de la Recommandation. Par exemple : i) la sensibilisation et le développement des compétences impliquent que les personnes plus informées et qualifiées, à leur tour, informent, éduquent et forment celles qui en ont besoin, lesquelles doivent être conscientes de l'intérêt qu'elles ont à gagner en autonomie et en connaissances ; ii) la responsabilité est partagée par toutes les parties prenantes selon leur rôle, leur capacité à agir et le contexte. D'où une nécessaire coopération, afin que celles qui ont des rôles complémentaires assument leur responsabilité de manière cohérente ; iii) si les droits de l'homme et les valeurs fondamentales sont généralement codifiés par la loi,

ils peuvent être exprimés dans des termes éthiques ; à ce titre, un dialogue et des échanges sont nécessaires entre les parties, afin de mieux les comprendre et les respecter. Par ailleurs, la mise en œuvre des Principes opérationnels requiert une étroite coopération entre les parties prenantes chargées de mener à bien les activités économiques et sociales et celles qui ont pour mission de fournir l'environnement numérique sous-jacent. Il en va de même pour les mesures de sécurité, l'innovation et les mesures de préparation, dont la pleine mise en œuvre ne peut se faire sans coopération, y compris pour les aspects non techniques nécessitant une modification des comportements humains et l'adoption de processus à l'appui de la gestion du risque de sécurité numérique.

La coopération visant à améliorer la gestion du risque de sécurité numérique devrait impliquer l'ensemble des parties prenantes, selon leur rôle. Elle devrait se faire au sein des organisations et transcender les silos. Les dirigeants au plus haut niveau ont un rôle essentiel à jouer pour s'assurer que les politiques et les cadres internes de gestion du risque créent les conditions propices à une coopération efficace. Il importe en particulier d'instaurer une collaboration entre les composantes de l'organisation qui utilisent l'environnement numérique pour mener à bien les activités économiques (« côté métier »), celles qui fournissent l'environnement (« côté informatique ») et celles qui veillent à la conformité juridique et réglementaire.

On peut citer une multitude d'autres formes de coopération, par exemple :

- entre les organisations, afin notamment de traiter le risque de propagation des menaces et des vulnérabilités entre les entreprises et les partenaires au sein de la chaîne de valeur. Ceci inclut les pouvoirs publics, avec une nécessaire coopération entre les différents ministères, organismes et niveaux de gouvernement (local/provincial/national, par exemple), et les sous-traitants ;
- entre les organisations d'un même secteur économique, exposées à des menaces communes. Dans certains cas, il arrive que les autorités publiques favorisent une telle coopération, dans le domaine des infrastructures critiques notamment ;
- entre les secteurs public et privé, ainsi des organisations du secteur privé, qui peuvent être amenées à coopérer avec les organismes d'application de la loi, les établissements d'enseignement et d'autres organismes publics ; et

- entre les organisations et les consommateurs et utilisateurs, et, plus généralement, la société civile.

Pour ce qui est de la définition de l'action publique, il importe d'adopter une approche multi-partite afin de créer les conditions propices à une participation élargie et à l'élaboration de politiques meilleures (Section 2. A. 4). Dans les faits, une telle approche peut se traduire par des partenariats et des initiatives public-privé dans de nombreux domaines, tels que la sensibilisation et le développement des compétences, la cybercriminalité (par le biais de la coopération avec les organismes d'application de la loi), la mise en place d'équipes CSIRT/CERT,[42] l'échange et le partage d'informations,[43] etc. La Section 2 (en particulier les paragraphes B. 3 et B. 4) propose de nombreux axes de coopération entre les secteurs public et privé.[44]

Enfin, la coopération devrait s'étendre, s'il y a lieu, au-delà des frontières.

Principes opérationnels

Le cycle global de gestion du risque de sécurité numérique ayant été présenté plus haut avec les « concepts clés », on s'attardera ci-après sur chacun des Principes. D'une manière générale, il convient toutefois de considérer la gestion du risque numérique comme un processus de décision créatif et souple, susceptible de permettre un accroissement des bienfaits d'une activité rendue à même de suivre au plus près l'évolution constante – et par conséquent incertaine – du contexte dans lequel elle s'inscrit. La gestion du risque numérique constitue une réponse dynamique à un enjeu qui l'est tout autant et offre souplesse et adaptabilité aux parties prenantes pour accroître leurs chances de succès. Aussi est-elle par essence :

- *Cyclique* : les activités économiques et sociales, l'environnement numérique dans lequel elles ont lieu et les risques numériques sont en perpétuelle évolution. Pour suivre le rythme, le mieux serait de soumettre ces risques à un suivi continu. Il s'agirait concrètement de définir un cycle général, déterminé par l'activité concernée, ainsi qu'un autre plus spécifique, déterminé par certains événements, tels que l'émergence de nouvelles menaces et vulnérabilités, la survenue de nouveaux incidents et l'évolution d'autres aspects contextuels. La nature cyclique de la gestion du risque est signifiée, dans le graphique 1, par les flèches partant du bas du schéma pour

revenir à la phase d'évaluation du risque, ou à celle de la conception dans le cas de l'innovation au niveau de l'activité.

- *Holistique* : l'environnement numérique étant interconnecté, la gestion du risque devrait obéir à une approche globale. Elle devrait par exemple embrasser l'ensemble de la chaîne de valeur de l'activité concernée, sachant que certaines vulnérabilités en un point donné de cette chaîne pourraient être exploitées par des menaces en provenance d'un autre point et porter à conséquences en un troisième. Il convient par ailleurs qu'elle couvre des aspects en rapport avec les personnes, les processus (c'est-à-dire les règles et procédures) et les technologies qui interviennent le long de la chaîne de valeur. Elle devrait par conséquent aller de pair avec la gestion d'autres catégories de risques, sans pour autant créer de doublons sur le plan des processus ou de la méthodologie.
- *Systématique* : la complexité d'un cycle holistique de gestion du risque sera vraisemblablement à l'image de la complexité de l'organisation et des activités en jeu. Une approche systématique est le meilleur moyen de gérer une complexité croissante, les différentes composantes étant isolées et traitées de manière individuelle dans une perspective d'ensemble.

