L'atout confiance
Maîtriser le risque numérique pour construire la cyber-résilience

Par **Fabien CAPARROS**
Agence nationale de la sécurité des systèmes d'information (ANSSI)

Figure 1 : Extrait de "Risk in focus 2021", enquête annuelle IFACI & ECCIA

Avoir confiance en son activité numérique

Précisons les termes. Pour une organisation, un risque stratégique peut être défini au travers de trois caractéristiques : elle ne peut y échapper ; l'impact est potentiellement mortel ; et elle ne peut le transférer totalement. Son caractère systémique signifie pour l'organisation que sa propre cybersécurité est aussi importante que celle de son écosystème.

Étant donné la nature à la fois stratégique et systémique du risque numérique pour une organisation, sa gestion est de la responsabilité du dirigeant. Elle ne peut être ni déléguée ni externalisée. Pour bien comprendre la nature du risque numérique en 2020, reprenons l'analogie développée par Knake et Clarke dans leur dernier livre *The Fifth Domain* (2019). Au cours de la décennie 2000, dans un cyberespace encore juvénile, la menace était principalement un virus ou un ver informatique. La probabilité pour une organisation d'être touchée grandissait mais restait supportable : le risque était technique. Dès lors, **2000 a été la décennie de la protection** et a vu la création de solutions techniques, tels les *firewalls* et autres antivirus. Puis, la décennie 2010 a

vu l'importance du cyberespace croître et de nouvelles menaces surgir, capables de contourner les protections pour viser des cibles stratégiques, comme les infrastructures. Ces menaces, dénommées *advanced persistent threats* (APT), ont fait évoluer le risque pour les organisations les plus essentielles à une nation. Il a donc fallu de nouvelles capacités pour les détecter et les contrer, avec leur lot d'acronymes : SOC, SIEM, CERT [1]... **2010 fut ainsi la décennie de la défense**. En 2020, avec le développement de la cybercriminalité, d'une part, et l'importance prise par le cyberespace, d'autre part, qui plonge les organisations dans des écosystèmes numériques profondément interconnectés et interdépendants, toutes les organisations sont concernées, quels que soient leur taille ou leur secteur. Le risque est devenu à la fois stratégique et systémique, et aucune organisation ne pourra vraisemblablement franchir cette décennie sans subir une attaque sérieuse, directe ou indirecte. **2020 sera donc la décennie de la résilience.**

Pour gérer un tel risque, le dirigeant d'une organisation aura besoin d'analyses de risque dédiées à la décision stratégique, de mettre en place une gouvernance adaptée, et de s'appuyer sur de nouvelles compétences. Le management du risque numérique consiste à éclairer la décision pour trouver le bon compromis entre exposition au danger, coût, et gains opérationnels espérés. Le domaine étant très technique, tant que le risque était également technique, cette décision était déléguée à l'expert qui pouvait garder la complexité à son niveau. Mais, dès lors que le risque est devenu stratégique, la responsabilité est revenue au décideur. Celui-ci doit, certes, monter personnellement en compétence, mais il ne va pas devenir pour autant un ingénieur en cybersécurité. L'analyse de risque qui permettait jusqu'alors à l'ingénieur de créer un système sécurisé au bon niveau doit, aujourd'hui, être un outil d'aide à la décision stratégique pour un décideur. Par ailleurs, la mise en œuvre des mesures de réduction du risque n'est plus limitée à l'utilisateur final, mais implique toutes les ressources de l'organisation, les trois lignes de défense chères aux managers des risques [2]. En conséquence, la gouvernance du risque et l'expertise évoluent au sein de l'organisation pour éclairer à la fois les fonctions techniques transverses en charge des technologies de l'information, les fonctions opérationnelles au cœur des différents métiers et les fonctions de direction.

