RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

REMPAR25

RETOUR D'EXPÉRIENCE DE L'EXERCICE DE CRISE D'ORIGINE CYBER MASSIFIÉ REMPAR25

SOMMAIRE

REMPAR25 : un exercice national unique et ouvert à tous pour améliorer la résilience cyber collective — 3

REMPAR25, une nouvelle édition qui passe à l'échelle pour accompagner l'ensemble du territoire national — 5

1. Un exercice massifié qui démontre la capacité de la France à s'entraîner à grande échelle pour faire face à une cyberattaque systémique fictive, mais crédible — 6

2. Un exercice avec une forte représentativité des différents secteurs d'activité, répartis sur l'ensemble du territoire — 11

3. Un exercice massifié qui permet d'évaluer le niveau de préparation de la Nation — 15

4. Plusieurs axes d'effort pour renforcer la résilience des organisations se dessinent pour les prochaines années — 24

Pour aller plus loin — 30

Annexe – Liste des partenaires — 31

REMPAR25 : UN EXERCICE NATIONAL UNIQUE ET OUVERT À TOUS POUR AMÉLIORER LA RÉSILIENCE CYBER COLLECTIVE

Le 18 septembre 2025, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a organisé l'exercice massifié REMPAR25, avec le soutien du Campus Cyber national, du Club de la continuité d'activité (CCA), du Club de la sécurité de l'information français (CLUSIF), du Club des experts de la sécurité de l'information et du numérique (CESIN) et d'au total 52 partenaires répartis sur l'ensemble du territoire.

Durant l'ensemble de la journée, ce sont près de 5 680 professionnels qui ont participé à l'exercice, dont 50 % de participants dont les métiers ne relevaient ni du numérique ni de la cybersécurité. Issus de 1 263 organisations publiques et privées, réparties dans 13 régions et 9 territoires ultramarins. Ils ont été invités à réagir aux impacts d'une crise d'origine cyber systémique, simulant une interruption massive des services numériques essentiels et conduisant à des impacts dans de multiples secteurs et pour de nombreux acteurs. Ce scénario de black-out numérique, qui fait la particularité des éditions REMPAR, a révélé l'importance cruciale des plans de continuité d'activité, et la nécessité pour chaque organisation d'intégrer la gestion de crise d'origine cyber dans sa stratégie, de manière proactive et collaborative avec l'ensemble des fonctions d'une organisation.

Après REMPAR22, qui avait rassemblé 550 participants venus de 100 entités franciliennes, cette nouvelle édition s'adressait aux organisations de toute nature sur l'ensemble du territoire français, en mettant en avant la pluridisciplinarité nécessaire au traitement des crises d'origine cyber.

Cet exercice, au travers de l'entraînement des niveaux opérationnels et stratégiques, s'inscrivait pleinement dans les objectifs visés par la directive NIS 2, ainsi que dans l'objectif stratégique de la Revue nationale stratégique, qui vise à doter la France d'une résilience cyber de premier rang.

Il regroupait cinq objectifs principaux et complémentaires :

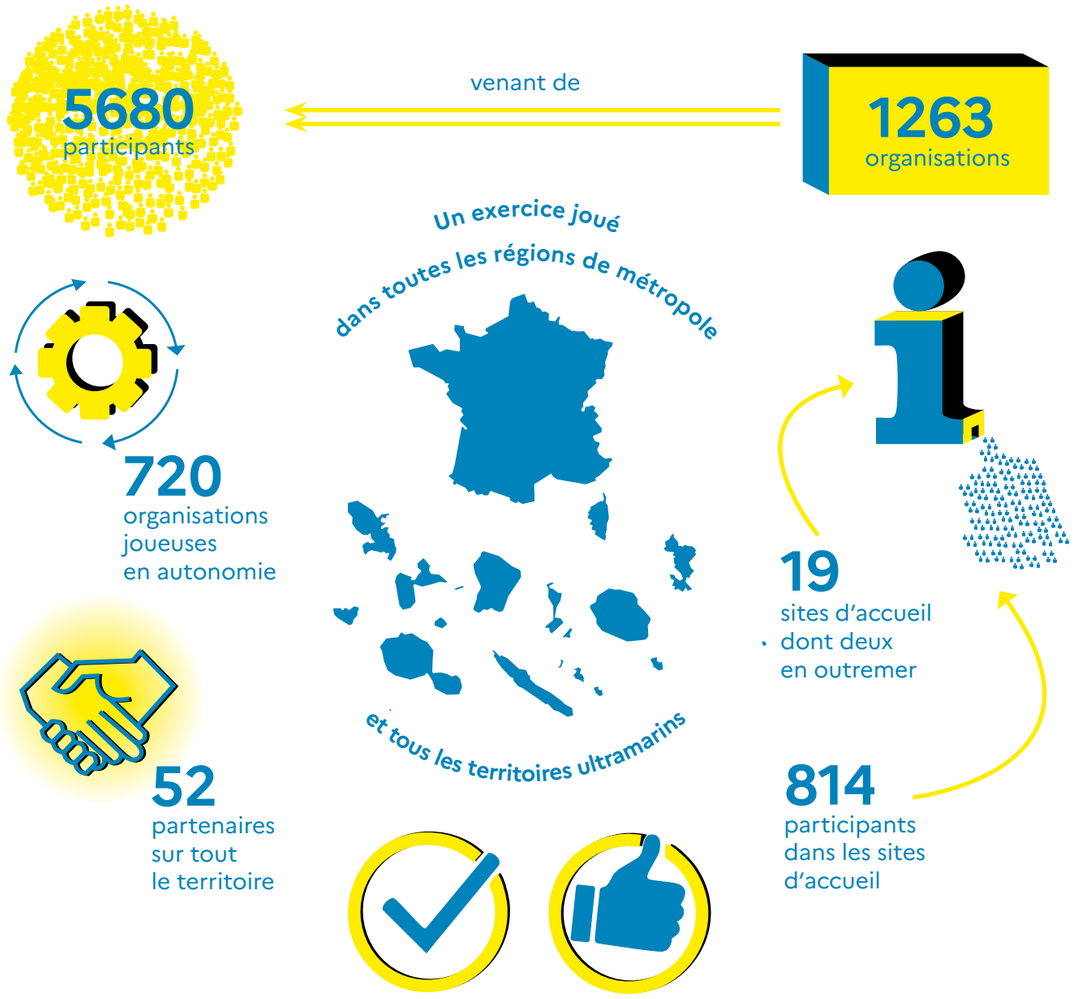
- → **01 —** Sensibiliser les non-experts de la cybersécurité ;
- → **02 —** Entraîner l'écosystème français aux enjeux de gestion de crise d'origine cyber ;
- → **03 —** Éprouver les capacités des organisations à réagir et tenir dans la durée ;
- → **04 —** Aborder la question de l'anticipation ;
- → **05 —** Introduire la notion de continuité d'activité.