L'adoption d'une approche cyclique, holistique et systématique pour la gestion du risque de sécurité numérique crée les conditions propices à une gestion conjointe du risque et des opportunités, comme on le verra plus loin (Principe 7, « Innovation »). Elle permet également une prise en considération plus complète et appropriée des droits de l'homme et des valeurs fondamentales, des intérêts légitimes d'autrui ainsi que de l'impact potentiel des mesures de sécurité sur ces droits et valeurs et sur l'environnement numérique.

Différentes méthodologies, normes et bonnes pratiques peuvent s'avérer utiles aux fins de la gestion du risque, et ce à de nombreux niveaux, que ce soit celui du processus pris dans son ensemble ou sous certains aspects plus spécifiques comme les mesures de sécurité ou la préparation.

5. Cycle d'évaluation et de traitement du risque

L'évaluation et le traitement en continu du risque sont essentiels pour que les décisions touchant la sécurité soient adaptées et proportionnées au risque et à l'activité économique et sociale en jeu.

L'évaluation du risque est un processus analytique que l'on peut décomposer en plusieurs étapes, au cours desquelles le risque est i) détecté : les facteurs de risque sont identifiés, souvent sur la base de l'expérience, de données historiques, d'analyses théoriques, d'avis et opinions autorisés, etc. ; ii) analysé : le risque est compris et son niveau déterminé ; comme indiqué plus haut, ce niveau est souvent exprimé en termes de probabilité et d'impact sur l'activité économique et sociale concernée; iii) évalué : le niveau du risque est comparé au niveau acceptable par rapport à l'activité, aux objectifs économiques et sociaux de celle-ci et aux bienfaits qui en sont attendus.

Même si l'évaluation du risque devrait s'intéresser au premier chef aux conséquences potentielles de l'incertitude sur les objectifs poursuivis, il convient également d'y prendre en considération, s'il y a lieu, les conséquences potentielles pour les tiers, dans la mesure où ceux-ci ont un rôle à jouer ou pourraient être affectés (par exemple dans leur vie privée ; voir l'encadré 4). L'évaluation du risque devrait également tenir compte de l'effet possible de l'incertitude sur l'écosystème numérique considéré dans sa totalité (risque collectif).

Le traitement[45] du risque est un processus décisionnel fondé sur le résultat de l'évaluation du risque, qui cherche à réduire celui-ci à un niveau acceptable au regard des bienfaits économiques et sociaux que l'on attend de l'activité considérée, sans méconnaître les incidences potentielles sur les intérêts légitimes d'autrui (« niveau acceptable de risque »). Au nombre de ces intérêts figurent les droits de l'homme et les valeurs fondamentales (Principe 3) ainsi que le fonctionnement de l'environnement numérique.

Il existe généralement quatre manières de traiter le risque (voir le graphique 1), qu'il est possible de combiner :

- *Accepter* le risque : « prendre le risque » et accepter l'effet de l'incertitude sur les objectifs, y compris si cela se traduit par un échec partiel ou total. Dès lors que l'activité en jeu est entreprise, le risque ne peut être entièrement éliminé, si bien qu'il faut accepter un risque « résiduel » (voir Principe 2, « Responsabilité »). En règle générale, la gestion du risque est efficace sur le plan économique du moment que les bienfaits retirés de l'exécution de l'activité l'emportent sur le risque résiduel.

- ***Réduire*** le risque à un niveau acceptable, à travers : i) le choix et l'application de mesures de sécurité aptes à protéger l'activité contre certaines menaces potentielles exploitant des vulnérabilités décelées lors de l'évaluation du risque (Principe 6) ; ii) la modification de l'activité, par exemple en la concevant ou conduisant différemment, ce qui peut conduire à innover (Principe 7) ; et iii) la définition, et si nécessaire l'application, de mesures de préparation pour faire face à la survenue d'incidents (Principe 8).
- ***Transférer*** le risque : déplacer vers un tiers les effets indésirables de l'incertitude qui entoure les objectifs de l'activité, au moyen, par exemple, d'un contrat tel que dans le cas d'une police d'assurance ; il pourrait être utile de s'intéresser à l'assurance du risque de sécurité numérique dans le cadre de travaux futurs.
- ***Éviter*** le risque : l'éliminer, en renonçant à exécuter l'activité ou en en éliminant la composante numérique.

Le « niveau acceptable de risque » doit être déterminé par la partie prenante qui exerce l'activité et est confrontée au risque. On appelle « appétit de risque » la mesure du risque qu'une partie prenante est prête à accepter lorsqu'elle entreprend une activité. Cet appétit est déterminé par de nombreux facteurs liés à l'activité en question et à ses objectifs, mais aussi à la culture et au style de l'organisation, à la situation du marché, à l'environnement technique, etc. Il peut aussi, dans certains cas, être limité par le contexte juridique et réglementaire. À moins que le risque ne soit accepté dans son intégralité, ou évité, une décision doit être prise quant à sa réduction au niveau acceptable ou son transfert.

6. Mesures de sécurité

Indispensables à la protection des activités économiques et sociales, les mesures de sécurité peuvent néanmoins avoir un effet négatif sur celles-ci. Ce Principe souligne que le meilleur moyen de garantir que les mesures de sécurité sont adaptées et proportionnées au risque et à l'activité économique et sociale en jeu est de les choisir, les mettre en œuvre et les améliorer à la lumière de l'évaluation du risque et du traitement retenu (voir plus haut la définition de la gestion du risque de sécurité numérique).

