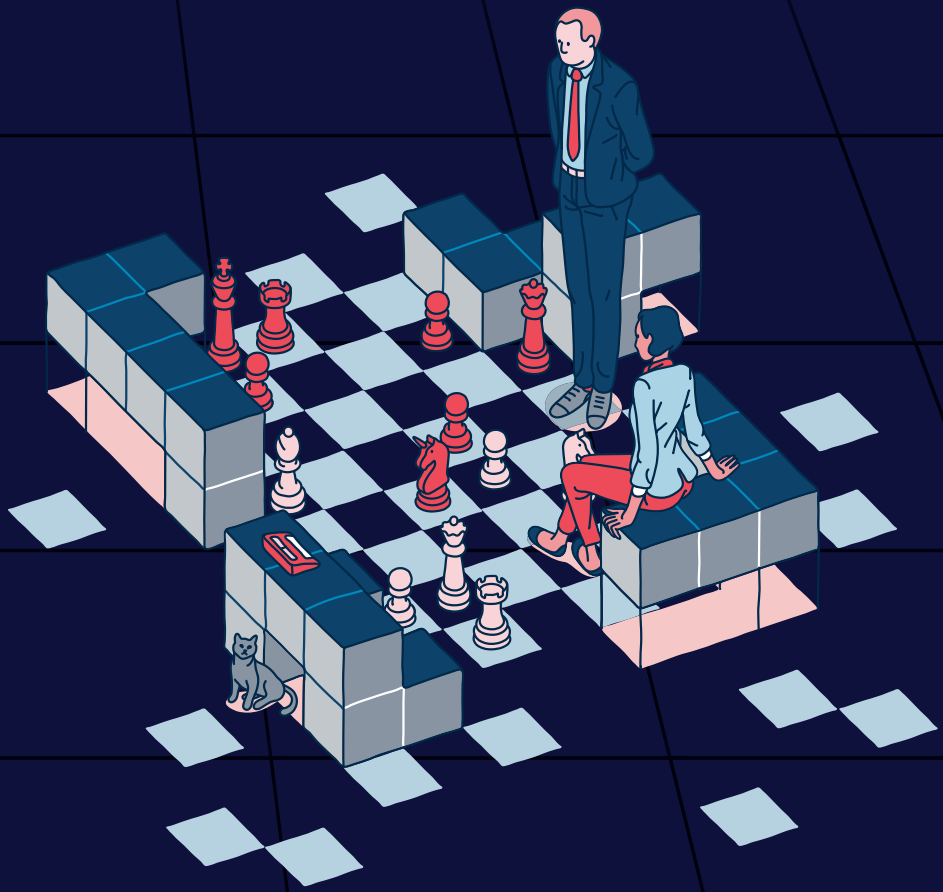
MAÎTRISE DU RISQUE NUMÉRIQUE

L'ATOUT CONFIANCE



AMRAE

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

MAÎTRISE DU RISQUE NUMÉRIQUE

L'ATOUT CONFIANCE

TABLE DES MATIÈRES

PRÉFACE

Pour quelles raisons l'AMRAE et l'ANSSI ont-elles décidé de prendre la plume ensemble ?

Brigitte Bouquot : Nous bâtissons depuis plusieurs années une relation de confiance dont j'apprécie les fruits : nos angles de vue sur le risque sont très complémentaires, celui de l'AMRAE économique au cœur de la gouvernance de l'Entreprise, celui de l'ANSSI technique au cœur des enjeux normatifs (de la sécurité) de l'État. Et c'est la clé pour apporter des réponses complètes aux questions que pose le développement de l'économie numérique dans le cyber espace. Seule une approche holistique permet de progresser dans la maîtrise des risques et la définition de standards pour les Entreprises. Le présent guide est donc la traduction concrète du sens que nous conférons à ce partenariat. On dit souvent que l'on doit se transformer pour ne pas disparaître, c'est particulièrement vrai en matière de risque numérique ! L'Entreprise doit le prendre, mais elle doit aussi déployer une politique de gestion des risques pour le maîtriser. Il en va de notre responsabilité à tous de nous emparer du sujet sans plus attendre. Demain, l'entreprise responsable et génératrice de confiance sera celle qui s'attache à maîtriser le risque numérique. Et si, plus que de contrainte, nous parlions d'avantage compétitif ?

Guillaume Poupard : On a plein de bonnes raisons de travailler ensemble ! Nous partageons en effet une ambition commune, mais nos connaissances et nos expériences sont complémentaires. Cela nous permet de nous enrichir mutuellement. C'est extrêmement précieux et j'en perçois pleinement les bénéfices en matière d'accompagnement et de dialogue avec nos propres bénéficiaires. Car c'est une réalité, nous parlons des langages différents et nous n'avons pas la même expérience du risque numérique. Ce guide est donc le fruit d'un travail d'équipe soutenu et passionné de la part de nos collaborateurs respectifs. Ils se sont, d'une certaine manière, glissés dans la peau de la cible sans jamais cesser de la consulter, pour répondre à ses préoccupations et lui permettre d'entrevoir toutes les perspectives d'un investissement dans la sécurité numérique, à plus ou moins long terme.

Le risque numérique appartient-il toujours à la catégorie des « nouvelles menaces » ou est-il devenu un incontournable ?

Brigitte Bouquot : Le risque numérique est vraiment devenu incontournable, mais nous avons encore du chemin à parcourir pour le maitriser ! Les décideurs, éclairés par les risk managers, en ont bien pris la mesure et le mettent progressivement au centre de la politique globale de gestion des risques. Mais c'est un écosystème bien plus vaste, industrie par industrie, qui doit s'organiser pour mieux l'appréhender. Je pense en particulier aux assurances dont l'offre se précise et s'étoffe. Le transfert à l'Assurance joue un rôle non négligeable dans l'engagement du dirigeant et dans la bonne résilience de l'organisation, qu'elle soit petite ou grande. Mais pour être durable, il suppose que l'entreprise connaisse mieux son risque numérique.

Guillaume Poupard : Les technologies numériques sont devenues des compagnons de tous les jours, au travail comme dans la vie. Elles sont une incontestable source d'opportunités, mais avec elles se développent de nouvelles menaces, toujours plus sophistiquées et destructrices. Cet état de fait pousse les organisations à se repenser et à appréhender le risque qui pèse sur elles dans une logique d'amélioration continue. Ai-je encore besoin de rappeler que le risque zéro n'existe pas ? Sans doute, car une cyberattaque peut rapidement mettre en péril la survie de l'organisation qui la subit ou, sans aller jusque-là, nuire gravement et durablement à son image et à la confiance qu'on lui accorde. Impossible donc d'ignorer ces enjeux et les réponses que nous tentons d'y apporter pour accompagner avec réalisme chaque acteur dans cette démarche, quels que soient son activité, la criticité de celle-ci, son niveau de maturité ou ses moyens.

Brigitte BOUQUOT, présidente de l'AMRAE
Guillaume POUPARD, directeur général de l'ANSSI

INTRODUCTION

Ce guide est né du constat suivant : le risque numérique qui pèse chaque jour davantage sur les organisations peut aller jusqu'à mettre en péril leur survie et celle de leurs parties prenantes. Selon l'ANSSI et l'AMRAE, il doit donc être considéré comme un risque à traiter au plus haut niveau de l'organisation et non plus seulement comme un risque dont l'évitement est l'affaire d'experts techniques.

Ce guide propose aux dirigeants et aux risk managers une démarche progressive pour construire étape par étape une politique de gestion du risque numérique au sein de leur organisation *(cf. Figure 1 – Démarche progressive de construction d'une politique de gestion du risque numérique). Dans le cas où cette politique existe déjà et nécessite d'être consolidée ou réorientée, le lecteur pourra y puiser les conseils et ressources utiles.*

La démarche proposée permet de :

- PRENDRE LA MESURE DU RISQUE NUMÉRIQUE : cette partie permet au lecteur de positionner son organisation dans le contexte de compétition économique au sein duquel elle évolue tout en appréhendant la place du risque numérique dans cette équation. Aujourd'hui, la réponse des organisations face au risque numérique figure parmi les enjeux les plus stratégiques. A l'instar d'autres risques de cette envergure (métier, juridique, commercial, financier, etc.), la gestion du risque numérique nécessite une approche holistique impliquant de nombreuses parties prenantes au sein de l'organisation.

- COMPRENDRE LE RISQUE NUMÉRIQUE ET S'ORGANISER (étapes 1 à 6) : cette partie s'attache à décrire la gouvernance à mettre en œuvre en vue d'initier la construction d'une stratégie de sécurité numérique. A chacune de ces étapes, dirigeants et risk managers auront le souci de valoriser les investissements inhérents à la gestion du risque numérique.

- BÂTIR SON SOCLE DE SÉCURITÉ (étapes 7 à 11) : cette partie introduit les principes de protection, de défense et de résilience appliqués au risque numérique. Y sont également abordés les processus et mesures de sécurité numérique à mettre en œuvre pour décliner la stratégie préalablement définie.

- PILOTER SON RISQUE NUMÉRIQUE ET VALORISER SA CYBERSÉCURITÉ (étapes 12 à 15) : cette partie décrit les mécanismes d'amélioration continue en matière de gestion des risques cyber. Cela comprend également les mécanismes de pilotage de la performance, indispensables à l'organisation pour rester compétitive.