L'ANSSI encourage les organisations à se saisir de ce retour d'expérience et du kit prêt à l'emploi pour le déployer. Les exercices de crise sont un outil efficace pour disposer d'une compréhension partagée des enjeux par des équipes pluridisciplinaires. La meilleure manière de gérer une crise d'origine cyber, c'est de s'y préparer.

« Organiser un exercice de cette ampleur, plus de 5 000 participants venant de plus de 1 200 organisations à travers toute la France, était un défi que nous avons collectivement relevé. La menace cyber est une réalité au quotidien. La France doit se préparer à gérer des crises d'origine cyber multiples. Toute organisation peut être amenée à gérer une crise d'origine cyber, d'où l'importance de s'entraîner pour être prêt le jour J. »

Vincent Strubel, Directeur général de l'ANSSI

REMPAR25 : UNE NOUVELLE ÉDITION QUI PASSE À L'ÉCHELLE POUR ACCOMPAGNER L'ENSEMBLE DU TERRITOIRE NATIONAL



Pour près de **95 %** des participants, **REMPAR25** a été l'occasion de mettre en place des actions sur les volets gestion de crise et/ou SSI.

REMPAR25 a répondu aux attentes de plus de 99 % des répondants

1. UN EXERCICE MASSIFIÉ QUI DÉMONTRE LA CAPACITÉ DE LA FRANCE À S'ENTRAÎNER À GRANDE ÉCHELLE POUR FAIRE FACE À UNE CYBERATTAQUE SYSTÉMIQUE FICTIVE, MAIS CRÉDIBLE

1.1 Un scénario réaliste qui s'appuie sur l'état de la menace cyber

Les scénarios des exercices REMPAR visent à entraîner à faire face à un *black-out* numérique. Ils permettent de sensibiliser les entités participantes aux risques de dépendance à la chaîne d'approvisionnement numérique, ainsi qu'à la nécessité de se préparer à être confronté à une crise d'origine cyber. Au niveau national, ils ont vocation à permettre une évaluation de la préparation de la Nation face à une crise d'origine cyber.

L'édition 2025 de REMPAR s'appuyait sur un scénario de compromission, par un acteur cyber étatique, de la mise à jour d'une solution de sécurité massivement utilisée (antivirus ou EDR [1]), donnant la possibilité à l'attaquant de saboter les infrastructures sur lesquelles la solution était installée. La cyberattaque entraînait également des fuites de données massives, orchestrées par l'acteur étatique, s'appuyant sur des groupes cybercriminels pour demander des rançons et ainsi masquer l'origine de l'opération de sabotage.

1. EDR : Logiciel de détection et de réponse, utilisé par les équipes informatiques pour détecter, contenir et enquêter sur les cyberattaques.

Pour rendre l'exercice progressif et immersif, le scénario se décomposait en trois phases successives :

- **Phase 1 – Exfiltration de données :** l'attaquant altérait le comportement de la solution de sécurité afin de collecter et exfiltrer des informations sensibles, une semaine avant le déclenchement de l'attaque par effacement de données. Partout où la mise à jour (fictive) avait été déployée (dans chaque organisation joueuse), le compte à rebours était lancé, pour se terminer le jour de l'exercice à 5h du matin (simulé), justifiant le déclenchement des cellules de crise ;
- **Phase 2 – Effacement de données :** l'attaque s'intensifiait avec un passage en mode destructif (effacement irréversible), entraînant des dysfonctionnements majeurs et la mobilisation urgente des équipes en cellule de crise. Cette phase était l'occasion de tester les enjeux de continuité d'activité, d'anticipation, ainsi que de détection et de réponse ;
- **Phase 3 – Divulgation de données :** les données volées durant la phase 1 étaient partagées à un groupe cybercriminel, puis progressivement publiées, accompagnées de demandes de rançon pour éviter leur divulgation complète. Cette phase était l'occasion de tester les enjeux de résilience liés à la communication, notamment à la pression médiatique simulée, et au juridique, en lien avec la publication de données et les déclarations à effectuer.

Ce scénario, commun à toutes les organisations, était conçu pour être adaptable aux contextes locaux, afin de garantir une expérience cohérente tout en tenant compte des réalités propres à chaque participant. Il permettait de tester la capacité des joueurs à détecter, analyser et gérer une crise d'origine cyber complexe, tout en assurant la continuité d'activité et la communication interne et externe.

Il prévoyait huit rôles distincts, « ressources humaines », « juridique », « finance », « communication », « métier », « décision », « informatique » et « cyber », pour mettre l'emphase sur la pluridisciplinarité et la coordination nécessaires à la résolution des crises d'origine cyber.

Plusieurs adaptations d'un même scénario étaient fournies, afin d'utiliser la « teinte » sectorielle la plus appropriée et en conduire les éventuelles adaptations. Les préfectures et les CSIRT territoriaux [2] disposaient également d'un scénario spécifique, reflétant le scénario principal, et leur permettant de s'entraîner à la mise en place d'un Centre opérationnel départemental, pour les préfectures, et d'une sollicitation massive de soutien sur le plan opérationnel, pour les CSIRT.