Face à ce constat, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est engagée avec ses partenaires dans une profonde refonte de sa doctrine de management du risque numérique. Dans un premier temps, le moteur a été repensé **:** la méthode d'analyse des risques numériques de l'ANSSI, EBIOS, avait été créée au début des années 2000, à l'instar des autres méthodes du domaine. Elle avait été régulièrement améliorée, mais restait inaccessible pour un non-expert. Sa nouvelle version, **EBIOS Risk Manager**, élaborée conjointement avec le club EBIOS [3], est ainsi pensée comme un outil d'aide à la décision stratégique, qui offre une vision partagée des risques pour les décideurs et les métiers. Puis, fruit d'une collaboration avec l'AMRAE [4], le guide « Maîtrise du risque numérique, l'atout confiance » propose une démarche progressive pour mettre en place une gouvernance du risque cyber au sein de l'organisation. Enfin, ces publications sont complétées par une collection de guides dédiés à la gestion des crises cyber et à un panorama des nouveaux métiers de la sécurité du numérique.

À l'heure de l'informatique en nuage, des services numériques et des attaques informatiques *via* la *supply chain*, la confiance en ses propres capacités à gérer les risques ne suffit plus. La confiance en ses partenaires numériques est tout aussi importante.

(1) *security operation center* (SOC) ; *security information and event management* (SIEM) ; *computer emergency response team* (CERT).
(2) Le modèle de la maîtrise des risques autour de trois lignes de défense est promu par les associations françaises AMRAE et IFACI depuis 2013. Il fait référence dans le domaine.
(3) Le club EBIOS est une association à but non lucratif qui regroupe les praticiens et les amateurs de la méthode EBIOS.
(4) L'AMRAE (Association pour le management des risques et des assurances de l'entreprise) est l'association professionnelle de référence des métiers du risque et des assurances en entreprise.

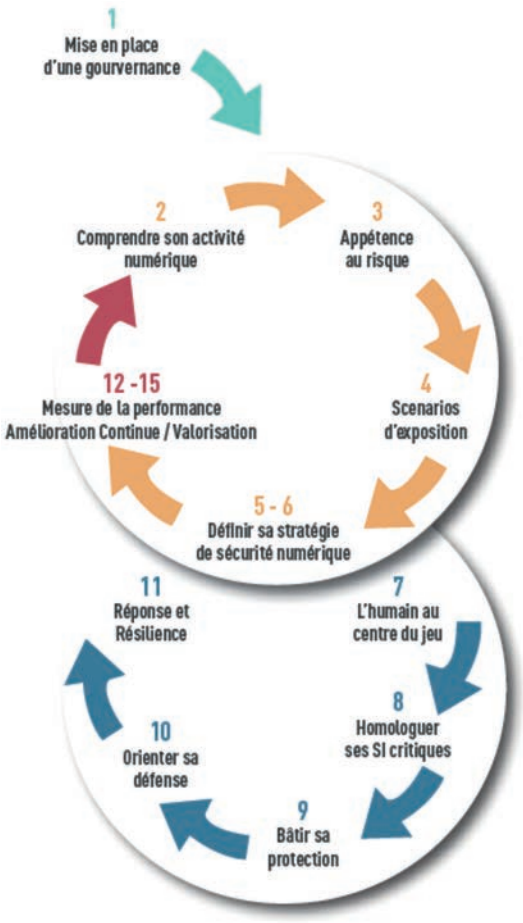

Figure 2 : démarche progressive de construction d'une gouvernance des risques cyber, extrait du guide « Maîtrise du risque numérique, l'atout confiance »

Avoir confiance en ses partenaires numériques

La question n'est pas d'avoir confiance dans le sérieux de ses partenaires numériques, mais de connaître, de renforcer et de surveiller la solidité des liens qui nous unissent à eux et les risques que cela induit. J'ai réalisé ma première analyse de risque EBIOS Risk Manager une année avant la parution de la méthode, en 2018, auprès d'une PME qui opère une plateforme informatique chargée de gérer les flux logistiques d'un grand port de France. Elle interconnecte ainsi toutes les parties prenantes publiques et privées du port. Lorsqu'on a évoqué la confiance qu'ils pouvaient avoir envers leurs partenaires numériques, à l'aune de l'attaque qui a frappé le port d'Anvers en 2011 [5], certains transitaires ont été qualifiés avec humour de « truands-sitaires »… De la même manière, l'attaque NotPetya [6], en 2017, a utilisé comme vecteur d'infection un logiciel de comptabilité imposé par les services administratifs ukrainiens aux entreprises commerçant en Ukraine. Pourtant, dans ces deux situations, il n'est pas question de se passer de ces liens numériques qui unissent les organisations à des partenaires privés ou publics. Il convient donc d'évaluer les risques, de prendre les mesures adéquates et de gérer les risques résiduels. Nous sommes bien dans le champ du management du risque.