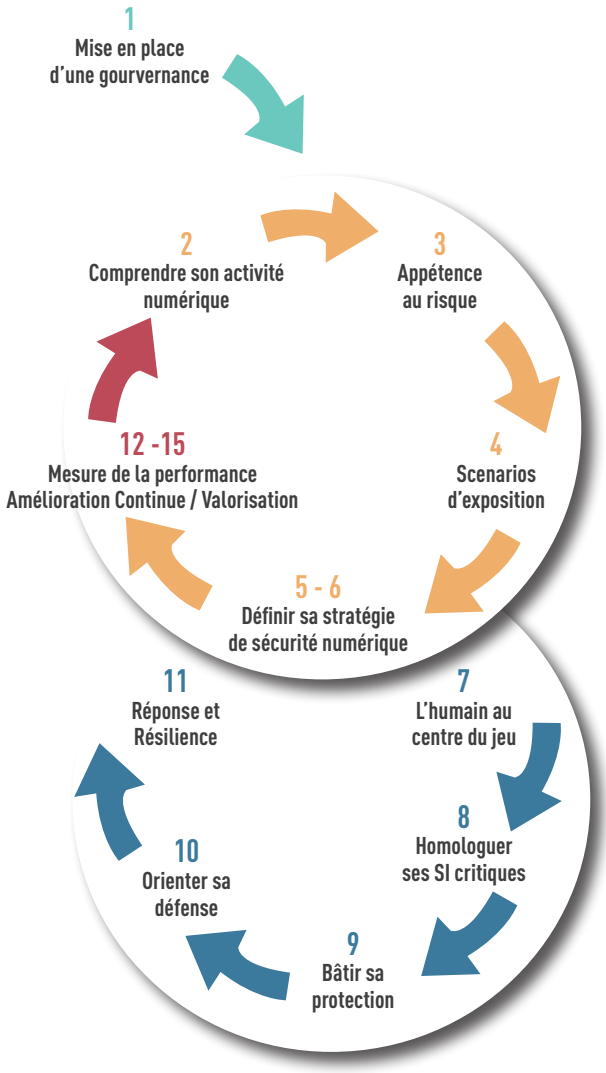


Figure 1 – Démarche progressive de construction d'une politique de gestion du risque numérique

PRENDRE LA MESURE

DU RISQUE NUMÉRIQUE

Manager le risque numérique nécessite de mettre en œuvre une approche holistique faisant appel à tous les acteurs de l'organisation. L'AMRAE décrit cette approche par le concept des « trois lignes de maîtrise[1] ».

Pour être efficace, une politique de management du risque numérique nécessite donc d'être comprise et soutenue par l'ensemble des parties prenantes de l'organisation, à commencer par son dirigeant.

Mondialisation économique et interconnexion

La transformation numérique touche tous les pans de la société (entreprises, administrations, citoyens, etc.) et a donné naissance à un nouvel espace de communication et de partage d'informations : le cyberespace.

Il a pour caractéristique de s'affranchir des frontières traditionnelles entre Etats - qu'elles soient territoriales ou politiques - et renverse la notion d'espace-temps.

Espace de création de valeur mais aussi d'échange et d'affrontement, le cyberespace est devenu le théâtre d'interactions sociales, techniques, économiques, opérationnelles et politiques. Dans cette nouvelle dimension, les règles de la concurrence évoluent et les attaquants redoublent d'ingéniosité pour parvenir à leurs fins. Qu'ils s'agissent d'individus isolés ou de groupes opérant depuis le territoire national ou l'étranger, les attaquants exploitent les nouveaux rapports de force issus de la mondialisation, de l'hypermédiatisation et des nouveaux usages numériques.

Les attaques issues de ces stratégies offensives peuvent profiter des relations de confiance entre parties prenantes (par exemple, une entreprise et son fournisseur) en vue d'impacter de manière imprévisible et fulgurante les organisations. Dans certains cas, ces attaques leur sont fatales.

[1] *Cf. Figure 2 - Les trois lignes de maîtrise, p13*

Le risque numérique, d'un risque technique à un risque d'entreprise

Durant de nombreuses années, les entreprises et collectivités ont mis en œuvre une gestion des risques IT portant sur la seule sécurité de leurs systèmes d'information. Celle-ci se basait sur des critères tels que la confidentialité, l'intégrité et la disponibilité et s'appliquait principalement aux activités transverses ou de support.

Avec la transformation numérique de l'ensemble des acteurs de la société et de leur interconnexion croissante, la gestion des risques IT a progressivement évolué au sein des organisations vers une gestion globale du risque numérique. Ce dernier, au regard du contexte décrit précédemment, pèse de plus en plus fortement sur l'activité des organisations.

Une vision holistique des risques

L'évolution du risque numérique dans l'organisation engage dorénavant la responsabilité du dirigeant vis-à-vis de sa gestion et de son traitement. Cette responsabilité est accentuée par les réglementations actuelles (RGPD[2], NIS[3], LPM[4], etc.).

Devant l'accroissement du risque numérique et sa propension à gagner toutes les activités de l'organisation, les dirigeants doivent définir avec les conseils d'administration et les directions métiers de nouveaux seuils d'acceptabilité du risque (appétence aux risques). Ces risques ne sont pas limités à la seule organisation mais concernent également les parties prenantes de la chaîne de valeur avec lesquelles ils doivent être partagés.

L'évolutivité et la transversalité de cette catégorie de risque obligent dorénavant les dirigeants à reconsidérer leur modèle de gestion des risques de telle sorte que le risque numérique rejoigne les préoccupations stratégiques, économiques ou juridiques des organisations.

Pour acquérir cette vision holistique des risques et veiller à ce qu'ils soient clairement corrélés aux objectifs de l'organisation, qu'elle soit publique ou privée, un comité des risques numériques doit être mis en place. Une attention particulière sera portée à sa capacité à s'affranchir des silos fonctionnels, métiers et opérationnels existants.

[2] Règlement général sur la protection des données (RGPD)
[3] Directive européenne Network and Information Security (NIS)
[4] Loi de programmation militaire (LPM)

COMPRENDRE

LE RISQUE NUMÉRIQUE ET S'ORGANISER

ÉTAPE 1. Définir un cadre de gouvernance du risque numérique

Une bonne gouvernance du risque numérique passe par la mise en place d'un comité dédié et adapté aux réalités de l'organisation.
Son rôle est de définir la stratégie de sécurité numérique de l'organisation, de s'assurer de sa mise en œuvre, de piloter la performance et de valoriser les investissements réalisés.

Définir un cadre de gouvernance du risque numérique

La gouvernance du risque numérique s'inscrit dans une démarche de long terme et doit pouvoir trouver sa place dans le fonctionnement habituel de l'organisation. Elle est pilotée par un comité des risques numériques[5].

L'objectif du comité est de mettre en œuvre la stratégie de sécurité numérique en s'appuyant sur une connaissance actualisée des risques numériques qui pèsent sur les activités de l'organisation. Il est présidé par la direction générale de l'organisation et accueille a minima un représentant de chacunes des trois lignes de défense ainsi qu'un membre en charge du développement des activités.

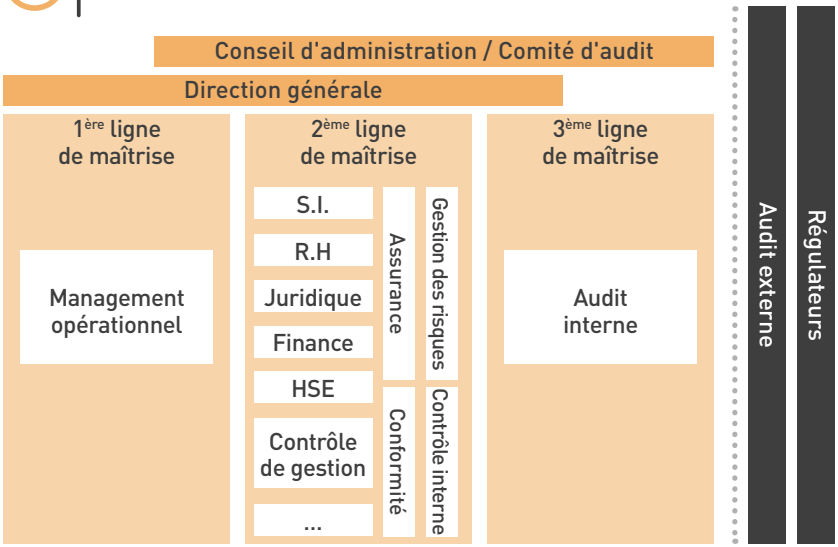
[5]Le comité des risques numériques s'inscrit dans une gouvernance globale de maîtrise du risque numérique lorsque celle-ci est prévue par l'organisation.

Le concept dit des « *trois lignes de défense* » est né d'un partenariat entre l'*European Confederation of Institutes of Internal Auditing* (ECIIA) et la *Federation of European Risk Management Associations* (FERMA).

L'Association de Management des Risques et des Assurances de l'Entreprise (AMRAE) et l'Institut Français de l'Audit et du Contrôle Internes (IFACI) proposent un modèle de gouvernance des risques fondé sur « trois lignes de maîtrise[6] ».

1. La première ligne de maîtrise rassemble les fonctions opérationnelles et les responsables métiers.
2. La deuxième ligne de maîtrise regroupe les spécialistes des risques (y compris numériques) à même d'assister les fonctions opérationnelles dans l'identification et l'évaluation des principaux risques relevant de leur domaine d'expertise.
3. La troisième ligne de maîtrise assure une fonction d'audit (interne ou externe selon la taille de l'organisation) indépendante et liée au plus haut niveau de l'organisation.

Modèle des trois lignes de maîtrise



Fonctions participant au dispositif de maîtrise globale des risques

Figure 2 - Les trois lignes de maîtrise

[6] L'AMRAE et l'IFACI ont adapté le concept dans un ouvrage répondant aux attentes de leurs cibles : Trois lignes de maîtrise pour une meilleure performance : fiabiliser la stratégie par une gestion organisée des risques, AMRAE et IFACI, 2015.

Les organisations FERMA et ECIIA ont également publié un guide de recommandations sur l'organisation interne nécessaire à la gestion des risques numériques : *At the Junction of Governance and Cyber-security*, FERMA et ECIIA, 2017, www.ferma.eu.

Les missions du comité des risques numériques :

1. Rédiger et maintenir à jour la Politique de Sécurité des Systèmes d'Information (PSSI) qui régit la gestion du risque numérique.
2. Définir la stratégie de sécurité numérique de l'organisation et les investissements nécessaires à sa mise en œuvre.
3. Veiller en priorité à la sécurité des services numériques les plus critiques. Ces services ou ces systèmes d'information font l'objet d'une homologation de sécurité[7].
4. Assurer le pilotage de la performance et l'amélioration continue de la gestion du risque numérique.
5. Définir une stratégie de valorisation des investissements réalisés dans le champ de la sécurité numérique.