2. Les CSIRT (Computer Security Incident Response Team) territoriaux sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

1.2 Une ingénierie d'exercice unique, qui s'appuie sur l'expérience des Jeux Olympiques et Paralympiques 2024, avec un accompagnement responsabilisant les participants

Afin de favoriser une mobilisation large et inclusive, deux modalités de participation étaient proposées :

- **Modalité 1 – En autonomie dans les locaux de l'organisation :** les participants jouaient l'exercice dans leur propre environnement, avec leurs équipes et leurs outils, et testaient leur dispositif de crise (option privilégiée par les organisations désireuses de tirer des enseignements tangibles à mettre en place dans leur contexte) ;

- **Modalité 2 – Participation dans une cellule de crise fictive :** jusqu'à trois représentants de l'organisation étaient accueillis sur l'un des sites prévus pour intégrer une cellule de crise fictive (option privilégiée par les organisations souhaitant mieux comprendre la cinématique d'un exercice de gestion de crise d'origine cyber et échanger avec leurs pairs).

Ce double format était conçu pour créer les conditions d'un apprentissage partagé et d'une montée en maturité généralisée face aux enjeux cyber.

Plus qu'un exercice, REMPAR25 était un véritable programme d'accompagnement, étendu de mars à septembre 2025, qui a permis à 720 organisations de suivre un parcours visant à déployer l'exercice au sein de leur structure, au travers de :

- La préparation et la mise à disposition d'un kit documentaire d'exercice complet adaptable aux spécificités des organisations participantes ;
- L'invitation à un webinaire de lancement, à quatre webinaires de mise en œuvre et à un briefing général, entre mars et septembre 2025, expliquant le projet REMPAR25, les enjeux et la méthodologie d'acculturation et d'appropriation du kit documentaire ;
- Un suivi sous la forme de sessions de questions-réponses hebdomadaires à partir de juin 2025 pour répondre aux questions des organisateurs, et favoriser l'acculturation et l'appropriation des enjeux de REMPAR25.

Chaque organisation a ainsi pu bénéficier d'un accompagnement et d'un suivi dans l'adaptation de REMPAR25 à son contexte et à son niveau de maturité.

La modalité de participation dans des cellules fictives a été choisie par 814 personnes (venant de 555 organisations) qui ont eu l'opportunité de rejoindre l'un des 19 sites d'accueil (17 dans l'hexagone et 2 en outre-mer) mis en place par les Campus Cyber territoriaux, les préfectures, les CCI et des métropoles. Cela a constitué une première sensibilisation à la gestion de crise d'origine cyber et permis de développer les premiers réflexes.

Des équipes projet locales se sont constituées sur l'ensemble du territoire, menées par les délégués régionaux de l'ANSSI et soutenues par l'écosystème local, assurant les rôles d'organisation, d'animation et d'observation pour chaque site.

L'ensemble des structures participantes ont pu bénéficier d'une plateforme de pression médiatique simulée permettant de les entraîner pleinement à la communication de crise d'origine cyber. Entretenant un environnement de jeu partagé, l'usage de cette plateforme a été unanimement salué pour le réalisme qu'elle a apporté, ainsi que le lien qu'elle a permis de créer entre les participants. Elle a notamment permis une visibilité sur les actions de communication publique des participants dans le cadre de l'exercice.

L'exercice a également permis de présenter le savoir-faire français aux partenaires internationaux francophones invités pour l'occasion. Au-delà de la présentation de l'exercice et de son ingénierie, ces derniers ont pu jouer l'exercice en assumant des rôles fictifs pour se plonger pleinement dans la simulation.

2. UN EXERCICE AVEC UNE FORTE REPRÉSENTATIVITÉ DES DIFFÉRENTS SECTEURS D'ACTIVITÉ, RÉPARTIS SUR L'ENSEMBLE DU TERRITOIRE

Les organisations participantes sont unanimement positives : 99,54 % des répondants indiquent que l'exercice REMPAR25 a globalement répondu à leurs attentes et 99,08 % souhaitent participer à une prochaine édition de l'exercice. 94,95 % jugent le programme d'accompagnement globalement adapté à leurs besoins et 98,62 % estiment que les ressources fournies leur ont permis de mener l'exercice dans de bonnes conditions.

Plus de 80 % des répondants qui estimaient avoir un niveau de maturité faible en gestion de crise d'origine cyber avant l'exercice indiquent avoir progressé, passant à modéré, voire averti[3]. De la même façon, plus de 70 % des répondants estimant partir d'un niveau de maturité modéré avant l'exercice, indiquent désormais être avertis, voire experts.

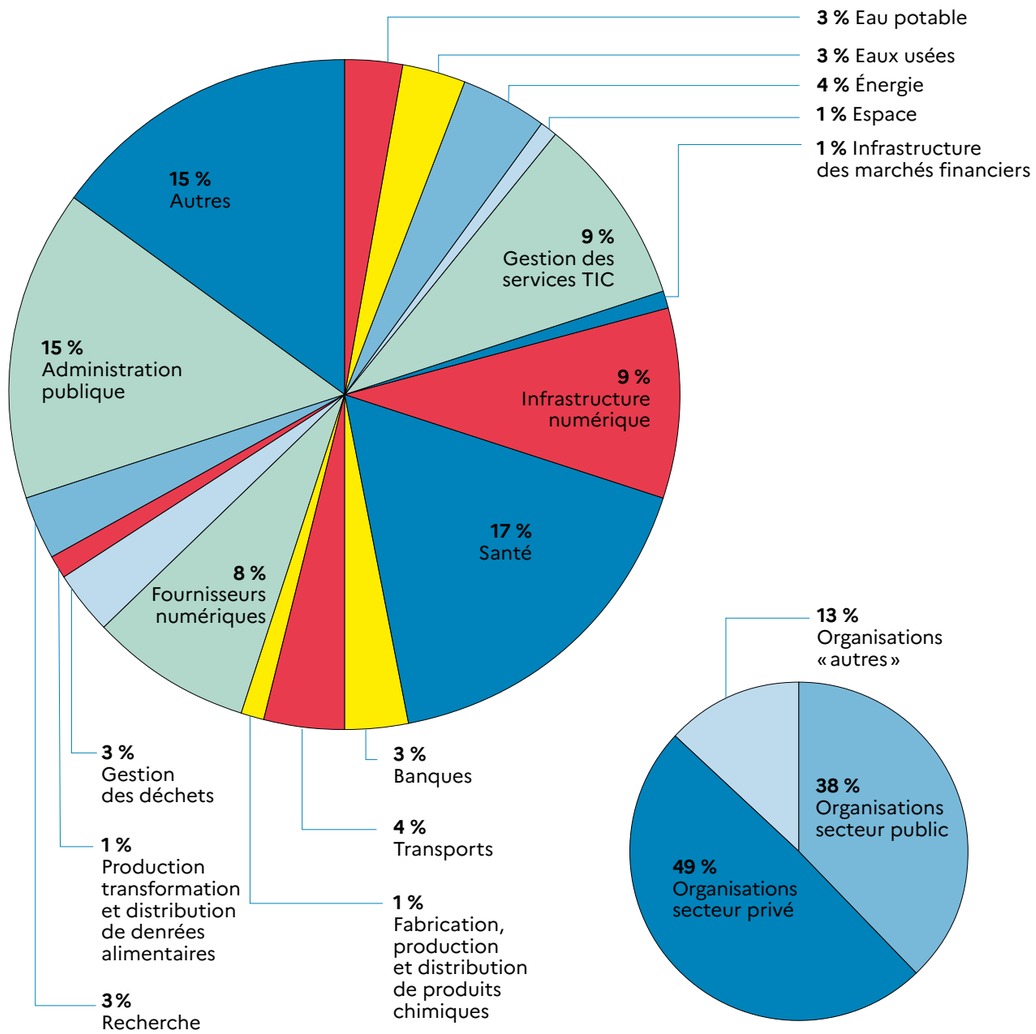
Il a pu être noté une véritable prise de conscience que la crise d'origine cyber concerne – à l'instar d'autres types de crise – l'ensemble des pans d'une organisation. Les efforts doivent cependant être poursuivis pour impliquer davantage les métiers car, malgré une diversité importante des participants qui ont armé les différentes cellules, une surreprésentation des métiers du numérique a été constatée (environ 50 % contre 20 % attendus). La prochaine édition devra mettre l'accent sur la mobilisation de relais non cyber pour continuer à toucher une population plus vaste.