Les mesures de sécurité peuvent par exemple alourdir le coût de l'activité et avoir une incidence sur son utilité, ses résultats et son potentiel d'amélioration.

Nombre de mesures de sécurité d'ordre technique peuvent entraîner une certaine diminution des flux d'informations (ainsi des pare-feux) ou imposer des éléments de procédure additionnels (par exemple, l'authentification). Il en est qui se traduisent par un surcroît de complexité (par exemple la cryptographie) et impliquent des arbitrages sur le plan de la fonctionnalité pour rester applicables. Parmi les mesures de sécurité susceptibles de porter atteinte aux droits de l'homme et aux valeurs fondamentales, citons celles nécessitant l'accès à des données personnelles, comme le contrôle et l'analyse des flux de trafic afin de détecter des menaces de sécurité (par exemple, l'« inspection approfondie des paquets »). Les professionnels de la sécurité sont régulièrement confrontés à des données personnelles dans le cadre de leurs activités. Il leur arrive ainsi de devoir accéder à des comptes personnels pour analyser un incident ou de devoir transférer à des tiers des informations personnelles en rapport avec un incident aux fins d'un complément d'analyse ou d'une expertise judiciaire. La gestion de crise peut aussi donner lieu à des situations où il est par exemple nécessaire d'interrompre un service pour enrayer la propagation d'une menace, ce qui peut aller à l'encontre des droits des utilisateurs. Le cycle de gestion du risque de sécurité numérique propose une approche systématique permettant de prendre en considération et de prévenir les effets négatifs potentiels des mesures de sécurité à l'aide d'outils et de procédés adaptés.

Les mesures de sécurité, appelées aussi parfois « mécanismes », « contrôles » ou « garanties », peuvent être de nature très différente : numérique (par ex. un logiciel de sécurité), physique (par ex. des cadenas, caméras, et clôtures) ou hybride (par ex. une carte à puce) ; s'appliquer aux personnes (par ex. une formation), aux processus (par ex. des règles ou pratiques en matière d'organisation) ou aux technologies (par ex. la cryptographie) ; être d'ordre juridique (par ex. un contrat), procédural (par ex. des normes) ou administratif, etc. Ce ne sont ici que quelques exemples de classifications envisageables.

Les mesures de sécurité visent également à traiter les vulnérabilités. Tout comme les menaces, les vulnérabilités évoluent en permanence dans l'environnement numérique. Les organisations devraient par conséquent rechercher continuellement les vulnérabilités, les évaluer et y apporter une réponse appropriée dans les plus brefs délais afin de conserver une longueur d'avance sur les menaces nouvelles ou émergentes.

Le risque étant par nature dynamique, les mesures de sécurité devraient être choisies au moment de la planification de l'activité et mises à jour tout au long de son cycle de vie, suivant l'approche cyclique, holistique et systématique décrite précédemment. Certaines de ces mesures devraient faire partie intégrante de l'activité dès sa conception, c'est-à-dire en être une composante essentielle du fait, par exemple, qu'elles sont indispensable ou qu'elles visent un pan de cette activité qui ne pourra pas être modifié ultérieurement. Le risque ayant toutefois un caractère dynamique, d'autres mesures de sécurité devraient être introduite tout au long du cycle continu d'évaluation et de gestion du risque.

Les parties prenantes qui interviennent dans la conception, la gestion et le fonctionnement de l'environnement numérique devraient toujours se conformer aux bonnes pratiques et appliquer les normes en vigueur en ce qui concerne les mesures de sécurité. De nombreuses normes et bonnes pratiques à caractère général ou sectoriel peuvent s'appliquer aux mesures de sécurité. La mise en œuvre de ces normes aide en règle générale à traiter certains aspects communs de la gestion du risque, ce qui permet de libérer du temps et des ressources pour des problèmes spécifiques à l'organisation ou à l'activité.

Les parties prenantes qui développent et tiennent à jour des produits et services informatiques devraient y intégrer des mesures de sécurité et fournir à leurs clients les renseignements et, s'il y a lieu, l'assistance dont ils ont besoin pour évaluer et traiter les risques liés à l'utilisation de ces biens et services.

7. Innovation

En plus de l'adoption de mesures de sécurité, les parties prenantes peuvent réduire leur exposition au risque de sécurité numérique par l'innovation, que celle-ci intéresse l'activité concernée ou les mesures de sécurité. L'innovation est généralement définie comme la mise en place d'un produit (bien ou service) ou d'un procédé (mode de production ou de fourniture) nouveau ou sensiblement amélioré, d'une nouvelle méthode de commercialisation ou d'une nouvelle méthode organisationnelle dans les pratiques de l'entreprise, l'organisation du lieu de travail ou les relations extérieures.[46]

Dans le contexte de la gestion du risque de sécurité numérique, l'innovation aux fins de la réduction du risque peut prendre des formes très diverses,

touchant ou non aux aspects numériques. Elle peut par exemple porter sur le modèle économique ou d'activité de l'organisation, ses processus (comme les méthodes de paiement), voire même entraîner la redéfinition de composantes non numériques – physiques, juridiques ou autres – d'un produit. L'introduction d'une innovation destinée à réduire l'effet possible de l'incertitude sur une activité peut elle-même créer des incertitudes sur d'autres aspects de cette activité. Elle devrait par conséquent donner lieu à un nouveau cycle d'évaluation et de traitement du risque.