[7] *Cf. Étape 8 - Homologuer ses services numériques critiques*

ÉTAPE 2. Comprendre son activité numérique

Appréhender et comprendre son activité numérique précèdent toute démarche de gestion du risque numérique.
L'activité d'une organisation repose sur des processus et informations qui la lient à ses fournisseurs, ses clients, ses administrés, ses partenaires, etc. Ces valeurs métiers[8], comme les nomme l'ANSSI, sont elles-mêmes supportées par des services et systèmes d'information qu'il importe de cartographier très tôt.

Identifier ses valeurs métiers et biens supports critiques

L'identification des valeurs métiers et des biens supports[9] les plus critiques se fait en partant des missions de l'organisation qui lui permettent de créer de la valeur pour descendre progressivement vers les services numériques qui les sous-tendent.

Dans un premier temps, l'objectif n'est pas d'être exhaustif mais de faire ressortir les activités principales et les services numériques ou les systèmes d'information les plus essentiels. Ce niveau de détail est suffisant pour construire ses pires scénarios de risque[10] et pour identifier les services numériques et les systèmes d'information qui feront l'objet d'une attention spécifique du comité à travers une démarche d'homologation de sécurité[11].

Pour les services numériques les moins critiques, les mesures de sécurité qui s'appliquent de manière systématique reposent sur une approche par conformité aux normes et bonnes pratiques et sur la contruction d'un socle de sécurité.

[8]Valeur métier (business asset) : composante essentielle à l'accomplissement des missions de l'organisation. Il peut s'agir d'un service, d'une fonction support, d'une étape d'un projet ou de toute information ou savoir-faire associé. EBIOS Risk Manager, ANSSI, 2018, www.ssi.gouv.fr/ebios.
[9]Bien support (supporting asset) : composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle. EBIOS Risk Manager, ANSSI, 2018, www.ssi.gouv.fr/ebios
[10]Cf. Étape 4 – Construire ses pires scénarios de risque
[11]Cf. Étape 8 – Homologuer ses services numériques critiques

Cartographier son écosystème

La transformation numérique plonge l'organisation dans un écosystème très intégré avec ses diverses parties prenantes. On parle alors d'entreprise étendue, incluant l'organisation dans une chaîne globale de production. Le corolaire est que le risque numérique ne s'arrête pas aux frontières de l'organisation.

C'est pourquoi il est indispensable de mener un travail de cartographie de l'écosystème de l'organisation afin d'avoir une vision de ses interactions et de ses flux. De même, parce que l'écosystème influence l'organisation dans sa gestion des risques, le dirigeant doit inclure dans la définition de l'appétence aux risques[12] de l'organisation ses parties prenantes, leurs niveaux de menace et les principes de partage du risque.

Enfin, les acteurs de l'écosystème évoluant au gré des opportunités économiques, cette cartographie pourra être mise à jour à travers une activité de veille de l'information[13].

Pour aider l'organisation à cartographier son écosystème et évaluer la menace numérique qui pèse sur elle, l'ANSSI propose une approche simple et efficace capable de mettre en évidence les parties prenantes qui fragilisent le plus l'organisation (cf. atelier 3 de la méthode EBIOS Risk Manager).

Identifier le cadre légal et réglementaire qui régit ses activités numériques

Le dirigeant doit connaitre les exigences légales et réglementaires applicables à son organisation et être capable d'apprécier son niveau de conformité à leur égard. S'il n'est pas toujours facile d'identifier le cadre légal et réglementaire applicable à son organisation, initier la réflexion selon les axes ci-dessous permet toutefois de dresser un état des lieux assez complet de sa situation en vue d'en dégager les obligations afférentes.

- Les missions et activités de l'organisation : exigences de sécurité incluses dans les contrats passés avec ses clients, fournisseurs ou partenaires.
- Le secteur d'activité : exigences particulières de protection en fonction du secteur d'activité de l'organisation (public, santé, nucléaire, transports, finances, etc.).

[12] *Cf. Étape 3 – Définir son seuil d'acceptation des risques*
[13] *Cf. Étape 12 – Connaissance : de la veille à l'analyse*

- La nature de l'organisation : l'Etat peut par exemple attribuer les statuts particuliers d'opérateur d'importance vitale (OIV) ou d'opérateur de service essentiel (OSE) à l'organisation.
- La nature des informations manipulées : exigences applicables à la manipulation de certaines informations sensibles (par exemple, les données à caractère personnel).
- Le cadre national et international : contraintes légales nationales et internationales ayant pour objectifs la protection des populations et l'économie des nations.

Pour l'aider à déterminer le cadre légal et réglementaire qui lui est applicable et l'assister dans sa démarche de mise en conformité, l'organisation peut avoir recours à des compétences externes spécialisées dans le conseil juridique.

ÉTAPE 3. Connaître son seuil d'acceptation des risques

L'appétence aux risques est le niveau de risque qu'un dirigeant accepte de prendre pour soutenir les activités et le développement de son organisation. Elle appuie les décisions stratégiques et oriente les opérations.

Comment connaître son appétence aux risques

L'appétence aux risques est fortement liée à la culture de l'organisation, à son secteur économique, ses implantations et à sa stratégie de développement. Elle formalise les attentes des instances dirigeantes en matière de prise de risques. Fruit d'échanges avec les parties prenantes de l'organisation (banques, assurances[14], partenaires, clients ou fournisseurs[15], etc.), l'appétence aux risques définit le seuil d'acceptation des risques de l'organisation.

Pour être efficace, l'appétence aux risques doit être régulièrement réévaluée au moyen d'indicateurs de performance[16] et à la lumière des évolutions[17] que connait l'environnement (sociales, techniques, économiques, environnementales et politiques).

Une méthode d'aide à la définition d'une politique d'appétence aux risques est proposée dans l'ouvrage Management du risque : une approche stratégique, AFNOR édition, 2018.

[14] *Cf. Étape 6 – Mettre en place des polices d'assurance adaptées*
[15] *Cf. Étape 2 – Comprendre son activité numérique*
[16] *Cf. Étape 14 – Agilité : l'amélioration continue et la performance*
[17] *Cf. Étape 12 – Connaissance : de la veille à l'analyse*

ÉTAPE 4. Construire ses pires scénarios de risque

Associée à une approche par conformité aux bonnes pratiques[18], l'identification et la quantification financière des scénarios de cyberattaque les plus critiques pour l'organisation, constituent l'étape initiale de la stratégie de sécurité numérique.

Adopter une approche par conformité aux risques les plus vraisemblables

Le respect de normes[19] et de bonnes pratiques en matière de sécurité des systèmes d'information permet d'anticiper la survenance des cyberattaques les plus vraisemblables. En prenant ainsi connaissance des mesures de sécurité numériques indispensables à la construction du socle de sécurité[20], l'organisation devient capable de recentrer son analyse de risque en s'intéressant aux scénarios les plus critiques pour son activité..

Identifier les scénarios de cyberattaque critiques[21]

Le comité des risques numériques élabore des scénarios de cyberattaque susceptibles d'impacter une ou plusieurs activités vitales pour l'organisation. Ces impacts peuvent être numériques, physiques, financiers, liés à la réputation ou encore juridiques. Le niveau de risque est ensuite défini en fonction de la gravité de ces impacts et de la vraisemblance de ces scénarios. La vraisemblance reflète le degré de faisabilité ou de possibilité qu'un attaquant aboutisse à son objectif (cf. Figure 3).

[18] Guides techniques et recueils de bonnes pratiques élémentaires de l'ANSSI - https://www.ssi.gouv.fr/bonnes-pratiques/
[19] Famille ISO/IEC 27000 - Systèmes de management de sécurité de l'information, ISO - www.iso.org
[20] Cf. Étapes 9, 10 et 11
[21] Les ateliers 2 et 3 de la méthode d'analyse des risques EBIOS Risk Manager de l'ANSSI peuvent aider à identifier les scénarios de risque numérique les plus critiques. EBIOS Risk Manager, ANSSI, 2018 - www.ssi.gouv.fr/ebios/

Quelle que soit la structure de l'organisation, le comité doit fonder l'élaboration de ces scénarios sur les questions suivantes.

- Quels sont les évènements redoutés qui peuvent impacter les valeurs métiers de l'organisation ?
- Quels sont les attaquants susceptibles de porter atteinte aux activités de l'organisation et quels sont leurs objectifs ?
- Mes systèmes d'information sont-ils suffisamment robustes pour résister à une cyberattaque ciblée ?
- Quels sont les risques tiers qui peuvent impacter l'organisation (risque d'image négative, de non-conformité, sanitaire, environnemental, etc.) ?

L'élaboration de scénarios de cyberattaque permet de mettre en évidence l'existence de systèmes d'information (internes ou externes) qui, dans un premier temps, n'avaient pas été identifiés comme critiques.

Les services numériques critiques identifiés à l'étape 2 devront faire l'objet d'une attention spécifique de la part du comité des risques numériques. Cela se traduira notamment par la mise en œuvre d'une démarche d'homologation de sécurité[22].

Quantifier les impacts des scénarios de cyberattaque critiques

Quantifier financièrement les impacts des scénarios de cyberattaque les plus critiques éclaire la prise de décision quant aux options de traitement des risques. Afin de déterminer le coût de la réussite d'un scénario de cyberattaque, une analyse financière peut être menée en tenant compte des éléments suivants :

- les engagements contractuels conclus avec les tiers ou le non-respect des contraintes légales et réglementaires applicables ;
- les pertes d'exploitation et de production ;
- la perte ou la destruction d'informations essentielles ;
- la remédiation des systèmes d'information et la reprise d'activité.

[22] *Cf. Étape 8 – Homologuer ses services numériques critiques*

Cependant, certains coûts sont plus difficiles à estimer. C'est notamment le cas de ceux engendrés par une perte de confiance ou une atteinte à l'image. Pour estimer le coût de tels impacts, la mise en oeuvre d'une stratégie de veille de l'information[23] permettra à l'organisation de s'informer sur les cyberattaques à l'encontre d'organisations de tailles et d'activités similaires.

La description précise des conséquences d'un scénario peut respecter différentes phases : la crise, la remédiation et l'amélioration.