La prise en compte du risque cyber dans les plans de continuité d'activité est jugée toujours faible. La réglementation NIS 2, qui insiste notamment sur ce point, devrait être un levier d'amélioration dans les années à venir. De même, si une meilleure prise en compte de la communication de crise d'origine cyber a été constatée, un axe de progression important demeure.

L'ensemble des organisations ont également pu capitaliser, voire découvrir, un écosystème cyber riche, avec un maillage du territoire sur lequel elles peuvent s'appuyer. Cet écosystème doit désormais se consolider pour mobiliser pleinement des relais, hors du cyber, se densifier et se structurer.

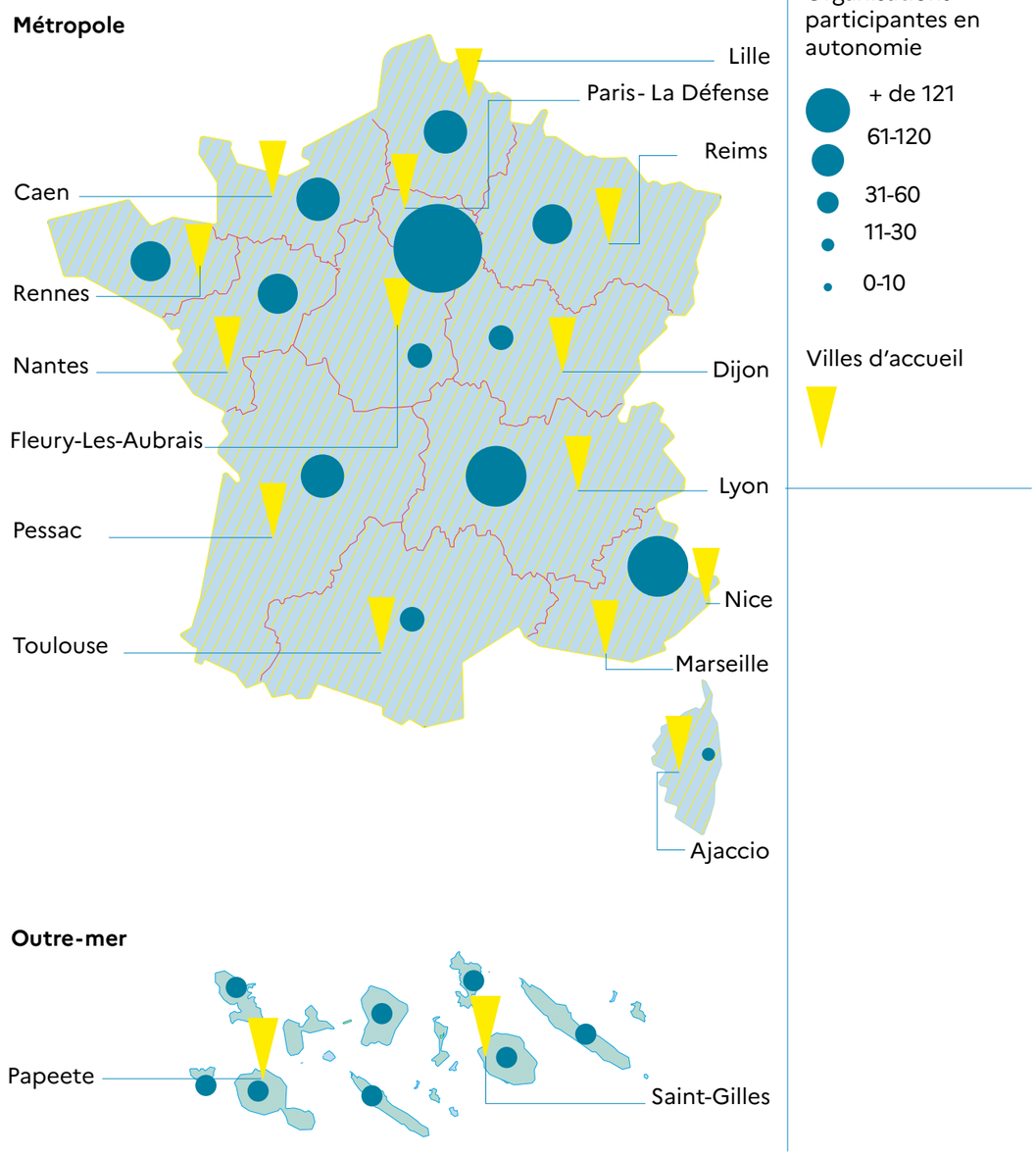
3. Niveaux proposés : faible, modéré, averti, expert.