La gestion du risque de sécurité numérique peut donc devenir un moteur d'innovation pour autant qu'elle soit considérée comme faisant partie intégrante des processus décisionnels concernant une activité donnée. Lorsque les décisions relatives à la gestion du risque de sécurité sont dissociées du processus de prise de décisions économiques et sociales, il est plus difficile de leur reconnaître un tel potentiel. Elles peuvent au contraire apparaître comme des inhibiteurs ou des contraintes subies davantage que comme un stimulant pour l'avantage concurrentiel.

Le fait est que risque, innovation et progrès économique et social sont intimement liés. On s'aperçoit ainsi que bon nombre des inventions et des avancées de l'humanité au fil de l'histoire procèdent de la volonté ou de la nécessité de gérer l'incertitude : ainsi, si elle a certainement déterminé l'invention du parapluie, l'incertitude climatique a aussi suscité des progrès considérables dans l'agriculture de même que dans le stockage, le traitement et la distribution des denrées alimentaires pour réduire le risque de famine. Il serait opportun de chercher à mieux comprendre le lien entre risque et innovation dans l'environnement numérique.

De ce point de vue, il est possible également de donner du Principe une interprétation plus large, tendant à reconnaître que la gestion du risque peut être considérée comme une approche générale, à la fois pour préserver la valeur et la créer. La gestion du risque permet aux organisations de faire face aux incertitudes de manière systématique afin d'accroître leurs chances de succès dans un environnement en perpétuelle mutation. Cependant, comme on l'a vu, l'effet de l'incertitude sur une activité n'est pas nécessairement préjudiciable à celle-ci. Le risque a ses bons et ses mauvais côtés : les incertitudes peuvent être l'occasion

d'améliorer l'activité en jeu comme elles peuvent lui nuire. Si l'on voit le risque et les opportunités comme les deux faces de la même pièce en matière de décision, la gestion du risque peut s'apparenter à un cycle dans lequel : i) le « risque négatif » est évalué en même temps que le « risque positif » (les opportunités) ; ii) le traitement du risque consiste à décider comment ramener le premier au niveau acceptable mais aussi comment tirer parti du second – et donc saisir les opportunités qui se présentent – de manière à réaliser au mieux les objectifs visés. L'intégration de ces deux aspects dans un même cadre cyclique, holistique et systématique est à même d'accroître la souplesse et la faculté d'adaptation d'une organisation, de rendre celle-ci plus compétitive et de faciliter l'innovation.

Cette manière d'appréhender la gestion du risque est relativement nouvelle[47] et des travaux plus poussés seraient nécessaires là aussi pour mieux en comprendre les avantages potentiels ainsi que les obstacles à sa généralisation, notamment au regard de la gestion du risque numérique. Cela explique que la Recommandation traite du risque en ce qu'il suppose de préjudiciable, comme en témoignent les termes employés pour décrire les facteurs de risque (par ex. menaces, vulnérabilités et incidents) ainsi que la terminologie relative à la « sécurité » (par ex. confidentialité, intégrité, disponibilité), qui relève du domaine de la protection. Néanmoins, le Principe d'innovation souligne que l'on peut aussi voir dans la gestion du risque de sécurité numérique un moyen d'exploiter les opportunités qui se présentent et de favoriser ainsi l'innovation.

8. Préparation et continuité

À l'origine de la gestion du risque de sécurité numérique, il y a le constat qu'il est impossible d'offrir un environnement numérique entièrement « sûr et sécurisé » dans lequel les incidents sont toujours évités. Des incidents peuvent survenir et affecter les activités économiques et sociales quand bien même des mesures de sécurité rigoureuses sont appliquées et gérées comme il se doit. C'est pourquoi la gestion du risque numérique ne se limite pas au déploiement de mesures de sécurité et à l'innovation. Elle devrait comprendre également l'élaboration d'un plan de préparation et de continuité pour définir à l'avance les mécanismes qui permettront d'atténuer le risque en cas d'incident, en limitant les effets préjudiciables sur les activités économiques et sociales et en favorisant la continuité et la résilience de celles-ci.

Tout plan de préparation et de continuité devrait prendre en considération la vitesse à laquelle les incidents peuvent se propager et s'aggraver dans l'environnement numérique. On distingue généralement les niveaux d'escalade en fonction de la nature et de l'ampleur des conséquences sur les activités et objectifs économiques et sociaux en jeu. Différentes échelles peuvent ainsi être définies, par exemple : Alerte (impact nul), Incident (impact uniquement sur l'informatique), Urgence (impact économique et social limité) et Crise (impact menaçant la survie de l'organisation). Il est possible d'employer d'autres termes et gradations selon le contexte. À titre d'exemple, les pouvoirs publics peuvent envisager l'impact sur une organisation donnée, sur le secteur dont celle-ci relève, sur l'économie nationale dans son ensemble et au-delà des frontières du pays. L'attribution des responsabilités devrait être différente pour chaque niveau d'escalade de sorte que le risque soit correctement géré en cas d'incident. La coopération joue là encore un rôle central pour garantir que tant les effets économiques et sociaux d'un incident que ses aspects techniques sont bien compris des décideurs.

Un plan de préparation devrait couvrir la prévention et la détection des incidents de sécurité numérique, la réponse à ceux-ci et la reprise des activités. Il devrait également prévoir à la fois des interventions individuelles et des actions concertées, comme l'échange d'informations pertinentes avec d'autres parties prenantes, notamment entre les secteurs public et privé et par-delà les frontières nationales. Il convient de le tester, de l'évaluer et de le réviser en boucle, compte tenu de la nature dynamique du risque. Les équipes de réponse aux incidents de sécurité informatique (CSIRT), appelées également équipes d'intervention en cas d'urgence informatique (CERT) peuvent apporter une aide précieuse aux parties prenantes face à certains incidents de sécurité numérique. Les décideurs pourraient tirer avantage d'indicateurs statistiques comparables au plan international rendant compte de l'activité des CSIRT/CERT pour se faire une idée plus précise du niveau général de risque.