Pour chacune d'elles, les participants doivent spécifier quelles sont les parties impactées et à quel niveau. Ces données seront interprétées pour évaluer les hypothèses en montants financiers.

La crédibilité des estimations financières est capitale dans la prise de décision des dirigeants vis-à-vis de la stratégie de sécurité numérique.

[23] *Cf. Étape 12 – Connaissance : de la veille à l'analyse*

Communiquer sur les risques numériques

Activité	Evénement redouté	Impact
Création / R&D	Copie des données de R&D et fabrication de contrefaçons	**Impact financier** **Impact sur l'image et la confiance**
Fabrication	Fuite d'information sur les procédés de fabrication	**Impact juridique** **Impact sur l'image et la confiance**
	Indisponibilité de la chaine de production	**Impact financier** **Impact sur les objectifs de production**
Facturation / Commande	Vol de la base clients/ fournisseurs	**Impact juridique** **Impact concurrentiel**
	Indisponibilité du système de facturation	**Impact financier** **Impact sur les objectifs de commande**
	Fuite des données commerciales	**Impact financier**
Livraison	Corruption des bons de livraison	**Impact sur l'image et la confiance** **Impact sur les livraisons**

Figure 3 – Exemple de formalisation de scénarios de risque numérique

Le risk manager a pour mission de retranscrire de façon intelligible les différents scénarios de risque numérique en décrivant leur gravité et leurs impacts, y compris financiers. Cette synthèse des scénarios pesant sur l'activité de l'organisation sera présentée au dirigeant. Cela orientera le dirigeant dans ses prises de décision en matière de stratégie de sécurité numérique.

Pertes financières estimées	Gravité	Vraisemblance	Scénario de risque
25 % du CA	4 - Catastrophique	Vraisemblable	R1
25 % du CA	3 - Majeur	Vraisemblable	R2
80 k€/jour	4 - Catastrophique	Très vraisemblable	R3
4 % du CA	4 - Catastrophique	Vraisemblable	R4
80 k€/jour	3 - Majeur	Vraisemblable	R5
25 % du CA	3 - Majeur	Très vraisemblable	R6
80 k€/jour	4 - Catastrophique	Très vraisemblable	R7

ÉTAPE 5. Définir sa stratégie de sécurité numérique et de valorisation

Le dirigeant doit décider du traitement des risques numériques identifiés en fonction des enjeux et objectifs stratégiques de son organisation. Sur la base de ces choix, le comité des risques numériques établit la stratégie de sécurité numérique et définit les objectifs prioritaires, les ressources allouées et les étapes visant à atteindre le niveau de maturité cyber visé.

Investir dans la sécurité numérique représente un coût mais cela répond à une attente forte des clients et partenaires de l'organisation. Il est donc possible d'en faire un avantage compétitif en adoptant une approche de type *Cyber Business Partner (cf. Étape 15).*

Analyse des risques numériques

La phase d'analyse des risques correspond aux choix et arbitrages faits par le dirigeant au regard des enjeux et objectifs de son organisation. Ces choix doivent s'appuyer sur :

- la vraisemblance d'exploitation des chemins d'attaques et l'impact des pires scénarios sur l'organisation ;
- la capacité des mesures de sécurité en place à empêcher la survenance des scénarios ;
- les ressources financières, humaines et techniques disponibles.

En tenant compte de ces critères, le dirigeant sera en mesure de choisir les options de traitement des risques à retenir telles que la mise en œuvre de mesures de sécurité, l'évolution des processus métiers ou encore le transfert contractuel des risques vers des tiers externes (sous-traitants, assurances, etc.).

Stratégie de sécurité numérique

Les options de traitement des risques sont déclinées dans la stratégie de sécurité numérique qui sera pilotée par le comité des risques numériques. Cette stratégie comprend quatre axes :

- l'implémentation progressive du socle de sécurité afin de faire converger celui-ci avec la politique de sécurité des systèmes d'information (PSSI).

La mise en œuvre du socle de sécurité est détaillée dans la section « BÂTIR SON SOCLE DE SÉCURITÉ ».

- la mise en œuvre d'une réponse aux scénarios de cyberattaque critiques. Cette réponse se traduit par l'établissement d'un plan d'amélioration continue de la sécurité (PACS) incluant une démarche d'homologation[24].
- la valorisation de la sécurité numérique par la communication en vue de développer un avantage concurrentiel[25].
- une politique de transfert de risque efficace vers le marché de l'assurance pour compléter le schéma de gestion de risque. Cette politique doit être pensée de façon globale mais détaillée par une équipe spécifique incluant le risk manager, le courtier et l'assureur (cf. Étape 6).

Construire une réponse aux scénarios de cyberattaque critiques

La réponse aux scénarios de cyberattaque critiques requiert l'intervention d'experts en sécurité des systèmes d'information. Après avoir identifié les chemins d'attaque qui permettent la réalisation de ces scénarios critiques, ils proposent pour chacun d'eux des mesures de mitigation. Celles-ci visent à réduire la vraisemblance du scénario et à augmenter la difficulté pour l'attaquant d'atteindre son objectif.

Ces mesures peuvent s'appuyer sur des solutions techniques (numériques ou analogiques), humaines (internes ou externes) ou organisationnelles (notamment dans l'évolution des processus métiers). Elles seront ensuite consolidées dans le PACS (cf. exemple Figure 4).

Plan d'amélioration continue de la sécurité (PACS)

Lorsque le comité des risques numériques consolide les mesures de mitigation dans le PACS, il a pour objectif de faire progresser l'organisation en matière de sécurité numérique. Ce faisant, il s'engage sur la stratégie de sécurité numérique à moyen et long termes et doit prendre en considération les contraintes financières de l'organisation, l'optimisation des coûts et les investissements nécessaires à cette montée en maturité.

Lors de la construction du PACS, le comité des risques numériques peut par exemple indiquer : les mesures envisagées pour chacun des scénarios de cyberattaque critiques, le porteur du projet, les ressources nécessaires, une estimation du coût de la mise en œuvre, de sa complexité et les délais de mise en œuvre impartis.

[24]Cf. Étape 7 – Homologuer ses systèmes d'information critiques
[25]Cf. Étape 15 – Valorisation : la cybersécurité, un avantage compétitif

Plan d'Amélioration Continue de la Sécurité (PACS)

Mesure de sécurité		Scénarios de risque	Responsable
Nature	Mesure		
Facteur humain	Sensibilisation renforcée aux méthodes d'hameçonnage	R4/R6	Responsable sécurité
Protection des données	Protection renforcée des données de création, de fabrication et de livraison sur le SI (pistes : chiffrement, cloisonnement)	R1/R2/ R4/R6	Responsable informatique
Résilience	Plan de continuité d'activité avec un partenaire / sous-traitant	R3/R5	Responsable opérationnel
Résilience	Contrat d'assurance cyber / responsabilité civile	R3/R5/R7	Responsable financier

Figure 4 – Exemple de plan d'amélioration continu de la sécurité (PACS)

Comme dans tout système de management, le comité doit réévaluer les pires scénarios au regard de l'avancement du PACS. Via cette revue, il permet ainsi d'apprécier l'efficacité des mesures implémentées et le retour sur investissement de ces dernières.

Complexité	Coût estimé	Echéance	Priorité
+	5 k€	3 mois	P2
++	15 k€	3 mois	P1
+++	30 k€	1 mois	P2
++	5 k€/an	1 mois	P1

Valoriser son investissement dans la sécurité numérique

Les stratégies de sécurité d'une part et de valorisation d'autre part peuvent être conduites de manière simultanée et ce, dès le départ. Ainsi, pour transformer l'effort d'investissement en avantage concurrentiel, le comité des risques numériques peut envisager les investissements de sécurité à l'aune de leurs impacts sur les risques et de la valorisation que l'on peut en faire[26].

[26] *Cf. Étape 15 – Valorisation : la cybersécurité, un avantage compétitif*

ÉTAPE 6. Mettre en place des polices d'assurance adaptées

Parmi les mesures permettant d'améliorer la résilience de l'organisation, la mise en place d'une police d'assurance cyber adaptée est essentielle. En effet, l'assurance peut permettre à l'organisation d'encaisser le choc financier d'une éventuelle crise et, en particulier, les pertes de revenu liées à l'arrêt de l'activité durant la crise.

Grâce à l'ensemble des travaux déjà réalisés pour maîtriser son risque numérique, l'organisation doit avoir une idée plus claire de son risque résiduel et des impacts potentiels d'une crise non seulement sur son activité, mais aussi sur ses parties prenantes.

Faire l'inventaire des couvertures existantes

Avant de se mettre en quête d'une assurance spécifique, l'organisation doit d'abord faire un état des lieux de ses polices d'assurance dans le cas où l'une d'elle prévoirait la couverture d'incidents numériques. En effet, il est tout à fait possible que le risque numérique soit partiellement couvert au titre de dommages ou en termes de responsabilité civile.

Aujourd'hui toutefois, les couvertures classiques ne couvrent que très partiellement le risque numérique. S'il est parfois possible d'interpréter certaines clauses en faveur d'une prise en charge de ce type de risque, les assureurs sont généralement peu enclins à les couvrir. Ainsi, on tend de plus en plus vers une exclusion explicite du risque numérique des contrats d'assurance classiques, au profit de polices d'assurance plus spécifiques.

Principaux piliers d'une police d'assurance cyber

Figure 5 - Les quatre piliers d'une politique d'assurance cyber

Identifier la meilleure couverture

Une fois son bilan assurantiel achevé, l'organisation peut se mettre en quête d'une couverture spécifique. Contrairement aux polices classiques qui séparent les conséquences pour l'organisation (assurance dommage) de celles sur les tiers (assurance responsabilité), l'assurance cyber peut offrir une couverture des risques directs et indirects. Généralement, ces différents aspects se retrouvent ventilés dans quatre piliers suivants :

- Prévention : l'assureur va aider l'organisation à mettre en place ou améliorer la gestion de son risque numérique, en lui apportant son support dans l'application des démarches décrites dans cet ouvrage. Ainsi, la mise en place d'une police peut permettre à l'organisation d'améliorer sa gestion du risque numérique grâce, notamment, au diagnostic et recommandations émis par l'assureur.
- Assistance : en cas d'événement, l'assureur entrera en jeu pour apporter son expertise et permettre ainsi de sortir plus vite de la crise. En aidant au redémarrage rapide de l'activité, il peut permettre de réduire le montant des pertes.
- Couverture des opérations : l'assureur couvre les pertes financières directement subies par l'organisation : pertes d'exploitation, de revenus et dépenses supportées pour faire face à la crise.
- Couverture de la responsabilité : l'assureur va couvrir le coût des recours et dommages éventuellement subis par des tiers.