2.1 Distribution sectorielle des organisations participantes à REMPAR25



RÉPARTITION DES ORGANISATIONS PARTICIPANTES À REMPAR25

2.2 Distribution régionale des organisations participantes à REMPAR25



Organisations participantes en autonomie

- + de 121
- 61-120
- 31-60
- 11-30
- 0-10

Villes d'accueil

3. UN EXERCICE MASSIFIÉ QUI PERMET D'ÉVALUER LE NIVEAU DE PRÉPARATION DE LA NATION

À la suite de l'exercice REMPAR25, le 18 septembre 2025, l'ensemble des parties prenantes, toutes modalités confondues, ont été invitées à renseigner un questionnaire de retour d'expérience (RETEX) à chaud à l'issue de l'exercice. Ces retours ont ensuite été collectés et analysés afin de concaténer et de synthétiser les résultats obtenus.

Afin de tirer une lecture opérationnelle des observations recueillies auprès des organisations participantes en modalité 1, ces dernières ont été regroupées selon trois niveaux de préparation en gestion de crise d'origine cyber, définis à partir de plusieurs critères :

- La taille de l'organisation ;
- La proportion de participants hors IT/SSI ;
- La proportion de décideurs parmi les joueurs ;
- La participation préalable à un exercice de crise d'origine cyber ;
- Le nombre total de joueurs impliqués.

Cette classification distingue ainsi les niveaux suivants :

- **Niveau 1 (N1)** – maturité limitée ;
- **Niveau 2 (N2)** – maturité intermédiaire ;
- **Niveau 3 (N3)** – maturité avancée.

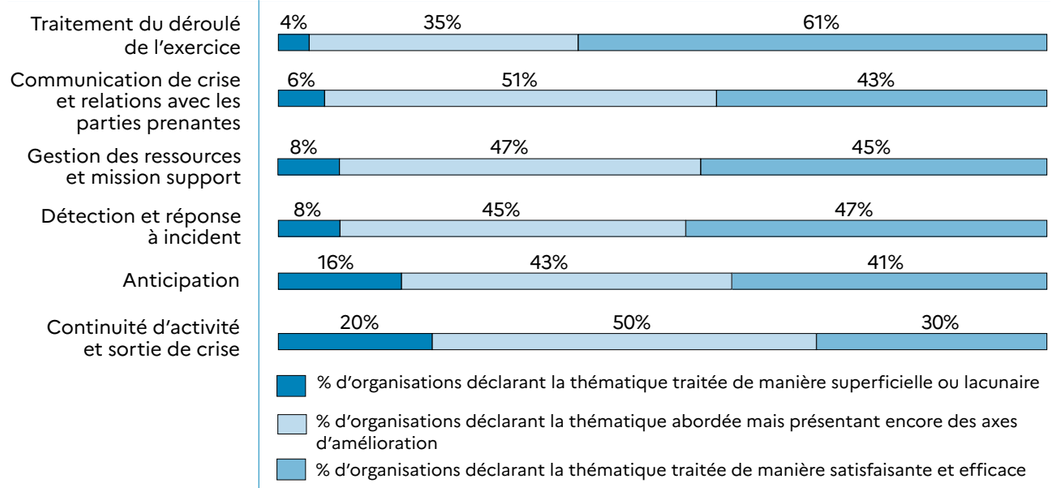
La présente section propose, **par niveau de préparation et par thématique**, une **synthèse des principaux points forts, axes d'amélioration et observations** remontés par les participants au sein du questionnaire de RETEX à chaud et lors des RETEX croisés.

À noter : les commentaires et observations retenus sont ceux qui se sont révélés les plus récurrents et représentatifs parmi l'ensemble des retours recueillis. Cette approche permet de faire émerger des tendances solides et significatives, tout en atténuant les biais liés à la diversité des profils d'organisations.

Les joueurs, observateurs et animateurs de chaque cellule de crise de l'exercice ont été amenés à se prononcer sur six thématiques structurantes, représentatives des grands volets de la gestion de crise d'origine cyber et de la façon de s'y entraîner :

- déroulé de l'exercice ;
- communication de crise et relations avec les parties prenantes ;
- gestion des ressources et missions supports ;
- détection et réponse à incident ;
- anticipation ;
- continuité d'activité et sortie de crise.

Niveau de traitement des différentes thématiques par les organisations participantes



Les résultats révèlent une maturité contrastée au sein de l'écosystème français. Si une culture des exercices de gestion de crise semble désormais bien ancrée, comme le déclare la majorité des organisations sur la thématique « déroulé de l'exercice », plusieurs volets essentiels de la gestion de crise d'origine cyber demeurent insuffisamment approfondis.

Les dimensions techniques (notamment la détection et la réponse à incident) apparaissent globalement mieux intégrées et structurées, traduisant un certain niveau d'appropriation opérationnelle. En revanche, des thématiques telles que la communication de crise, l'anticipation ou encore la continuité d'activité, présentent des marges de progression importantes.

Ces écarts soulignent la nécessité de renforcer les volets de préparation stratégique et de résilience organisationnelle, encore souvent traités comme secondaires par rapport à la réponse immédiate aux incidents et aux crises.

À noter que l'on observe un meilleur traitement sur l'ensemble des thématiques chez les organisations ayant déjà réalisé un exercice de gestion de crise d'origine cyber, par rapport à celles n'en ayant jamais réalisé. Ce constat met en évidence le rôle déterminant de l'entraînement

3.1 Une compétence et une appétence solide dans la conduite des exercices

Les organisations font preuve dans l'ensemble d'une bonne compréhension globale des enjeux liés à une crise d'origine cyber. L'exercice REMPAR25 a ainsi constitué un levier de sensibilisation et un premier ancrage méthodologique pour les organisations les moins matures, leur permettant de mieux cerner les réflexes essentiels à adopter en situation de crise. Les organisations d'un niveau modéré ont noté la mise en place de plans d'action définis, impliquant une hiérarchisation efficace des priorités et garantissant une réponse structurée et adaptée au rythme de l'exercice, parfois jugé très soutenu.