Enfin, des procédures de notification appropriées seraient à envisager dans le cadre de la mise en œuvre du plan de préparation. La notification peut être facultative dans certains cas et relever d'une obligation légale dans d'autres.

Annexe
Domaines de travail à envisager pour l'avenir

Les travaux futurs pourraient porter sur les domaines suivants :

- La gouvernance de la gestion du risque de sécurité numérique dans les organisations : une question technique devenue une priorité pour les dirigeants ;
- La gestion du risque au service de la vie privée : tirer des leçons de la gestion du risque de sécurité numérique pour une meilleure mise en œuvre des Lignes directrices de l'OCDE sur la vie privée. Explorer les points communs, les différences et les synergies entre la gestion du risque de sécurité numérique et de vie privée, ainsi que les opportunités pour un cadre commun ;
- Le lien entre innovation et gestion du risque de sécurité numérique ; faisabilité, avantages et inconvénients de l'application d'une approche de gestion des questions de sécurité numérique axée sur le risque et les opportunités (gestion du risque aux fins de la protection et de la création de valeur) ;
- L'assurance en matière de gestion du risque de sécurité numérique : perspectives et enjeux ;
- L'interprétation des Principes pour les PME et les individus ;
- Le contrôle dans le domaine de la gestion du risque numérique ;
- Orientations pour l'action des pouvoirs publics visée dans la Section 2 de la Recommandation ;
- La coopération internationale et les économies en développement ;
- Améliorer les indicateurs sur le risque de sécurité numérique.

Bibliographie

ACMA (Australian Communications and Media Authority) (2011), *An overview of international cyber-security awareness raising and educational initiatives*, www.acma.gov.au/theACMA/an-overview-of-international-cyber-security-awareness-raising-and-educational-initiatives.

Angwin, J. (2015), *The World's Email Encryption Software Relies on One Guy, Who is Going Broke*, www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke.

App Promo (2013), « App Promo White Paper – Slow and steady win the race: App Developers That Stick it Out Come Out on Top » – App Promo Developer Survey June 2013, http://app-promo.com/wp-content/uploads/2013/06/SlowSteady-AppPromo-WhitePaper2013.pdf (consulté le 25 août 2015).

App Promo (2012), « Wake Up Call – If You Spend It, They Will Come », http://app-promo.com/wake-up-call-infographic/ (consulté le 25 août 2015).

Ashford, W. (2013), *Targeted cyber espionage on the increase, McAfee warns*, www.computerweekly.com/news/2240185167/Targeted-cyber-espionage-on-the-increase-McAfee-warns.

Aven, T. (2012), « The risk concept—historical and recent development trends » dans *Reliability Engineering & System Safety*, vol. 99, mars 2012, pp. 33–44, http://dx.doi.org/10.1016/j.ress.2011.11.006.

CBC News (2012), « Nortel collapse linked to Chinese hackers », www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591 (consulté le 25 août 2015).

Choe, S. (2014), « Theft of Data Fuels Worries in South Korea », *New York Times*, www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html (consulté le 25 août 2015).

CIGI (Centre pour l'innovation dans la gouvernance internationale) (2014), résultats de l'enquête mondiale *CIGI-Ipsos sur la sécurité et la confiance liées à l'Internet*, https://www.cigionline.org/internet-survey (consulté le 25 août 2015).

CNIL (Commission Nationale de l'Informatique et des Libertés), (2012), *Gérer les risques sur les libertés et la vie privée*, la méthode, www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf.

Conseil de l'Europe (2001), *Convention sur la cybercriminalité*, http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm.

Dark Reading (2012), « 4 Long-Term Hacks That Rocked 2012 », www.darkreading.com/application-security/database-security/4-long-term-hacks-that-rocked-2012/d/d-id/1138643 (consulté le 25 août 2015).

ENISA (Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information) (2013), *National Cyber Security Strategies in the World*, www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (consulté le 25 août 2015).

ENISA (non daté), « Existing Taxonomies », www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies (consulté le 25 août 2015).

Europol (2013), *Notorious Botnet Infecting 2 Million Computers Disrupted*, www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted-0 (consulté le 25 août 2015).

Fechner, B. (2014), *Les entreprises françaises face au défi de l'espionnage industriel*, http://lexpansion.lexpress.fr/actualite-economique/les-entreprises-francaises-peuvent-elles-relever-le-defi-de-l-espionnage-industriel_1633978.html (consulté le 25 août 2015).

Gaudiosi, J. (2014), « Why Sony didn't learn from its 2011 hack? », http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/ (consulté le 25 août 2015).

ISOC (Internet Society) (2015), *Collaborative Security: An approach to tackling Internet Security issues*, www.internetsociety.org/collaborativesecurity.

Jackson, W. (2014), « Cyber Espionage Incidents Triple: Verizon Report », www.informationweek.com/government/cybersecurity/cyber-espionage-incidents-triple-verizon-report/d/d-id/1204612 (consulté le 25 août 2015).

Kim, Y. (2014), « Top executives resign over massive data leak », www.koreaherald.com/view.php?ud=20140120001002 (consulté le 25 août 2015).

Kitten, T. (2014), « Chase's Cybersecurity Budget to Double », www.bankinfosecurity.com/chases-cybersecurity-budget-to-double-a-7427 (consulté le 25 août 2015).

Lee, R., M. Assante, et T. Conway, (2014), *German Steel Mill Cyber Attack*, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Leyden, J. (2013), « Biggest DDoS attack in history hammers Spamhaus », www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood (consulté le 25 août 2015).

Molla, R. (2012), « Most app developers make less than $500 a month », https://gigaom.com/2012/10/04/most-app-developers-make-less-than-500-a-month-chart/ (consulté le 25 août 2015).