Compte tenu de ses différents leviers d'intervention, l'assurance cyber est un outil complexe qui requiert une véritable expertise. Il peut être judicieux de recourir aux services d'un courtier d'assurance au fait des enjeux de sécurité numérique et du contexte dans lequel évolue l'organisation concernée.

L'assurance cyber étant un produit encore récent, il n'existe pas pour le moment de véritable standard de marché.

Eprouver la solution choisie

La mise en place d'une assurance cyber n'est pas qu'une case à cocher. La police souscrite doit répondre aux besoins et à l'intérêt de l'organisation. Un bon moyen de s'assurer de la pertinence de son choix est, avant de s'engager, de tester les polices à l'aune des scénarios de risques identifiés par l'organisation.

L'organisation pourra ainsi évaluer la pertinence de sa couverture et, éventuellement, activer certaines variables (prix et montants, champ de la couverture, etc.).

Quatre conseils pour trouver la meilleure assurance cyber

- Se faire conseiller par un courtier qui connaît le sujet cyber mais aussi le secteur dans lequel évolue l'organisation. Il soutiendra la réflexion sur le niveau de couverture d'assurance nécessaire.
- Bien préparer la documentation à fournir aux assureurs en vue de l'évaluation du risque.
- Comparer les offres. Il peut y avoir de grandes différences entre les polices proposées, surtout si la couverture prévoit des spécificités relatives à l'activité de l'organisation (aviation, maritime, construction, etc.).
- Prendre le temps de mener à bien chaque étape pour disposer d'une connaissance fine de ses enjeux avant de se tourner vers le marché de l'assurance. L'objectif n'est pas de souscrire une police pour se rassurer, mais de s'engager pour un contrat véritablement adapté aux besoins de l'organisation.

Dans le document *Preparing for Cyber Insurance*, publié en octobre 2018, la *Federation of European RIsk Management Associations* (FERMA), *Insurance Europe* (représentant les assureurs) et la Fédération européenne des intermédiaires d'assurance (BIPAR) livrent un grand nombre d'éléments pour dialoguer avec le marché, vérifier de façon précise les conditions d'un éventuel contrat d'assurance cyber et comparer les offres.

www.ferma.eu

BÂTIR

SON SOCLE DE SÉCURITÉ

ÉTAPE 7. Placer l'humain au centre du jeu

L'humain est à l'origine et au cœur du dispositif.

Parce qu'il est au centre du jeu, il est souvent une cible privilégiée des attaquants.

En incluant pleinement le facteur humain dans la PSSI, il est possible d'obtenir des collaborateurs une participation active à la sécurité numérique de l'organisation suivie de résultats rapides et significatifs pour un coût raisonnable.

Sensibilisation et exercices

Le facteur humain est l'un des leviers d'action privilégiés par les attaquants. Il est donc essentiel de l'inclure dans la stratégie de sécurité numérique de l'organisation. Pour y parvenir, des actions de sensibilisation ou la conduite d'exercices réalistes[27] peuvent être organisées. L'enjeu est de développer une véritable culture de la sécurité numérique de telle sorte que les membres de l'organisation, appuyés de procédures de sécurité, parviennent à déjouer les pièges les plus courants tendus par les attaquants.

Les actions menées à chaque niveau (sensibilisation, exercices) doivent être renouvelées à intervalles réguliers pour être véritablement efficaces car les équipes se transforment, les bonnes pratiques s'évaporent et la menace ne cesse d'évoluer.

Acquisition et maintien des compétences

Pour les équipes dont la spécialité relève de la sécurité des systèmes d'information ou de l'informatique, l'acquisition et le maintien de compétences à l'état de l'art est à inclure dans le plan de formation annuel. Ces formations peuvent prendre la forme de programmes en ligne (MOOC [28]), de stages ou de formations continues[29].

[27] Scénarios de crise ou jeux de rôles (serious game). Les serious games en sécurité et cybersécurité pour le grand public et les professionnels, CCI, www.cci.fr/web/presse/actualite-fiche/-/asset_publisher/9FDf/content/actu-:-serious-games-pr-pro

[28] Améliorez vos connaissances et compétences en matière de sécurité numérique avec le MOOC SecNumAcadémie de l'ANSSI. www.secnumacademie.gouv.fr

[29] L'ANSSI a développé le label de formation SecNumedu-FC. Il référence les établissements proposant des formations continues dans le domaine de la sécurité du numérique. www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu

ÉTAPE 8. Homologuer ses services numériques critiques

Cette démarche est préalable à l'instauration de la confiance dans les services numériques de l'organisation. Grâce à une démarche itérative et pérenne, elle assure une maitrise des risques portant sur les services numériques les plus critiques et participe à la valorisation des investissements dans la sécurité numérique.

La démarche d'homologation[30] engage et responsabilise le dirigeant vis-à-vis des risques numériques qui pèsent sur les services numériques les plus critiques de son organisation. Elle garantit que les risques sont connus de lui et maîtrisés par ses équipes.

Cette démarche permet de constituer un véritable dossier de sécurité des services numériques et systèmes d'information critiques. Elle mobilise également les équipes et ressources nécessaires à son déroulement dans le cadre d'une démarche itérative. Ce dernier aspect assure une révision périodique du dossier de sécurité et des risques résiduels dans le cycle de vie des systèmes d'information.

Elle est menée par les responsables métiers avec l'assistance du responsable de la sécurité des systèmes d'information (RSSI) et du directeur des systèmes d'information (DSI) et comprend le passage par une commission d'homologation, présidée par le dirigeant. A cette occasion, les risques numériques, les réponses aux pires scénarios et la stratégie de traitement des risques lui sont présentés.

La démarche d'homologation peut être engagée par le dirigeant en parallèle de la construction du socle de sécurité de son organisation.

Dans certains cas, la démarche d'homologation peut être obligatoire. Citons par exemple l'instruction générale interministérielle n°1300[31], le référentiel général de sécurité (RGS)[32], la politique des systèmes d'information de l'État (PSSIE)[33] et la loi de programmation militaire[34] (LPM).

[30] L'homologation de sécurité en neuf étapes simples, ANSSI, 2017, www.ssi.gouv.fr/guide-homologation-securite
[31] Instruction générale interministérielle n° 1300, SGDSN, 2011, www.ssi.gouv.fr/igi1300
[32] Référentiel général de sécurité (RGS), ANSSI, 2014, www.ssi.gouv.fr/rgs
[33] Politique de sécurité des systèmes d'information de l'État, (PSSIE), ANSSI, 2014, www.ssi.gouv.fr/pssie
[34] Loi de programmation militaire 2014 à 2019, www.legifrance.gouv.fr

ÉTAPE 9. Bâtir sa protection

Protéger les activités métiers et les biens supports de l'organisation passe par la mise en œuvre de mesures de sécurité. Ces mesures se situent au carrefour de considérations organisationnelles, numériques et physiques.

Elles sont sélectionnées sur la base d'une approche par conformité vis-à-vis des différents référentiels de sécurité (légal, réglementaire, etc.) s'appliquant à l'organisation.

Eléments juridiques de protection

Une politique de prévention contractuelle active doit être déployée pour ne pas s'exposer à des poursuites parfois pénales de la part des clients et partenaires, quelle que soit leur nationalité. La responsabilité du dirigeant et la réputation de l'organisation en dépendent. A ce titre, il est essentiel d'observer quelques points d'attention juridiques :

- les obligations légales et réglementaires auxquelles l'organisation est soumise ;
- les contrats établis avec les tiers et notamment les sous-traitants (la juridiction applicable des éléments contractuels, la responsabilité civile professionnelle, les annexes de sécurité[35]) ;
- un « plan d'assurance sécurité » fourni par les tiers.

La mise en œuvre de mesures de protection juridiques à même de protéger l'organisation dans un environnement en constante évolution nécessite des compétences particulières en matière de conseil juridique.

Gestion de projets métiers

Toute évolution métier doit tenir compte des aspects de sécurité numérique et ce, le plus tôt possible. Afin de ne pas contraindre les métiers par des mesures trop lourdes vis-à-vis des besoins de sécurité, il est conseillé d'intégrer la sécurité de manière agile[36] dans les projets.

[35] *Les annexes de sécurité sont des exigences de sécurité contractuellement imposées aux partenaires, sous-traitants et fournisseurs.*

Etre attentif au niveau de sécurité numérique des composants dès la conception des architectures informatiques - *security by design* (ou « sécurité par conception ») - permet de limiter les vulnérabilités applicatives.

Enfin, la conduite d'un audit de sécurité[37] technique ou organisationnel par une entreprise tierce et indépendante[38] est une bonne manière de clore le projet et la démarche de sécurité afférente.

Maîtrise des usages numériques

L'usage professionnel et personnel des moyens informatiques (ordinateurs et téléphones mobiles, tablettes, supports amovibles, etc.), les déplacements et l'accès à des réseaux sans-fil dans l'organisation ou en dehors, sont autant de sources de menaces pour les systèmes d'information de l'organisation. Il convient d'anticiper ces situations afin de réduire son exposition à de telles menaces.

Les usages propres à chaque organisation doivent être maîtrisés et inscrits dans la PSSI de l'organisation. De plus, chaque usage ou moyen doit s'accompagner d'une procédure de maintien en condition de sécurité.

Il en va de même pour la manipulation et l'accès aux informations les plus sensibles de l'organisation. Il est indispensable de maîtriser leur diffusion et leur exposition, notamment vis-à-vis de personnes ou d'espaces que ces données ne concernent pas (par exemple, des données de R&D accessibles par un stagiaire ou depuis un salon professionnel).