Pour les organisations de maturité plus faible (N1), l'absence de documentation de crise a souvent limité la capacité des équipes à s'appuyer sur des référentiels ou procédures formalisés. Par ailleurs, le non-respect de la répartition des rôles au sein de la cellule de crise a parfois entraîné une confusion dans la prise de décision et dans la hiérarchisation des priorités. Des difficultés d'utilisation de la main courante ont également été relevées, traduisant un manque de familiarisation avec cet outil de traçabilité. Enfin, la procédure de gestion de crise, quand elle existait, a parfois été insuffisamment maîtrisée, ce qui a pu freiner la coordination et la réactivité collective lors du déroulé de l'exercice.

Les organisations les plus averties (N3) sur le sujet, ont, quant à elles, démontré d'excellents réflexes en matière de gestion de crise, tant sur le plan organisationnel qu'opérationnel. La documentation de crise était claire et mobilisée efficacement, la répartition des rôles bien respectée, et les procédures appliquées avec rigueur, traduisant une maîtrise solide des mécanismes de gestion de crise et une forte coordination au sein des cellules. Un travail en mode dégradé a souvent pu être mis en œuvre afin de tester la réactivité et les réflexes de la cellule de crise en situation d'indisponibilité des outils numériques habituels, permettant ainsi d'évaluer la capacité d'adaptation et de continuité opérationnelle des équipes.

3.2 La démonstration d'une réelle capacité de réaction sur le plan opérationnel, avec la mise en œuvre de réflexes pertinents en situation de crise

Les organisations, tous niveaux confondus (N1, N2 et N3), ont démontré une bonne maîtrise des premières actions de sécurité des systèmes d'information à mettre en œuvre en cas de crise d'origine cyber. Elles ont su identifier rapidement les mesures prioritaires de confinement et de sécurisation, traduisant une appropriation solide des réflexes techniques essentiels dès les premières phases de gestion de crise.

Les organisations de maturité limitée (N1) ont relevé un manque de cartographie à jour de leur système d'information, rendant plus difficile l'identification rapide du périmètre de compromission et la priorisation des actions de réponse en situation de crise.

Plusieurs organisations ont souligné une meilleure prise de conscience du rôle des aidants dans la réponse à incident en cas de crise d'origine cyber, marquant une évolution positive dans la compréhension des acteurs à mobiliser.

> Il est à noter que l'exercice restait d'un niveau de jeu opérationnel et stratégique, et n'adressait pas le niveau tactique, ce qui a limité la mise en œuvre concrète de certaines actions pour aborder de manière réaliste les thématiques de détection et de réponse à incident. Cette limite a pu freiner la mise en situation opérationnelle des équipes et réduire la portée pédagogique de ces séquences, en limitant leur capacité à analyser, prioriser et enclencher les actions techniques appropriées.

3.3 Une communication de crise souvent peu planifiée et tributaire de l'improvisation en situation de crise

Les organisations disposant d'un niveau de maturité limité (N1) ont relevé que les supports de communication existants au sein de leur organisation – notamment ceux destinés aux médias – étaient peu adaptés à la gestion d'une crise d'origine cyber, ne permettant pas une communication réactive et contextualisée. Elles ont également souligné une cartographie incomplète des parties prenantes et une analyse insuffisante des outils de contact, rendant plus complexe la mobilisation rapide des acteurs clés en situation de crise.

Les organisations avec une maturité intermédiaire (N2) ont exprimé une difficulté à anticiper les étapes successives de la communication de crise, ce qui a parfois entraîné un manque de visibilité sur la stratégie à moyen terme durant l'exercice, malgré leur capacité à formaliser rapidement une stratégie de communication, à la fois interne et externe, adaptée aux enjeux spécifiques d'une crise d'origine cyber. Cette réactivité a permis d'assurer une cohérence des messages diffusés et une gestion maîtrisée des interactions avec les différentes parties prenantes.

Les organisations les plus avancées (N3) ont démontré une préparation particulièrement avancée en matière de communication de crise, avec l'élaboration de modèles et d'éléments de langage prêts à l'emploi.

L'emploi de la plateforme de pression médiatique simulée, par les organisations concernées, a pu rendre concrète la mise en place d'une stratégie de communication.

> La thématique est bien prise en compte par l'ensemble des organisations. Toutefois, elles doivent travailler les aspects de communication en amont de la crise, afin de pouvoir les adapter à la situation rencontrée le moment venu. Les canaux et pratiques de communication alternatifs en cas d'indisponibilité des outils doivent encore faire l'objet de réflexion approfondie par les organisations.

3.4 L'appui logistique, les ressources humaines et les moyens juridiques et financiers demeurent insuffisamment organisés pour soutenir une gestion de crise dans la durée

Un manque de connaissance des métiers supports a été observé à plusieurs reprises au sein des cellules de crise des organisations avec une maturité limitée (N1), limitant la mobilisation efficace des compétences clés au moment opportun. Par ailleurs, une planification insuffisante de la répartition des rôles et des missions a été relevée, entraînant une coordination parfois imprécise et une perte d'efficacité opérationnelle durant la gestion de crise. Les observations formulées sur cette thématique mettent en évidence un traitement encore superficiel des aspects financiers, souvent évoqués sans être véritablement intégrés à la gestion de crise. Les risques psychosociaux sont généralement identifiés et compris, mais peu pris en compte dans les dispositifs opérationnels.

Les organisations avec une maturité intermédiaire ou avancée (N2, N3) se distinguent par une bonne gestion des impacts transverses, démontrant une vision d'ensemble claire et une capacité à anticiper les effets en cascade d'une crise d'origine cyber sur les différentes fonctions et activités de l'organisation. Elles ont néanmoins souligné l'absence d'une stratégie clairement définie sur les aspects juridiques, exprimant un besoin d'orientations précises quant aux obligations légales et aux démarches à suivre en cas de crise d'origine cyber, en dehors du dépôt de plainte. Enfin, plusieurs organisations ont mis en avant des manquements dans la répartition des rôles, entraînant par moments des zones de flou dans la coordination et la responsabilité des actions.