Néanmoins, l'évaluation de son écosystème numérique n'est pas chose aisée. Après presque deux années depuis le lancement d'EBIOS Risk Manager, il ressort que les organisations sont encore peu matures dans ce domaine. Prenons l'exemple d'une analyse de risque dans un aéroport. Naturellement, la question du risque terroriste vient en premier. Mais quand vous creusez les aspects métiers, il ressort que le chiffre d'affaires dépend en grande partie de l'exploitation des parkings. Or, ces parkings sont opérés par des partenaires externes, comme Q-Park ou Vinci, entre autres. Si le service venait à être indisponible, les pertes d'activité seraient rapidement très importantes. Quel est le niveau de dépendance vis-à-vis du service numérique fourni par le partenaire (prend-il en charge la perte d'activité éventuelle, l'atteinte à l'image…) ? Quel est son

(5) Le port d'Anvers a été victime d'une attaque particulièrement sophistiquée en juin 2011. Une *mafia* était parvenue à prendre le contrôle du système informatique dédié à la gestion des conteneurs pour pouvoir importer illégalement de la drogue.

(6) L'attaque informatique NotPetya a frappé en 2017 un grand nombre d'entreprises ayant des activités en Ukraine. Particulièrement destructrice, elle a paralysé les activités de nombreuses entreprises dont des multinationales pendant plusieurs jours, voire semaines, et a entraîné des dommages estimés par les autorités américaines à plus de 10 milliards de dollars.

niveau de pénétration dans les systèmes de l'aéroport lui-même s'il était le vecteur d'une attaque (souvenez-vous de NotPetya) ? Quel est son niveau de maturité en cybersécurité ? Peut-on avoir confiance en lui (souvenez-vous des « truands-sitaires ») ? À travers ces quatre questions, EBIOS Risk Manager propose, d'une part, d'évaluer pour chaque partenaire la criticité de la relation afin de doser l'effort que l'on va consentir dans la sécurisation de la relation, et, d'autre part, de faire une cartographie des risques sous forme de radar pour définir une stratégie dédiée à la gestion globale des partenaires numériques. Cette cartographie permet à la fois d'orienter l'effort de sécurité là où il est nécessaire et de diffuser largement la démarche au sein de toute l'organisation. Mais si les questions semblent simples, il ressort que les organisations sont aujourd'hui rarement en mesure d'y répondre. La confiance est donc donnée *a priori*, sur la base d'éléments fragiles, sans réaliser les risques pris, ce qui explique pour partie l'inquiétude des décideurs face au risque numérique (voir Figure 1).

En outre, le partage des responsabilités et des coûts liés à la cybersécurité est souvent mal maîtrisé par les organisations. Il est clair aujourd'hui que la sécurité est perçue comme un coût. Or, entre deux partenaires, la question du partage des coûts mérite d'être posée. Si nous caricaturons un peu : un responsable de la sécurité des systèmes d'information aura tendance à vouloir maîtriser au maximum sa propre sécurité. Il sera donc tenté de l'internaliser de manière à utiliser un système d'information capable d'évoluer dans un environnement extérieur en lequel il n'aura pas confiance *a priori*. *A contrario*, un acheteur voudra reporter l'effort sur le partenaire, quitte à faire jouer la concurrence pour que celui-ci prenne au maximum sa part. En attendant l'avènement éventuel du *Zero Trust Network* [7], la solution se situe entre les deux options.