Pour aider les dirigeants à prévenir les risques numériques engendrés par les usages en vigueur dans l'organisation, l'ANSSI publie des guides de bonnes pratiques appliquées à certains publics et/ou situations[39].

Barrières de protection numérique

Protéger ses activités métiers et biens supports, c'est aussi mettre en œuvre des mesures de protection applicatives, systèmes et réseaux.

[36] L'ANSSI met à la disposition des organisations un guide méthodologique pour les accompagner dans le développement sécurisé des projets et la gestion du risque numérique en mode agile. Agilité & sécurité numérique, ANSSI, 2018, www.ssi.gouv.fr/uploads/2018/11/guide-securite-numerique-agile-anssi-pa-v1.pdf

[37] Cf. Étape 14 – Agilité : l'amélioration continue et la performance

[38] Les PASSI sont des prestataires de service qualifiés par l'ANSSI spécialisés dans les activités d'audit de la sécurité numérique. www.ssi.gouv.fr/pass

[39] Recommandations sur le nomadisme numérique, ANSSI, 2018 - www.ssi.gouv.fr/nomadisme-numerique Sécurité numérique - Bonnes pratiques à l'usage des professionnels en déplacement, ANSSI, 2019 - www.ssi.gouv.fr/bonnes-pratiques-professionnels-en-deplacement

Cet arsenal de mesures techniques vise à limiter la conduite d'actions malveillantes sur les composants numériques et informations métiers afin de préserver leur disponibilité, leur confidentialité ou encore leur intégrité.

L'ajout de mesures de protection numérique peut engendrer un effet contraire si elles sont pourvues de vulnérabilités. Elles deviennent pour les attaquants des portes d'entrée supplémentaires vers les systèmes d'information. Il est donc important de choisir avec soin ses produits ou services de sécurité numérique et d'entretenir une relation de confiance avec le fabricant ou l'éditeur de celles-ci.

Dans certains cas, les organisations peuvent être soumises à des réglementations spécifiques en matière de protection numérique. Les opérateurs d'importance vitale[40] (OIV) et les opérateurs de service essentiel[41] (OSE) doivent ainsi se référer aux textes réglementaires les concernant pour orienter leurs choix en matière de solutions et de prestations[42] de sécurité numérique.

Barrières de protection physique

La maîtrise du risque numérique passe aussi par la maîtrise de son environnement physique et de ses locaux. Un contrôle d'accès physique aux systèmes d'information les plus critiques doit être mis en œuvre et associé à un système de vidéo protection. Pour compléter les moyens de protection physiques, il est fortement recommandé de prévoir des moyens d'alerte, voire de protection, contre les incidents environnementaux (incendie, inondation, surchauffe, etc.).

Toutefois, les moyens de protection précités demeurent des systèmes d'information à part entière. A ce titre, ils peuvent être exposés aux cyber-menaces et doivent être pris en compte dans les scénarios de risque.

Certaines organisations des secteurs de la recherche, de la défense ou de l'industrie sont soumises à des réglementations spécifiques en matière de protection physique.

Il convient alors de se rapprocher du Secrétariat général de la défense et de la sécurité nationale (SGDSN) pour prendre connaissance des réglementations spécifiques à la sécurité des secteurs d'activités d'importance vitale (SAIV), à la protection du potentiel scientifique et technique de la nation (PPST) ou encore à la protection du secret de la défense nationale (PSDN).

[40] Loi de programmation militaire (LPM)
www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france
[41] Directive européenne Network and Information Security (NIS)
www.ssi.gouv.fr/entreprise/reglementation/directive-nis
[42] Certification et qualification de sécurité délivrée par l'ANSSI, Les Visas de sécurité de l'ANSSI, www.ssi.gouv.fr/administration/visa-de-securite

ÉTAPE 10. Orienter sa défense et anticiper sa réaction

Défendre son organisation et ses activités métiers contre les cyberattaques, c'est orienter sa défense en fonction des pires scénarios de risque identifiés. La mise en œuvre de moyens de détection, de journalisation et de corrélation adaptés participera à la détection des cyberattaques. Tandis que les processus d'identification et de gestion d'une cyberattaque permettront de contenir et maîtriser ses impacts sur les activités de l'organisation.

Détecter les cyberattaques

Détecter les cyberattaques consiste avant tout à orienter ses moyens de détection vers les chemins et méthodes empruntés par les attaquants[43]. Des dispositifs de détection des cyberattaques visant les biens supports et activités métiers identifiés comme les plus critiques doivent être mis en œuvre sur décision des RSSI et DSI. Ces dispositifs peuvent être placés sur les réseaux bureautiques mais aussi sur les réseaux de production ainsi que sur les postes utilisateurs, les postes nomades et les accès Internet.

Journalisation et corrélation

En complément des dispositifs de détection, il est recommandé de mettre en œuvre un système de journalisation qui enregistre les événements relatifs à l'accès aux systèmes d'informations et aux données sensibles. Ces évènements et journaux sont ensuite corrélés et analysés pour contribuer efficacement à la détection des cyberattaques.

En fonction du cadre légal et réglementaire de l'organisation, celle-ci peut avoir l'obligation de recourir à des prestataires de service qualifiés par l'ANSSI spécialisés dans les activités de détection des cyberattaques[44].

[43] *Cf. Étape 6 – Placer l'humain au centre du jeu*
[44] *Prestataires de détection des incidents de sécurité (PDIS) - www.ssi.gouv.fr/pdis*

Qualifier et gérer une cyberattaque

Qualifier une cyberattaque consiste à identifier les activités et biens supports affectés par l'attaque et, surtout la gravité de ces impacts. Il s'agit alors de réagir, de traiter et de classer les incidents. Pour ce faire, il convient de répondre aux questions suivantes :

- que faire lors de la détection d'un incident ?
- qui alerter ?
- quelles sont les premières mesures à appliquer ?
- quelle est l'impact de la cyberattaque sur le fonctionnement de mon organisation ?

Une procédure d'escalade doit être définie pour gérer les incidents au juste niveau de responsabilité (métiers, DSI, RSSI) et décider du déclenchement ou non de la cellule de crise pour les organisations les plus importantes ou soumises à des obligations spécifiques. Enfin, la gestion d'une cyberattaque doit intégrer une phase d'analyse post-incident qui permettra d'améliorer l'efficacité des mesures de sécurité initialement déployées.

Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) produit et met à disposition un certain nombre de notes d'information, de bulletins d'actualité et d'alertes[45].

En cas d'acte ou de suspicion de cyber-criminalité, la plateforme cybermalveillance.gouv.fr peut accompagner les entreprises :

- **en les mettant en relation avec des prestataires de proximité compétents pour identifier la nature de l'incident et remettre les systèmes en état de fonctionnement ;**
- **en les redirigeant vers d'autres plateformes (PHAROS, Perceval, signal spam, etc.) ;**
- **en mettant à leur disposition de nombreux contenus et conseils pratiques.**

[45] *Les bons réflexes en cas d'intrusion de son système d'information, CERT-FR, 2002, www.cert.ssi.gouv.fr/information/CERTA-2002-INF-002*

ÉTAPE 11. Faire preuve de résilience en cas de cyberattaque

La résilience d'une organisation à la suite d'une cyberattaques relève de sa capacité à maintenir son activité malgré la survenance d'une action malveillante à son encontre.

Activer la cellule de crise

Si le fonctionnement de l'organisation est fortement impacté par la cyberattaque, le comité des risques numériques doit être convoqué et la cellule de crise constituée. Les membres de la cellule définissent et lancent les actions à mettre en œuvre pour limiter les impacts de la cyberattaque en cours et prévenir la propagation de la crise et ses effets de bord (financiers, juridiques, opérationnels, professionnels ou d'image). Si l'impact de l'attaque est proche des limites de l'appétence au risque[46], alors le plan de continuité d'activité (PCA) doit être activé.

La communication de crise

La communication de crise fait partie intégrante du dispositif de gestion de crise. Transverse, elle poursuit deux objectifs :

- la réduction des impacts directs de la cyberattaque (alerte des parties prenantes, instructions et coordination des opérations) ;
- et la préservation de la réputation (médiatique, financière, juridique, etc.) de l'organisation.

Pour mener à bien ces deux objectifs, il est nécessaire de mener un travail d'anticipation, tant sur le volet organisationnel (définition d'un dispositif de communication de crise, entrainement des communicants, etc.) que sur le volet opérationnel (identification de scénarios types, définition de plans de communication dédiés, préparation d'éléments de réponse clés en main, etc.).

[46] *Cf. Étape 3 – Définir son seuil d'acceptation des risques*

Relations avec les autorités

En cas de cyberattaque, il est nécessaire de prendre contact avec les forces de police ou de gendarmerie afin de les informer de la situation. Vous pouvez solliciter les services territoriaux de police ou de gendarmerie de proximité. En cas de dépôt de plainte, il est recommandé de se faire assister par un avocat spécialisé afin de déterminer les infractions pénales dont vous ou votre organisation êtes victime.

En fonction du cadre légal et réglementaire dans lequel s'inscrit l'organisation (OIV, OSE, etc.), celle-ci peut être dans l'obligation d'informer l'ANSSI de tout incident cyber. www.ssi.gouv.fr/en-cas-dincident

Le Plan de Continuité d'Activité (PCA)

Le PCA vise à garantir la survie de l'organisation à la suite d'une cyberattaque. Il organise le redémarrage des activités le plus rapidement possible avec le minimum de perte d'informations, avec ou sans l'assistance d'un prestataire. Pour être pertinent, le PCA prend appui sur l'étude des pires scénarios. Il constitue un chapitre essentiel de la politique de sécurité de l'organisation et doit être revu, testé et enrichi à intervalles réguliers pour rester efficace.

Pour vous aider dans la constitution de votre PCA, vous pouvez vous appuyer sur les ressources suivantes :

- ISO 22301 : 2012 Systèmes de management de la continuité d'activité - www.iso.org
- Guide pour réaliser un plan de continuité d'activité, SGDSN, 2015 - www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf
- Plan de continuité d'activité à l'usage du chef d'entreprise en cas de crise majeure, DGE, 2015 - www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf

Le Plan de Reprise d'Activité (PRA)

L'objectif du PRA est de procéder à la reconstruction des systèmes d'information et des données afin de redémarrer les applications et processus métiers le plus rapidement possible en cas de cyberattaque critique. Le PRA est constitué d'un ensemble de procédures techniques, organisationnelles et de sécurité et peut s'appuyer sur des partenaires et prestataires externes.