NACD (National Association of Corporate Directors), (2014), *NACD Reports Directors Dissatisfied with Cyber and IT Risk Information*, www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=12530 (consulté le 25 août 2015).

Nations Unies (2013), *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=F.

Nations Unies (2003), *Création d'une culture mondiale de la cybersécurité, Résolution adoptée par l'Assemblée générale, A/RES/57/239*, www.un.org/fr/ga/search/ view_doc.asp?symbol=A/RES/57/239.

Nations Unies (1966a), *Pacte international relatif aux droits civils et politiques*, www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx.

Nations Unies (1966b), *Pacte international relatif aux droits économiques, sociaux et culturels*, www.ohchr.org/FR/ProfessionalInterest/Pages/CESCR.aspx.

Nations Unies (1948), *Déclaration universelle des droits de l'homme*, http://www.un.org/fr/documents/udhr/.

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST (National Institute of Standards and Technology), (2012), *Guide for conducting risk assessment, NIST Special publication 800-30, rév. 1*, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

O'Connor, C. (2014), « Target CEO Gregg Steinhafel Resigns in Data Breach Fallout », www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout (consulté le 25 août 2015).

OCDE (Organisation de Coopération et de développement économiques) (2014), *Recommandation sur les stratégies numériques gouvernementales*, http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=306&Instrument PID=326&Lang=fr&Book=False.

OCDE (2013a), *ICTs and the Health Sector: Towards Smarter Health and Wellness Models*, Éditions OCDE, Paris, http://dx.doi.org/10.1787/9789264202863-en.

OCDE (2013b), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=fr&Book=False.

OCDE (2012a), *Connected Minds: Technology and Today's Learners, La recherche et l'innovation dans l'enseignement*, Éditions OCDE, Paris, http://dx.doi.org/10.1787/9789264111011-en.

OCDE (2012b), « ICT Applications for the Smart Grid: Opportunities and Policy Implications », *OECD Digital Economy Papers*, no 190, Éditions OCDE, Paris, http://dx.doi.org/10.1787/5k9h2q8v9bln-en.

OCDE (2012c), « Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online », *OECD Digital Economy Papers*, no 214, Éditions OCDE, Paris, http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OCDE (2012d), « Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy », *OECD Digital Economy Papers*, no 211, Éditions OCDE, Paris, http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OCDE (2011), *Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet*, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView. aspx?InstrumentID=270&InstrumentPID=275.

OCDE (2008), *Recommandation du Conseil sur la protection des infrastructures d'information critiques*, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView. aspx?InstrumentID=121&Lang=fr&Book=False.

OCDE (2002), *Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité*, www.oecd.org/internet/ieconomy/15582260.pdf.

OCDE et Eurostat (2005), *Manuel d'Oslo : Principes directeurs pour le recueil et l'interprétation des données sur l'innovation, 3e édition, La mesure des activités scientifiques et technologiques*, Éditions OCDE, Paris, http://dx.doi.org/10.1787/9789264292260-fr.

OSCE (Organisation pour la sécurité et la coopération en Europe) (2013), *Série initiale de mesures de confiance de l'OSCE visant à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication, Décision no 1106 du Conseil permanent*, www.osce.org/fr/pc/109641?download=true.

Peters, S. (2014), « Pharmaceuticals, Not Energy, May Have Been True Target of Dragonfly, Energetic Bear », www.darkreading.com/pharmaceuticals-not-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869 (consulté le 25 août 2015).

Piper, A. (2014), « Risk-informed innovation: Harnessing risk management in the service of innovation, The Economist Intelligence Unit », www.economistinsights.com/technology-innovation/analysis/risk-informed-innovation (consulté le 25 août 2015).

Prince, B. (2014), « Incident Response Plans Lacking in Many Organizations: Survey », www.securityweek.com/incident-response-plans-lacking-many-organizations-survey (consulté le 25 août 2015).

Rawlinson, K. (2015), « Charlie Hebdo: 'Islamist cyber attacks' hit France », www.bbc.com/news/technology-30850702 (consulté le 25 août 2015).

SecurEnvoy (2012), « The RSA Security breach – 12 months down the technology turnpike », www.securenvoy.com/blog/2012/04/27/the-rsa-security-breach-12-months-down-the-technology-turnpike/ (consulté le 25 août 2015).

Westby, J. (2012), *Governance of Enterprise Security: CyLab 2012 Report – How Boards & Senior Executives Are Managing Cyber Risks*, http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

Yadron, D. (2014), « Internet Security Relies on Very Few », www.wsj.com/news/articles/SB10001424052702303873604579495362672447986 (consulté le 25 août 2015).

Notes

1. C'est le cas par exemple de l'énergie (voir OCDE, 2012b), des transports, des activités manufacturières, etc.
2. Voir OCDE, 2013a.
3. Voir OCDE, 2012a.
4. Voir www.oecd.org/fr/apropos/quifaitquoi/.
5. Voir www.oecd.org/fr/sti/ieconomie/.
6. Voir www.oecd.org/fr/juridique/instruments-juridiques.htm.
7. Représentés respectivement par le Comité consultatif économique et industriel auprès de l'OCDE (BIAC), le Comité consultatif de la société civile sur la société de l'information auprès de l'OCDE (CSISAC) et le Comité consultatif technique sur l'Internet (ITAC).
8. Par exemple, la précédente Recommandation (les Lignes directrices sur la sécurité de 2002) est citée dans la norme ISO 27001:2002 et a inspiré la Résolution 57/239 des Nations Unies (Nations Unies, 2003).
9. Conseil de l'Europe, 2001. Voir également le Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC) à l'adresse www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp.
10. Voir www.interpol.int/fr/Crime-areas/Cybercrime/Cybercrime.
11. Voir, par exemple, Nations Unies, 2013.
12. Voir OSCE, 2013.
13. En particulier via le Groupe de Travail sur les Télécommunications et l'Information (APEC TEL).
14. Par exemple local, régional, provincial, fédéral, etc. Voir plus loin les explications concernant « les parties prenantes et leurs rôles ».
15. Voir la partie « Applicabilité des Principes » pour plus de précisions sur les notions de rôle, de capacité à agir et de contexte.
16. CNIL, 2012, p. 12.
17. Ashford, 2013; Feshner, 2014; et Jackson, 2014.
18. Voir notamment Dark Reading, 2012, qui cite des exemples d'attaques à long terme contre la Chambre de commerce des États-Unis, Nortel, Coca-Cola et le ministère des finances du Japon. La faillite de Nortel pourrait avoir été la conséquence du cyberespionnage dont l'entreprise a été victime et, en particulier, de 10 années d'intrusion furtive dans son système informatique. Voir CBC News, 2012.