Se pose alors la question de la responsabilité en cas d'attaque. Il suffit de regarder les clauses de limite de responsabilité imposées par certains *cloud providers* pour se convaincre que cette question est loin d'être anodine. Vient alors la couverture assurantielle. Là aussi, l'âge de la confiance sans

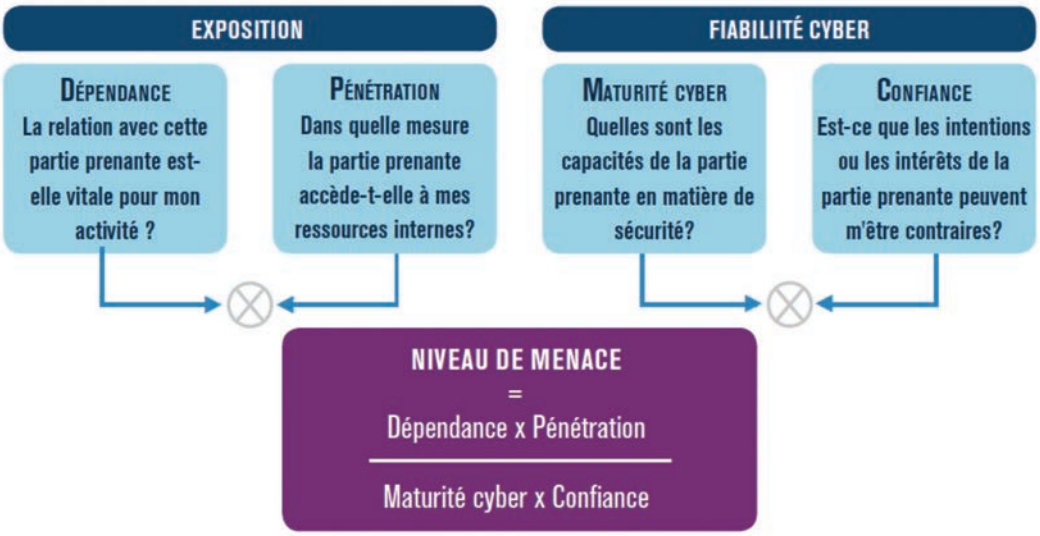

Figure 3 : évaluation du risque lié à une relation numérique avec un partenaire, d'après la méthode EBIOS Risk Manager

(7) Les modèles *Zero Trust* font l'hypothèse que le système d'information d'une organisation, même contrôlé, peut être compromis ou peut abriter une menace intérieure. Ils préconisent donc de considérer l'ensemble de la chaîne de connexion depuis l'usager, de segmenter les ressources, de développer les contrôles et de cesser de faire dépendre l'accès aux ressources de la présence ou non au sein du périmètre du SI.

réelle maîtrise est terminé. Les régulateurs ayant imposé aux assureurs de faire une revue de leurs couvertures dites « silencieuses », le marché s'est durci, et les assureurs sont très regardants face à leur propre exposition à un risque systémique.

Après la confiance dans son activité et la confiance dans ses relations avec ses partenaires numériques, vient la question de la confiance dans son environnement. Comment structurellement mettre en place des mécanismes vertueux pour renforcer la cyber-résilience de son écosystème numérique ?

Avoir confiance en son environnement numérique

Alors que les écosystèmes numériques sont de plus en plus imbriqués, interconnectés et interdépendants, utiliser le management des risques pour améliorer la transparence des offres au sein des chaines de valeur permettrait de bâtir des chaines de confiance. La crise sanitaire en cours a donné un nouvel éclairage sur la question de la confiance entre un offreur et un acheteur au sein d'une chaine de valeur, et a montré les insuffisances du modèle actuel. Au moment de choisir les bons prestataires de visioconférence, le débat autour de la sécurité numérique a été vif comme en témoigne le cas révélateur des offres de la société Zoom [8]. Dans ce contexte, le système actuel de certification de sécurité n'a pas apporté un éclairage suffisant. L'idée d'une meilleure transparence dans les offres est alors apparue et est actuellement étudiée au sein de l'OCDE. Ainsi, au travers d'une démarche d'analyse de risque pertinente et adoptée à la fois par les acheteurs et les offreurs, il pourrait être possible pour les acheteurs de définir les bonnes mesures de sécurité nécessaires dans leur contexte d'emploi et pour les offreurs de se différencier. En complément ou au travers des certifications de sécurité, cette transparence dans les offres pourrait permettre de construire des chaines de confiance au sein des écosystèmes numériques.