> Il est à noter une prise de conscience accrue de l'importance d'intégrer des représentants de sujets transverses au sein de la cellule de crise (juridique, RH, communication, etc.), afin d'assurer une approche plus globale et cohérente de la gestion de crise d'origine cyber. Néanmoins, ces aspects sont encore mal traités par les organisations.

3.5 Des travaux amorcés au sein des organisations pour instruire l'anticipation dans la gestion des crises d'origine cyber

Les organisations de maturité limitée et intermédiaire (N1, N2) ont fait preuve d'une capacité d'anticipation fondée sur le bon sens, bien que non formalisée dans des procédures établies. Cette approche intuitive leur a néanmoins permis de prendre une certaine avance sur le scénario et de réagir de manière cohérente face aux premiers signaux de crise. Elles ont toutefois exprimé une difficulté à comprendre pleinement les enjeux et objectifs de l'anticipation dans le cadre d'une gestion de crise d'origine cyber, cette dimension étant souvent assimilée à la réaction immédiate plutôt qu'à la mise en place d'une capacité en conduite pour prendre du recul et anticiper les actions à venir, notamment les actions « métier » en mode dégradé. Certaines ont géré la crise de manière réactive, avec peu ou pas d'anticipation de la part des joueurs durant l'exercice, traduisant une dépendance aux événements déclenchés plutôt qu'une démarche proactive de gestion du scénario.

Les organisations avec une maturité intermédiaire (N2) ont néanmoins démontré une bonne anticipation des impacts informatiques, rendue possible par la mobilisation d'équipes IT/SSI disposant d'une connaissance fine de leur environnement technique et des interdépendances critiques de leur système d'information.

Les organisations les plus matures (N3) se sont distinguées par la réalisation de scénarios d'anticipation pendant l'exercice, démontrant une maîtrise avancée de la planification et de la projection opérationnelle. Elles ont également engagé une réflexion sur la mise en place d'une cellule dédiée à l'anticipation, visant à renforcer la veille, l'analyse prospective et la coordination interservices en amont des situations de crise. Elles ont relevé une difficulté à faire évoluer les scénarios d'anticipation au fil de la progression de la crise, peinant à adapter leurs hypothèses initiales et à actualiser leurs plans d'action en fonction des nouveaux éléments de situation.

L'anticipation structurée est une thématique encore mal comprise par les organisations qui peinent à la mobiliser pleinement pour les accompagner dans la gestion de la crise.

3.6 Des dispositifs de continuité d'activité et de sortie de crise existants, mais peu testés ou actualisés

Les organisations avec une maturité intermédiaire (N2) se distinguent par la disponibilité d'une documentation opérationnelle – notamment des plans de continuité d'activité (PCA) et des fiches réflexes – facilitant la gestion des différentes phases de crise, contrairement aux organisations les moins matures (N1). Elles ont également démontré une bonne maîtrise des modes de fonctionnement dégradés, permettant aux équipes métiers de maintenir leurs activités essentielles tout en adaptant leurs processus à la situation. Les problématiques de sortie de crise ont été peu traitées, la priorisation des activités et des applications critiques demeurant souvent complexe en situation de tension. Les plans de continuité d'activité existants sont par ailleurs souvent méconnus des équipes, jamais éprouvés ou insuffisamment adaptés à la réalité d'une crise, limitant leur utilité opérationnelle. Enfin, des difficultés persistantes dans la gestion de la continuité des activités transverses (ressources humaines, finances, juridique, etc.) ont été relevées, traduisant une coordination inégale entre les fonctions dites supports.

Les organisations avec une maturité avancée (N3) se distinguent par une documentation de continuité d'activité (PCA, fiches réflexes) claire, connue et régulièrement éprouvée par les équipes concernées, garantissant une mobilisation rapide et efficace en situation de crise. Elles ont également formalisé un plan d'action de sortie de crise, structurant les étapes de reprise et de retour à la normale. Enfin, la mise en place d'une stratégie de reconstruction du système d'information à la suite de la crise témoigne d'une approche proactive et résiliente, intégrant pleinement la dimension post-crise dans leur dispositif de gestion de crise d'origine cyber.

À noter que le format de l'exercice a peu permis l'instruction réaliste de la phase de sortie de crise, les conditions simulées de reprise ne reflétant pas pleinement la complexité temporelle d'un véritable redémarrage post-crise, pour des raisons de temps de jeu.

Les dispositifs de continuité d'activité sont des dispositifs historiques de la gestion de crise, globalement maîtrisés par les organisations. Toutefois, ils doivent continuer à s'opérationnaliser pour être pleinement utilisés par l'ensemble des équipes, et non seulement les équipes IT/SSI, comme un outil au service de la gestion de la crise dans sa globalité.

4. PLUSIEURS AXES D'EFFORT POUR RENFORCER LA RÉSILIENCE DES ORGANISATIONS SE DESSINENT POUR LES PROCHAINES ANNÉES

La synthèse proposée ci-après met ainsi en lumière les thématiques de gestion de crise identifiées comme acquises par la majorité des organisations, ainsi que les axes de progression récurrents observés ou remontés dans le cadre du processus de retour d'expérience à froid et à chaud.

4.1 Thématiques désormais bien intégrées avec un effort qui doit être maintenu

⟶ **Communication interne**
La communication interne s'impose comme un point fort. Les cellules savent diffuser de manière claire et cohérente les consignes. Elles accordent également une attention à la circulation de l'information, en tenant régulièrement informé le personnel de l'évolution de la crise.

⟶ **Communication externe incluant la communication avec les autorités et l'éditeur**
La communication externe est désormais globalement bien intégrée. Des éléments de langage clairs et cohérents sont partagés en évacuant le « bruit » avec une stratégie de communication externe adaptée au contexte de crise. La communication avec les autorités et les parties prenantes externes est également prise en compte.

4.2 Thématiques partiellement maîtrisées devant faire l'objet de consolidation par les organisations

⟶ **Prise en compte de l'organisation étendue et limitation de la propagation de l'attaque**
Les réflexes techniques sont globalement bien appliqués : levée de doute, déclenchement d'actions immédiates sur le terrain, utilisation d'une cartographie des systèmes d'information impactés. En revanche, des mesures essentielles permettant de limiter les risques de propagation sont moins systématiques : coupure des flux entrants et sortants pour s'isoler ou prendre en compte la gestion de l'informatique de l'ombre (*shadow IT*). Ces éléments témoignent d'une prise en compte limitée des interdépendances amont et aval des organisations.