19. Voir, par exemple, Europol, 2013.

20. Voir OCDE, 2012d et ENISA, 2013.

21. Une enquête réalisée en 2012 auprès de 108 collaborateurs d'entreprises du Forbes Global 2000 a révélé que 57 % des sondés n'analysent pas l'adéquation de leur assurance contre les risques numériques ou ne mènent pas d'activités clés susceptibles de les aider à gérer les risques d'atteinte à la notoriété et les risques financiers associés au vol de données confidentielles et propriétaires et aux violations de sécurité. Westby, 2012. Voir également NACD, 2014 et Prince, 2014.

22. CIGI, 2014 : 78 % des utilisateurs sont préoccupés par le risque de piratage de leurs comptes bancaires personnels. 77 % des utilisateurs craignent qu'une personne ne pirate leurs comptes en ligne et ne dérobe leurs données personnelles. 72 % des utilisateurs sont préoccupés par le risque de voir les institutions de leur pays être la cible d'une cyberattaque émanant d'un gouvernement étranger ou d'une organisation terroriste.

23. Il existe de nombreuses normes et méthodologies basées sur les risques, émanant de divers organismes nationaux, régionaux et internationaux, gouvernementaux ou non, suivant une approche générale ou sectorielle (finances, administration publique, etc.). L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) en recense 17, consultables à l'adresse http://rm-inv.enisa.europa.eu/methods. À cette liste non exhaustive s'ajoutent, notamment, le Guide for conducting risk assessment (NIST, 2012) et le cadre Cybersecurity Framework (NIST, 2014) du NIST. Les normes reflètent souvent des perspectives particulières, ciblent des publics différents et utilisent des termes et des définitions divers, sans nécessairement être incohérentes avec la Recommandation. Par exemple, l'expression « traitement du risque » peut correspondre à ce que certaines normes appellent « atténuation du risque » ; des normes évoquent la « réduction du risque » là où d'autres préfèrent « atténuation du risque ». Il en va de même pour « évitement du risque » et « suppression du risque », « vulnérabilité » et « faiblesse », etc.

24. Il peut y avoir des recoupements, lorsque la violation des droits de propriété intellectuelle est consécutive à un incident de sécurité, par exemple, en cas d'intrusion dans le système informatique d'une organisation en vue de dérober un secret industriel ou commercial, ou de diffusion de contenu illégal (tel que des propos haineux) via la défiguration d'un site Internet.

25. Par exemple, dans l'affirmation « si vous traversez la rue, vous courez le risque d'être renversé par une voiture », l'accent est mis sur un événement ou un incident ; en revanche, lorsque l'on dit « les voitures représentent un risque pour les piétons qui traversent la rue », on insiste sur la menace ou le danger ; enfin, la formulation « si vous ne prêtez pas attention lorsque vous traversez la rue, vous risquez de mourir » met en évidence la conséquence de l'incident.

26. Le terme « professionnels des TIC » peut inclure des parties prenantes individuelles dont l'activité principale n'est pas liée aux TIC, comme c'est le cas de nombreux développeurs d'applications mobiles (« apps »).

27. Pour certains problèmes techniquement complexes, il arrive que le risque puisse être réduit mais non de telle sorte qu'il soit possible d'en confier le contrôle aux individus. C'est par exemple le cas avec les services en réseau ou autres services à distance, pour lesquels les solutions de sécurité seront appliquées de manière centralisée.

28. SecurEnvoy, 2012.

29. Le marché s'entend ici au sens large comme l'espace ou l'offre et la demande se rencontrent, y compris en ce qui concerne les logiciels gratuits ou libres.

30. Voir Angwin, 2015 et Yadron, 2014.

31. 68 % des personnes interrogées déclarent avoir perçu moins de 1 000 USD de revenus depuis le lancement de leurs applications, tandis que 29 % des sondés indiquent n'avoir généré aucun revenu (App Promo, 2013). La plupart des développeurs d'applications gagnent moins de 500 USD par mois (Molla, 2012). Voir également App Promo, 2012.

32. Voir VI : [Le Conseil] « Convient que les Principes sont complémentaires et doivent être pris comme un tout ».

33. Par exemple, un ordinateur ou un équipement infecté peut être utilisé pour attaquer les actifs d'autrui (dans le cadre d'attaques par déni de service distribué, par exemple) ; de même, outre l'atteinte aux intérêts économiques de l'organisation victime d'un incident, la divulgation de données à caractère personnel suite à une violation de sécurité peut avoir des incidences sur la vie des personnes dont les données ont été dérobées.

34. Pour une analyse comparative internationale des initiatives, voir ACMA, 2011.

35. OCDE, 2012d.

36. Le dixième paragraphe du préambule de la Recommandation (« Conscient …») souligne que les parties prenantes partagent la responsabilité de la protection de l'environnement numérique. Pour de plus amples informations au sujet de la notion de « responsabilité collective », voir ISOC, 2015.

