Retrouver des leviers de souveraineté dans le cyberespace grâce à une meilleure organisation des missions dans le champ de la cybersécurité

Par Hugo ZYLBERBERG
Chef d'État-Major de la sous-direction Stratégie de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Dans un environnement cyber désormais caractérisé par l'instabilité numérique, il est essentiel de retrouver des leviers d'action pour mieux prendre en compte le risque cyber à tous les niveaux des organisations. À cet effet, l'organisation de l'État semble utile pour identifier des fonctions prioritaires et des objectifs stratégiques qui permettent de répondre concrètement à ces enjeux majeurs de cybersécurité.

Introduction

La transformation numérique des dernières décennies plonge les organisations publiques et privées dans un environnement nouveau : après une longue période de développements numériques tous azimuts, le risque cyber qui caractérise désormais l'environnement numérique les force à s'intéresser à leur cybersécurité.

Dans ce contexte de plus en plus marqué par l'instabilité numérique où de grandes cyberattaques font régulièrement l'actualité, les dirigeants s'intéressent de plus en plus fréquemment et intensément aux risques cyber. Dans les *Global Risks Report* annuels du World Economic Forum[1], le risque cyber est par exemple mentionné comme l'un des risques majeurs en 2012 puis en 2014, avant d'être systématiquement mentionné depuis 2019.

Cependant, cette rapide transformation numérique peut donner la sensation de manquer de leviers d'action pour traiter ces risques. Dès 2014, Pierre Bellanger écrit ainsi « nous sommes à cet instant le garde-manger, le minerai numérique ou encore l'éventuel champ de bataille » des puissances numériques[2], un rôle essentiellement passif où les leviers d'action appartiennent à d'autres acteurs. Pourtant, les leviers de gouvernance et de décision dont disposent les dirigeants n'ont pas miraculeusement disparus : ils doivent être adaptés à l'ère cyber – voire remplacés par de nouveaux lorsqu'ils sont devenus obsolètes.

[1] Voir par exemple l'édition 2023 du WEF Global Risks Report accessible en ligne : https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

[2] BELLANGER P. (2020), « Trois empires et un garde-manger », *Le Débat*, vol. 209, n°2, pp. 57-64.

Le risque cyber et ses caractéristiques

Description de l'environnement de risque cyber

L'environnement numérique se caractérise par son instabilité. Selon le baromètre annuel du Club des experts de la sécurité de l'information et du numérique (CESIN), « plus d'une entreprise sur deux considère toujours que le niveau de menaces en matière de cyber espionnage est élevé (50 %) »[3]. L'impact du risque cyber dépend cependant de la taille de l'organisation qui en est victime. L'Association pour le management des risques et des assurances de l'entreprise (AMRAE) indique que les entreprises de taille moyenne ont déclaré des sinistres à hauteur de 4,5 millions d'euros en 2022, un chiffre qui a presque doublé par rapport à une enquête similaire réalisée en 2021. Pour les plus petites entreprises, la situation est probablement du même ordre, même si les chiffres manquent pour venir étayer cette situation. Plus globalement, les assureurs ont encaissé 316 millions d'euros de primes dédiées à la couverture des risques numériques en France, soit un bond de 72 % par rapport à 2021[4].

En outre, à l'inverse d'autres catégories de risques accidentels pour lesquels il est possible de bénéficier de modélisation afin de les rendre plus prévisibles, le risque cyber est par nature stratégique : un acteur malveillant se trouve de l'autre côté du clavier, et tente de faire réussir l'attaque. Pour se défendre, il est donc nécessaire de se prémunir de toutes les attaques qu'il peut concevoir – alors que pour l'attaquant, une seule faille est suffisante.

La prise en compte du risque cyber dans les organisations

Pour y faire face, les stratégies de gestion des risques commencent nécessairement par leur identification : quels sont les risques cyber majeurs auxquels je dois faire face, et comment puis-je y répondre ? Afin de caractériser ces risques cyber, la méthode EBIOS RM[5] propose deux composantes : une source de risque et un objectif visé.

La source de risque est définie comme un « élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque ». Une source de risque peut être caractérisée par sa motivation, ses ressources, ses compétences, ses modes opératoires (de prédilection). À titre d'exemple, des groupes criminels, des services étatiques, des concurrents ou des employés internes peuvent tous être considérés comme des sources de risque. L'objectif visé est la finalité de l'attaque : par exemple obtenir le paiement d'une rançon, obtenir des informations privilégiées à des fins d'espionnage industriel, exercer une vengeance…

Pour identifier des risques, la méthode EBIOS RM permet d'abord d'identifier des scénarios stratégiques d'attaque : qu'est-ce qu'un attaquant pourrait vouloir attaquer ? L'objectif de cette première étape est de comprendre ce que des attaquants pourraient vouloir attaquer. Une entreprise de services numériques pourra par exemple vouloir préserver la confidentialité des informations de ses clients, alors qu'une entreprise de biotechnologies pourra s'attacher davantage à l'intégrité de ses données de recherche. Dans tous les cas, le risque opérationnel portant sur la continuité d'activité peut consti-

[3] L'édition 2022 du baromètre du CESIN est accessible en ligne : https://www.cesin.fr/articles-slug/?slug=1432-8%C3%A8me%20%C3%A9dition%20du%20barom%C3%A8tre%20annuel%20du%20CESIN

[4] L'édition 2023 de l'étude LUCY - Lumière sur la cyberassurance est accessible en ligne : https://www.amrae.fr/bibliotheque-de-amrae?combine=&ref_id=4626&ref_type=publication&items=4626

[5] Les documents relatifs à la méthode EBIOS RM sont disponibles en ligne : https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

tuer une cible privilégiée des attaquants car cela leur permet de demander une rançon aux victimes afin de pouvoir redémarrer leur activité.