Tout comme le PCA, le PRA prend appui sur l'étude des pires scénarios. Intégré à la politique de sécurité de l'organisation, il doit être revu, challengé et enrichi à intervalles réguliers pour rester efficace.

Relation avec votre assureur

Durant la gestion de crise, l'activation de la police d'assurance souscrite lors de l'étape 6 peut se révéler nécessaire. Cela permet notamment à l'organisation de bénéficier de ressources spécifiques supplémentaires pour l'aider à gérer la crise et revenir au plus vite à une situation normale. Selon la couverture d'assurance choisie et la gravité de l'incident, les ressources suivantes peuvent intervenir :

- des experts cyber, pour gérer l'incident et mener les investigations nécessaires à sa qualification et à sa maitrise ;
- des experts système, pour aider à la reconstruction des systèmes d'information et à la restauration des données ;
- des conseillers juridiques pour préserver les responsabilités civile et pénale de l'organisation et de son dirigeant ;
- des conseillers en communication de crise afin d'assister le dirigeant dans la gestion de la crise, en limiter les impacts et de préserver l'image de l'organisation.

L'assurance cyber permet également d'amortir le choc financier, en particulier, les pertes de revenu liées à l'arrêt de l'activité.

Enfin, l'assurance peut permettre de faire face aux frais potentiels engendrés pour compenser les dommages causés à des tiers du fait de l'incident survenu. La prise en compte de cet aspect est essentiel pour préserver la réputation et la crédibilité de l'organisation vis-à-vis de ses parties prenantes.

PILOTER SON RISQUE

NUMÉRIQUE ET VALORISER SA CYBERSÉCURITÉ

ÉTAPE 12. Connaissance : de la veille à l'analyse

Devant la transformation numérique, l'organisation n'a pas d'autre choix que d'être à l'écoute du monde dans lequel elle évolue. Il lui est vital de comprendre son environnement et ses dynamiques pour anticiper les menaces et leurs impacts.

Cibler et structurer sa démarche de veille

Comme spécifié dans l'étape 2, le comité des risques numériques doit inclure dans le cadre de la gestion du risque numérique de l'organisation la mise en place d'une démarche de veille de l'information continue et itérative. La stratégie de veille adoptée a pour objectif le maintien à jour des connaissances de l'organisation vis-à-vis de ses activités, de son écosystème (concurrence, e-réputation, aspects juridiques, capacité technologique, développement numérique, etc.), des sources de menace et méthodes d'attaques.

Repositionner l'organisation dans son environnement

Le maintien à jour des connaissances sectorielles, métiers et transverses de l'organisation aide le comité des risques numériques dans sa prise de décision face à de nouvelles menaces, vulnérabilités ou contraintes légales et réglementaires.

ÉTAPE 13. Engagement : de l'adhésion à l'action

Obtenir l'engagement de ses collaborateurs et des parties prenantes de l'organisation dans la stratégie de sécurité numérique permet de gagner en agilité face à la menace.

Ainsi, l'exploitation du facteur humain comme vecteur d'attaque est réduite, tandis que l'acuité des collaborateurs face aux pièges tendus par les cyber-attaquants est renforcée.

Fédérer ses collaborateurs et parties prenantes

C'est au travers de la mise en œuvre d'un véritable plan d'engagement, découlant de la stratégie de sécurité numérique, que les différents acteurs (internes et externes) de l'organisation se sentiront pleinement impliqués dans la démarche de gestion du risque[47]. Ainsi il sera possible de considérer l'humain comme un acteur de défense plutôt que comme un vecteur d'attaque.

Ce plan d'engagement repose sur trois axes :

- L'autorité. Le dirigeant doit communiquer auprès de ses collaborateurs et parties prenantes les informations de contexte (économiques, politiques, etc.), les impacts des risques numériques sur l'organsation (pertes financières, chômage technique, etc.), les enjeux de la sécurité numérique (protection des données et du savoir-faire, fraude et corruption, maintien de la production, etc.), et les missions et objectifs de chacun.
- Les compétences. Les collaborateurs doivent être entrainés et formés, ainsi leurs compétences seront maintenues dans le temps.
- Les moyens. Les moyens informatiques fournis aux collaborateurs et parties prenantes doivent leur permettre d'accomplir leurs activités dans le respect de la PSSI et des procédures de sécurité numérique.

[47] *Cf. Étape 7 – Placer l'humain au centre du jeu*

L'engagement comme indicateur de performance

La mesure de l'engagement des collaborateurs et parties prenantes en tant qu'acteurs de la défense de l'organisation doit être menée de manière régulière au travers d'enquêtes et de questionnaires internes.

Cet indicateur permet notamment de détecter les signaux faibles d'une démotivation ou d'une incompréhension des enjeux de la sécurité numérique de la part des différents acteurs (internes et externes) de l'organisation.

ÉTAPE 14. Agilité : l'amélioration continue et la performance

En inscrivant sa stratégie de gestion du risque numérique dans une démarche itérative d'amélioration continue, l'organisation s'adapte aux nouvelles menaces, renforce son socle de sécurité et maitrise ses investissements.

Stratégie d'audit et de contrôle

La mise en place d'une stratégie efficace d'audit et de contrôle permet de s'assurer du maintien du niveau de sécurité de l'organisation. Les audits et contrôles portent sur la conformité des mesures organisationnelles, numériques ou physiques. Ils mettent en évidence les points de vigilance et de non-conformité à l'égard des référentiels et de la mise en œuvre du PACS.

La stratégie d'audit et de contrôle doit être revue à intervalles réguliers pour y intégrer les évolutions de l'organisation et de son environnement.

En fonction du cadre légal et réglementaire de l'organisation, celle-ci peut avoir l'obligation de recourir à des prestataires de service qualifiés par l'ANSSI spécialisés dans les activités d'audit de la sécurité numérique. www.ssi.gouv.fr/passi

S'adapter en permanence à la menace

La démarche d'amélioration continue portée par le comité des risques numériques doit s'appuyer sur :

- la stratégie de veille de l'information ;
- les outils de mesure de la performance (indicateurs et tableau de bord) ;
- les résultats des actions de contrôle et d'audit.

En intégrant la connaissance des nouvelles menaces, les objectifs de la stratégie de sécurité numérique et la correction des non-conformités d'audits, l'organisation est en mesure d'adapter de manière dynamique sa stratégie de gestion du risque.

Elle devient ainsi capable de faire évoluer son PACS de manière agile et d'anticiper le risque numérique et ses impacts (cf. Figure 6).

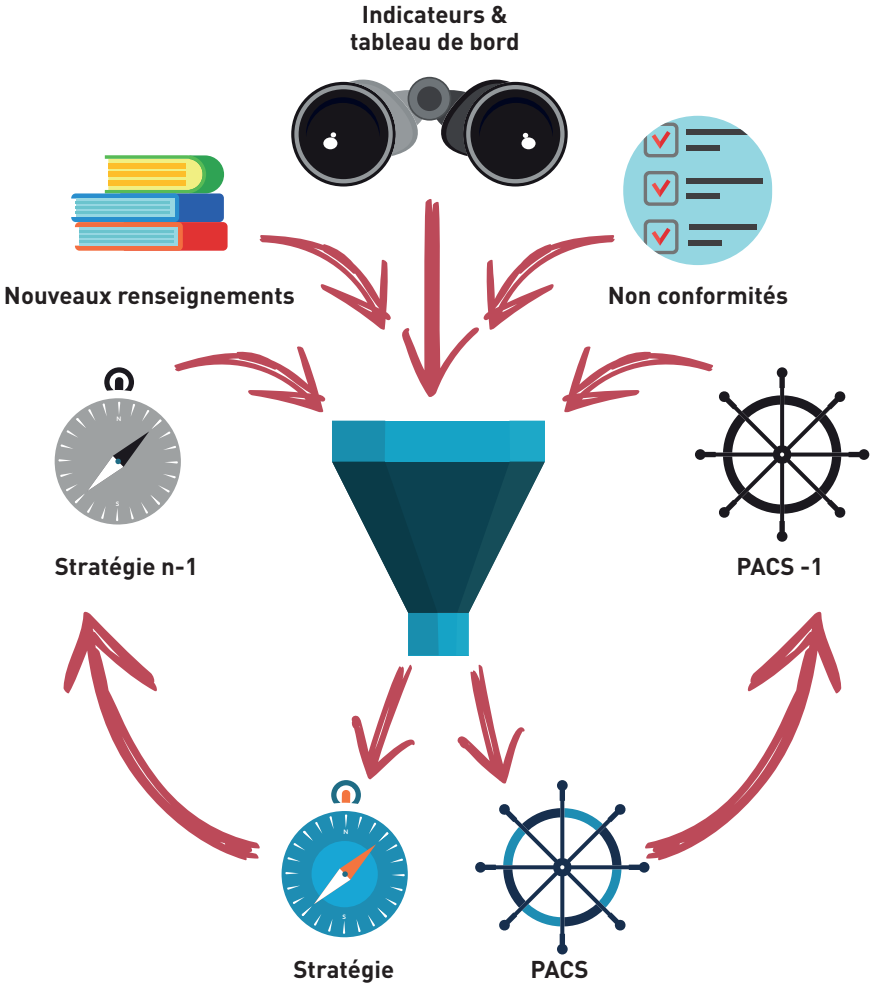


Figure 6 – Cycle d'amélioration continue

Piloter la performance

Pour permettre au comité des risques numériques de piloter correctement la gestion du risque numérique, celui-ci doit se doter d'outils de mesure prenant la forme d'indicateurs (stratégiques, de pilotage, opérationnels, organisationnels ou techniques).

Pour être pleinement exploitables, ces données peuvent par la suite rejoindre des tableaux de bord dynamiques en vue d'obtenir une représentation visuelle de l'atteinte des objectifs et ainsi faire émerger les tendances ou les dérives.