37. Nations Unies, 1948, 1966a et 1966b.

38. Il importe de souligner que la Recommandation utilise l'expression « mesures de sécurité » pour désigner les mesures prises dans le cadre de la gestion du risque de sécurité numérique. Les autres types de mesures de sécurité sortent du champ d'application.

39. Le Communiqué expliquant les principes contenus dans la Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet de 2011 (OCDE, 2011) indique : « […] Il importe sans conteste de préserver le car-

actère ouvert et accessible de l'Internet afin de garantir la liberté d'expression, de faciliter les échanges licites d'informations, de connaissances et d'opinions entre internautes et de soutenir une recherche et un développement auxquels nous devons tant d'innovations aujourd'hui largement présentes dans nos économies […] ». La Recommandation de 2011 elle-même recommande que, « dans l'élaboration ou la révision de leurs politiques à l'égard de l'économie Internet, les Membres, en coopération avec l'ensemble des parties prenantes, prennent en compte les principes de base suivants[:] […] « Assurer la transparence, l'égalité de traitement et l'imputabilité des actes ». Sur ce dernier point, le Communiqué explique encore que « pour renforcer la confiance du public dans l'environnement Internet, il conviendrait d'encourager des processus d'élaboration des politiques et des orientations essentielles assurant la transparence, l'égalité de traitement et l'imputabilité des actes. La transparence garantit que les internautes disposent d'informations à jour, accessibles et exploitables adaptées à leurs droits et à leurs centres d'intérêt. L'égalité de traitement assure des procédures de prise de décision prévisibles régissant la définition, la revendication et la défense des droits. L'imputabilité est assurée par des politiques qui rendent les parties redevables de leurs actes sur l'Internet lorsque les circonstances l'exigent. […] »

40. OCDE 2013b, troisième partie, paragraphe 15 a).

41. Les Lignes directrices de 2002 sur la sécurité présentent la coopération comme un concept utile. La Recommandation en fait un Principe à part entière, soulignant ainsi sa pertinence accrue et son rôle essentiel à l'appui des autres Principes.

42. Le consortium coréen de CERT, CONCERT, en offre un exemple intéressant. Créé en 1996, il a pour mission de favoriser l'échange et le partage d'informations, ainsi que la coopération avec les partenaires sur des questions d'intérêt commun liées à la sécurité. Il regroupe plus de 300 unités chargées de la sécurité de l'information dans les entreprises, ainsi que les instituts et autorités concernés en Corée. Voir www.concert.or.kr.

43. À l'instar du partenariat britannique Cyber-security Information Sharing Partnership (CiSP). Voir www.cert.gov.uk/cisp.

44. Dans l'expression « public-privé », le terme « privé » désigne les parties prenantes qui n'appartiennent pas au secteur public, comme les entreprises, les organisations sans but lucratif, les organisations de la société civile, les milieux universitaires, la communauté technique, etc.

45. Le « traitement » du risque est parfois appelé différemment, « atténuation » du risque par exemple. On se reportera à l'encadré consacré à la terminologie et aux définitions. Parmi les autres termes connexes, citons l'acceptation ou prise de risque, sa réduction, atténuation ou minimisation, son transfert ou reallocation, son évitement ou sa suppression.

46. OCDE/Eurostat, 2005.

47. Piper, 2014.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements oeuvrent ensemble pour relever les défis économiques, sociaux et environnementaux liés à la mondialisation. À l'avant-garde des efforts engagés pour comprendre les évolutions du monde actuel et les préoccupations qu'elles suscitent, l'OCDE aide les gouvernements à y faire face en menant une réflexion sur des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et la problématique du vieillissement démographique. L'Organisation offre aux gouvernements un cadre leur permettant de confronter leurs expériences en matière d'action publique, de chercher des réponses à des problèmes communs, de recenser 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 Corée, 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, 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 laTurquie. La Commisssion européenne participe aux travaux de l'OCDE.

Les Éditions OCDE assurent une large diffusion aux travaux de l'Organisation. Ces derniers comprennent les résultats de l'activité de collecte de statistiques, les travaux de recherche menés sur des questions économiques, sociales et environnementales, ainsi que les conventions, les principes directeurs et les modèles développés par les pays membres.

La gestion du risque de sécurité numérique pour la prospérité économique et sociale

RECOMMENDATION DE L'OCDE ET DOCUMENT D'ACCOMPAGNEMENT

Les menaces de sécurité numérique potentiellement lourdes de conséquences économiques sont récemment devenues plus nombreuses et sophistiquées, alors même que l'environnement numérique est devenu un maillon essentiel du fonctionnement de l'économie et un facteur important de croissance, de bien-être et d'inclusivité. Pour profiter pleinement des avantages liés à l'environnement numérique, les parties prenantes doivent absolument cesser d'aborder le risque de sécurité numérique sous un angle technique dissocié de considérations économiques et sociales plus larges. Il leur faut d'urgence intégrer la gestion de ce risque à leurs processus décisionnels en matière économique et sociale. Les responsables de l'action publique doivent également mesurer toute la complexité du risque de sécurité numérique dans ses multiples dimensions, de la prospérité économique et sociale aux activités de police (lutte contre la « cybercriminalité ») en passant par la défense, la sécurité nationale et la sécurité internationale.

Cette Recommandation de l'OCDE et son Document d'Accompagnement offrent des orientations sur ces aspects.

Partie I. Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale

Partie II. Document d'accompagnement de la Recommandation du Conseil de l'OCDE sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale

éditionsOCDE
www.oecd.org/editions

ISBN 978-92-64-24609-6
93 2015 05 2 P