Une fois ces risques identifiés, il s'agit de trouver des leviers d'action permettant soit de réduire leur probabilité d'occurrence, soit de réduire leur impact lorsqu'ils surviennent. S'il existe des modèles permettant aux organisations de mesurer leur maturité ou leur niveau de cybersécurité, il n'existe pas encore de modèle général d'organisation des activités relatives à la cybersécurité des organisations.

Afin de gérer leurs risques cyber en mettant en œuvre une stratégie, les dirigeants doivent donc répondre à la question suivante : comment concevoir et gouverner les leviers d'action dont disposent les organisations pour maîtriser leurs risques cyber ?

De quels leviers d'action disposent les organisations pour répondre à ce nouvel environnement de risque cyber ?

L'organisation de l'État pour assurer ses missions dans le champ de la cybersécurité permet d'éclairer les différents leviers dont disposent les organisations. Les travaux de la *Revue stratégique de cyberdéfense* de 2018 ont en effet abouti à la définition de plusieurs missions, et à la création d'un ensemble d'instances qui forment la gouvernance cyber de l'État en matière de lutte informatique défensive.

Cette gouvernance cyber recouvre désormais trois champs d'action prioritaires qui font chacun l'objet d'une comitologie dédiée :

- l'amélioration du niveau de cybersécurité de l'État ;
- la prise en compte des enjeux de sécurité numérique dans les politiques publiques ;
- la réponse aux agressions.

Transposés aux organisations publiques comme privées, ces trois champs d'action offrent une structure qui permet de catégoriser et d'identifier les leviers d'action à la disposition de leurs dirigeants.

L'amélioration du niveau de cybersécurité

Ce premier champ d'action concerne autant les mesures de cybersécurité mises en place au sein des infrastructures numériques que les outils et les services spécifiquement dédiés à la cybersécurité. Il s'agit donc d'une part d'exigences vis-à-vis des équipes qui déploient et maintiennent le système d'information et d'autre part de ressources informatiques en propre destinées à assurer la cybersécurité de l'organisation. La sécurité de la chaîne d'approvisionnement matérielle et logicielle des organisations constitue en particulier un point d'attention majeur pour maîtriser ses dépendances et obtenir une compréhension de son environnement de risque la plus fidèle possible.

L'objectif de ces activités est de parvenir à identifier les éléments les plus sensibles au sein d'un système d'information parfois tentaculaire et de définir une stratégie permettant d'atteindre un niveau de sécurité suffisant pour prévenir les risques au sein du système d'information.

La prise en compte des enjeux de sécurité numérique dans les projets

Ce second champ d'action concerne l'intégration de la sécurité dans les projets de l'organisation et la sensibilisation des métiers au risque cyber. Il s'agit donc de définir un

processus par lequel les projets doivent anticiper, prendre en compte et répondre à leurs propres risques de cybersécurité.

L'objectif de ces activités est de parvenir à anticiper les nouveaux risques que les projets issus des métiers peuvent occasionner et de conseiller les porteurs de projets pour leur permettre d'y répondre.

La gestion des incidents de cybersécurité

Ce troisième champ d'action concerne la réaction d'une organisation face à ses incidents de cybersécurité. Il s'agit donc de parvenir, le plus rapidement possible, à lever le doute concernant les incidents en cours et d'en limiter la durée et l'impact.

L'objectif de cette troisième activité est de mettre en place des processus d'escalade permettant d'éviter que les incidents ne se transforment en crise et de gérer les crises qui doivent l'être.

Chaque champ d'action constitue ainsi une fonction qui peut être confiée à différentes personnes au sein d'une organisation mais sans laquelle la prise en compte des risques cyber sera insuffisante.

Conclusion

La stratégie cyber de grandes organisations pourrait utilement s'appuyer sur cette structure afin d'effectuer un diagnostic des missions, rationaliser leur gouvernance et fixer des objectifs qui permettent de retrouver des leviers d'action dans le cyberespace. Cependant, cette prise en compte se heurte à un autre obstacle : celui des talents.

Selon certaines études[6], le secteur de la cybersécurité (estimé à plus de 4,5 milliers de personnes en 2022), manquerait encore de près de 3,5 milliers de professionnels. Pour la France, l'Observatoire des métiers de la cybersécurité de l'ANSSI a publié en 2022 une étude sur l'attractivité et la représentation des métiers de la cybersécurité[7]. Il reste cependant beaucoup à faire pour favoriser la croissance d'un écosystème de formations, techniques et non techniques, initiales et continues, qui attirent une diversité de profils afin de garantir qu'outre une bonne organisation des missions de cybersécurité, ces missions soient attractives et pourvues pour faire face à cet immense défi.

[6] Voir par exemple le Cybersecurity Workforce Study de (ISC)² accessible en ligne : https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[7] L'enquête 2022 de l'Observatoire des métiers de la cybersécurité de l'ANSSI est accessible en ligne : https://www.ssi.gouv.fr/uploads/2021/10/20221115_observatoire_enquete_2022.pdf