Dès à présent, les parties prenantes d'un même écosystème numérique réclament des gages de confiance, notamment les clients des entreprises et les usagers des administrations. Plutôt que d'être considéré comme un coût, l'effort de sécurité peut donc être valorisé au sein des offres de valeur privées ou des missions de service public. Si l'analyse semble évidente, la mise en œuvre est plus difficile. Faire travailler ensemble les responsables de la sécurité du numérique et les responsables métiers ne va pas de soi. Cela a amené l'ANSSI et l'AMRAE à proposer dans le guide « l'atout confiance » une gouvernance mixte, qui intègre le métier dans les comités de management du risque cyber. Ainsi, il devient possible de bâtir des stratégies qui allient sécurité du risque numérique et valorisation des efforts de sécurité. Un euro dépensé pour la sécurité peut alors être un euro valorisé pour répondre à la demande d'une relation de confiance de la part des clients ou des usagers.

Enfin, le plus grand moteur de la résilience d'un écosystème numérique est le système assurantiel. Or aujourd'hui il n'est pas encore en mesure de remplir son office. Pour pouvoir être pleinement efficace, un système assurantiel doit partager un état de l'art à peu près stabilisé et ainsi agir à la fois sur la réduction du risque individuel et du risque systémique. En premier lieu, cela concerne les mesures de sécurité pour réduire le risque, ce que nous appelons « le socle de sécurité » dans EBIOS Risk Manager. C'est sans doute le domaine le plus mature aujourd'hui. À ces mesures de sécurité doit être associé un système d'inspection et d'évaluation de référence, en lequel les différentes parties ont confiance. Ce système peut être transversal ou sectoriel, comme les certifications des navires marchands pour le secteur du transport maritime. Puis vient la connaissance de la menace pour, d'une part, connaître les modes d'action actuels, les cibles, mais

(8) Durant les premiers mois de la crise sanitaire, la société Zoom qui offre des solutions de visioconférence a fait l'objet de sévères critiques mettant en cause la sécurité de ses solutions.

également anticiper les tendances. D'autre part, cette connaissance doit être statistique pour bâtir des modèles agrégés de prédiction des impacts financiers. Enfin, se pose la question de l'aspect systémique du risque qui doit être couvert par des mécanismes dédiés, comme la réassurance ou les systèmes de type « catastrophe naturelle » qui impliquent davantage l'État. Dans tous ces domaines, l'état de l'art n'est pas encore suffisamment stabilisé, mais les acteurs du système assurantiel innovent et progressent, sous le regard attentif de leurs régulateurs.

Conclusion

Pour une organisation, publique comme privée, le management du risque numérique permet de mieux appréhender la question de la confiance dans son activité numérique. Devant la complexité du risque, ses aspects stratégiques et systémiques, ce management nécessite de bâtir la confiance dans son organisation et ses capacités propres autant que dans ses liens avec ses différents partenaires. Il requiert également d'œuvrer à la construction de mécanismes vertueux de cyber-résilience, qui amèneront la confiance au cœur de l'écosystème numérique.

Si l'on peut légitimement ne pas partager l'optimisme excessif de Clarke et Knake, qui annoncent la victoire inéluctable de la sécurité des organisations contre les cyberattaquants, nous les rejoindrons bien volontiers sur le fait que 2020 sera la décennie de la cyber-résilience.

Bibliographie

IFACI & ECIIA (2020), "Risk in focus 2021", rapport.

CLARKE R. & KNAKE R. (2019), *The fifth domain,* New York, Penguin press.

ANSSI (2018), « La méthode EBIOS Risk Manager ».

ANSSI (2019), « Maîtrise du risque numérique, l'atout confiance ».

ANSSI (2020), « Organiser un exercice de gestion de crise cyber ».

ANSSI (2020), « Panorama des métiers de la cybersécurité, édition 2020 ».

ANSSI (à paraître), « Gérer une crise cyber ; La communication de crise face à une crise cyber ».