Exemple d'indicateurs		
Stratégiques	**De pilotage**	**Opérationnels**
Etat de la gouvernance du risque numérique	- Fréquence des comités des risques numériques - Fréquence des audits de conformité - Fréquence de revue de la stratégie de traitement des risques - Nombre de dérogations à la PSSI - Fréquence de revue de la réglementation - Fréquence de réévaluation des scénarios de cyberattaque	
Etat du risque numérique	- Taux de couverture des risques - Taux des parties prenantes critiques - Taux d'analyse des risques sur les nouveaux projets - Taux de SI critiques couverts par une homologation - Nombre de non-conformités ouvertes - Taux d'avancement du PACS - Fréquence des tests de PCA	- Nombre de pertes ou vols d'équipements et terminaux - Pourcentage des systèmes identifiés comme vulnérables - Taux de mise à jour antivirus et correctifs sur les postes et serveurs - Nombre de composants opérationnels (matériel et applicatif) obsolètes ou non maintenus

Exemple d'indicateurs		
Stratégiques	**De pilotage**	**Opérationnels**
Etat de la gestion des incidents de sécurité	- Nombre d'incidents de sécurité maitrisés - Nombre d'incidents de sécurité non maîtrisés - Temps d'interruption des activités	- Nombre de cyberattaques détectées - Taux de disponibilité des applications métiers critiques - Pourcentage d'incidents de sécurité en fonction des environnements (messagerie, intranet, extranet, etc.)
Etat de la documentation de sécurité	- Fréquence de revue de la politique de sécurité - Fréquence de revue des processus de sécurité métiers	- Nombre de nouvelles procédures de sécurité rédigées
Etat des actions de sensibilisation, formation et entrainement	- Taux de sensibilisation - Taux de compétence des équipes - Nombre d'exercices de crise réalisés	- Attestations de sensibilisation - Attestations de formation pour les administrateurs

Figure 7 – Exemple d'indicateurs

ÉTAPE 15. Valorisation : la cybersécurité, un avantage compétitif

Evaluer le retour sur investissement des efforts consacrés à la sécurité numérique reste difficile, tout comme de quantifier leurs bénéfices.

En valorisant ces investissements et en adoptant une approche *Cyber Business Partner*, l'organisation peut développer son avantage concurrentiel, aborder de nouveaux marchés, générer de la croissance et faire évoluer positivement et stratégiquement son image.

Développer une approche de type *Cyber Business Partner*

Une gestion structurée du risque numérique portée par une démarche pérenne[48] induit des investissements humains et financiers, dont il est difficile d'apprécier la rentabilité.

A contrario, les parties prenantes poussées par la transformation numérique attendent de l'organisation qu'elle aille au-delà de la simple gestion du risque numérique et qu'elle se positionne véritablement comme un tiers de confiance numérique.

En adoptant une approche *cyber business partner* auprès des acteurs de son écosystème (clients, partenaires, fournisseurs et investisseurs), l'organisation apporte ainsi la garantie d'une maturité cyber compatible avec le seuil d'acceptation du risque de ses parties prenantes.

Elle valorise ainsi les investissements de sa stratégie de sécurité numérique pour les transformer en avantages concurrentiels. L'organisation apporte alors à l'ensemble de son écosystéme des valeurs autres que le coût telles que la confiance, la proactivité ou encore l'optimisation d'investissements[49].

[48] *Cf. Étape 8 – Homologuer ses services numériques critiques*
[49] *Cf. Étape 5 – Définir sa stratégie de sécurité numérique et de valorisation*

Dès lors, l'organisation peut s'appuyer sur cette valorisation comme gage de confiance pour :

- générer de la croissance et saisir des opportunités de développement auprès de ses investisseurs et partenaires ;
- rationaliser et optimiser sa police d'assurance cyber auprès de son assureur ;
- accéder à de nouveaux marchés (notamment sensibles) en se positionnant comme opérateur de confiance maitrisant l'ensemble de la chaine de production et d'approvisionnement.

Enfin, en associant cette démarche à une stratégie de communication, l'organisation influera sur le niveau de maturité cyber de son écosystème et fera évoluer positivement son image de marque.

Aujourd'hui, cet élément commence à être pris en compte par certains organismes tels que les agences de notation. Certaines organisations ont vu l'évaluation de la qualité de leur crédit sanctionnée du fait d'un événement cyber.

Les organisations doivent être capables d'anticiper dès aujourd'hui les attentes futures de clients, de régulateurs et d'investisseurs vis-à-vis de leur capacité à gérer le risque numérique et à leur apporter des garanties.

Bibliographie

Étape 1

FERMA et ECIIA, *At the Junction of Governance and Cyber-security,* FERMA et ECIIA, 2017, www.ferma.eu

IFACI et AMRAE, *Trois lignes de maîtrise pour une meilleure performance,* 2015, www.amrae.fr

Étape 2

ANSSI, *EBIOS Risk Manager*, 2018, https://www.ssi.gouv.fr/ebios

Étape 3

SUTRA G., *Management du risque : une approche stratégique*, Afnor éditions, 2018

Étape 4

ANSSI, *Guides techniques aux recueils de bonnes pratiques*, www.ssi.gouv.fr/bonnes-pratiques

International Organization for Standardization, Famille ISO/IEC 27000 - Systèmes de management de la sécurité de l'information, ISO, www.iso.org

Étape 6

FERMA, BIPAR et Insurance Europe *Preparing for Cyber Insurance*, 2018, www.ferma.eu

Étape 8

ANSSI, *L'homologation de sécurité en neuf étapes simples*, 2017, http://www.ssi.gouv.fr/guide-homologation-securite

SGDSN, *Instruction générale interministérielle n° 1300*, 2011, www.ssi.gouv.fr/igi1300

ANSSI, *Le Référentiel général de sécurité (RGS*), 2014, www.ssi.gouv.fr/rgs

ANSSI, *La Politique de sécurité des systèmes d'information de l'État, (PSSIE)*, 2014, http://www.ssi.gouv.fr/pssie

Étape 9

ANSSI, *Agilité & sécurité numérique – Méthode et outils à l'usage des équipes projet,* 2018, https://www.ssi.gouv.fr/administration/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet

ANSSI, *Recommandations sur le nomadisme numérique*, 2018, www.ssi.gouv.fr/nomadisme-numerique

ANSSI, *Bonnes pratiques à l'usage des professionnels en déplacement*, 2019 - www.ssi.gouv.fr/bonnes-pratiques-professionnels-en-deplacement

Étape 10

CERT-FR, *Les bons réflexes en cas d'intrusion de son système d'information :* CERTA-2002-INF-002, 2002, www.cert.ssi.gouv.fr

Étape 11

International Organization for Standardization, ***ISO 22301:2012 Systèmes de management de la continuité d'activité*****,** 2012, www.iso.org

SGDSN, *Guide pour réaliser un plan de continuité d'activité*, 2015 - www.sgdsn.gouv.fr

DGE, *Plan de continuité d'activité à l'usage du chef d'entreprise en cas de crise majeure*, 2015, www.entreprises.gouv.fr

Autres ressources utiles

AMRAE et CESIN, *Cyber risques - Outil d'aide à l'analyse et au traitement assurantiel*, 2015, www.amrae.fr

IFACI, *Cyber-risques : Enjeux, approches et gouvernance*, 2018, https://docs.ifaci.com

Fédération Française de l'Assurance, *Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise*, 2017, www.ffa-assurance.fr

ANSSI, *Guide pour la cartographie du système d'information,* 2018, www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation

AMRAE, *La Cartographie: un outil de gestion des risques*, Collection Maîtrise des Risques, 2010, www.amrae.fr

AMRAE, *La Communication sur les Risques,* Collection Maîtrise des risques, 2016, www.amrae.fr

AMRAE, PME et ETI ; *La gestion des risques est aussi pour vous !*, Collection Maîtrise des risques, 2018, www.amrae.fr

IFIE et AMRAE, *Le Risk Manager & l'Intelligence Economique*, Collection Maîtrise des risques, 2010, www.amrae.fr

AMRAE, *Les Plans de Continuité d'Activité,* Collection Maîtrise des risques, 2015, www.amrae.fr

CLUSIF et AMRAE, *Risk Manager et Responsable sécurité du système d'information : deux métiers s'unissent pour la gestion des risques liés aux Systèmes d'Information,* Collection Maîtrise des risques, 2008, www.amrae.fr

AMRAE, *Trajectoire vers un Enterprise Risk Management*, Collection Maîtrise des risques, 2012, www.amrae.fr

IRT System X, *La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance*, www.irt-systemx.fr

DARSA J.-D. et DUFOUR N., *Le coût du risque - Un enjeu majeur pour l'entreprise,* GERESO édition, 2018, 2e édition

Revue de la Gendarmerie nationale, *Sécurité et vie privée by design,* décembre 2018

Lcl TORRISI C., *kit de sensibilisation des atteintes à la sécurité économique, édité par l'INHESJ et la DGGN,* 2019, https://inhesj.fr https://www.gendarmerie.interieur.gouv.fr

Association pour le Management des Risques et des Assurances de l'Entreprise
AMRAE • 80 boulevard Haussmann 75008 Paris
www.amrae.fr • amrae@amrae.fr

Agence nationale de la sécurité des systèmes d'information
ANSSI • 51, boulevard de la Tour-Maubourg • 75 700 PARIS 07 SP
www.ssi.gouv.fr • communication@ssi.gouv.fr

Elaborée par l'ANSSI et l'AMRAE, la démarche décrite dans ce guide s'appuie sur l'expérience des principaux acteurs de la maitrise du risque numérique.
En 15 étapes, cet ouvrage de référence accompagne les dirigeants et dirigeantes des organisations publiques ou privées de toute taille dans une démarche qui draine des enjeux stratégiques, économiques, d'image...
Parce que demain, l'organisation responsable et génératrice de confiance sera celle qui s'attache à maitriser le risque numérique, leurs directions doivent le comprendre, soutenir les mesures nécessaires et apprendre à valoriser cet investissement.

www.amrae.fr
www.ssi.gouv.fr

9 791097 351014

ISBN : 979-10-97351-01-4