⟶ **Facteurs humains et gestion du personnel**
Le facteur humain est désormais mieux intégré dans la gestion de crise d'origine cyber avec la mise en œuvre des mesures adaptées : mise en congé, télétravail à titre exceptionnel, ainsi que la mobilisation de renforts. En revanche, ces mesures sont encore trop réactives et non anticipées en particulier dans le suivi et pilotage des ressources humaines.

⟶ **Gestion des impacts sur l'activité de l'entité**
Cette thématique est marquée par une bonne réactivité opérationnelle, mais une approche souvent superficielle de la priorisation et du redémarrage. Les impacts métiers sont globalement bien identifiés et gérés, mais rarement hiérarchisés, ce qui limite la capacité à prioriser efficacement les actions de reprise. Les processus de contrôle et de vérification avant la remise en service des SI ne sont pas toujours envisagés, traduisant une approche parfois trop hâtive dans la reprise.

⟶ **Solutions de travail dégradé envisagées – PCA Cyber**
Cette thématique est partiellement maîtrisée, combinant de bons réflexes en matière de continuité à des lacunes dans l'analyse de fond. Des mesures de continuité adaptées sont globalement mises en place, avec des réactions appropriées pour éviter une sur-crise comme la vérification de l'intégrité des sauvegardes. En revanche, la projection de la durée d'indisponibilité et de l'impact sur les modes dégradés est peu menée. Cela témoigne de l'absence encore trop importante de dispositif de continuité d'activité « cyber » prenant en compte les spécificités, notamment la durée potentiellement longue.

⟶ **Gestion de la sortie de crise et de « l'après »**
Les organisations intègrent la nécessité du dépôt d'une plainte, traduisant une bonne compréhension des démarches post-incident immédiates. En revanche, les documents de sortie de crise, tels que les plans d'action de reprise ou de renforcement, ne sont pas formalisés, limitant la capitalisation des enseignements et le retour à la normale.

4.3 Thématiques avec des axes d'amélioration importants qui doivent faire l'objet d'efforts par les organisations

⟶ **Affaires juridiques et assurantielles**
Les dispositifs juridiques et assurantiels permettant de couvrir les effets de bord liés à une crise sont encore rarement anticipés ou testés. Ils sont pourtant, en particulier pour l'assurance-cyber, des dispositifs indispensables pour soutenir la résolution de la crise et éviter des sur-crises.

⟶ **Pilotage des impacts économiques**
Le traitement superficiel de cette thématique révèle une maîtrise encore limitée des volets économiques de la gestion de crise. Certains dispositifs peinent à prendre leur place dans la gestion de la crise : procédure d'achat en situation d'urgence, dédommagement, réalisation d'un bilan financier post-crise ou évaluation des impacts formalisés débouchant sur des mesures concrètes de gestion ou d'arbitrage budgétaire.

Il est à noter que la surreprésentation d'une population IT/SSI dans les participants peut expliquer une prise en compte limitée des enjeux économiques.

⟶ **Orientation des investigations par les cellules de crise**
Les cellules de crise proposent peu d'orientations précises pour alimenter les investigations techniques et guider efficacement les recherches. Cette approche réactive, plutôt que proactive, limite la profondeur des analyses et la structuration de la démarche d'investigation.

⟶ **Anticipation des impacts de la crise et des décisions sur les activités de l'entité**
Les organisations ont une sensibilité accrue aux vulnérabilités techniques notamment celles liées à un défaut des solutions de sécurité (scénario de l'exercice), mais qui ne génèrent pas encore une réflexion sur les impacts opérationnels, juridiques, financiers et réputationnels. Les scénarios d'anticipation métier sont encore trop peu élaborés, et des actions préventives en amont d'une éventuelle exfiltration et divulgation de données ont été peu menées, témoignant d'une trop faible maturité sur l'anticipation.

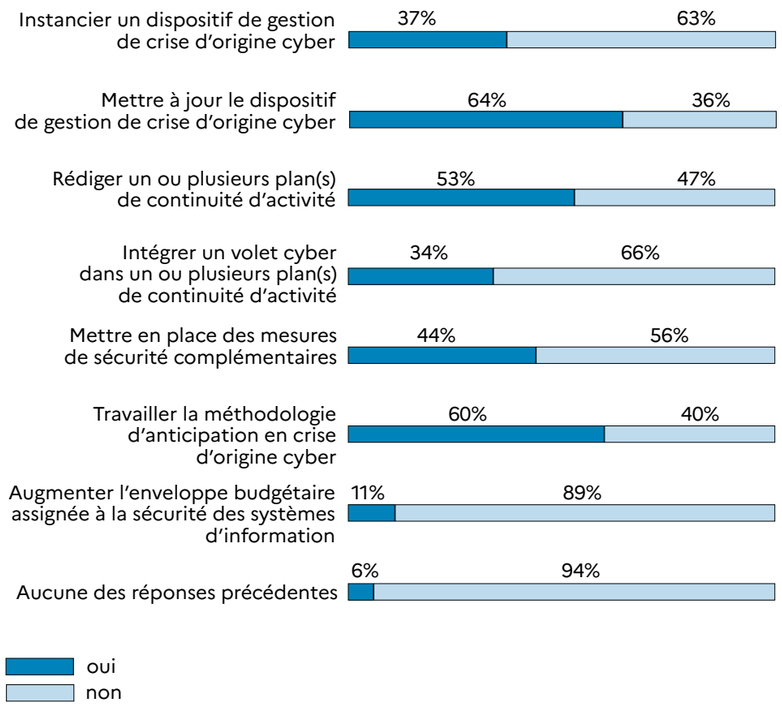
Des axes d'efforts déjà identifiés par les participants dans le cadre de leur plan d'actions post exercice

Quelques semaines après l'exercice, il a été proposé aux participants en autonomie de partager les grands axes de leurs plans d'action issus de ce dernier. L'enseignement principal de ce RETEX à froid est la prise de conscience des participants de l'importance de se saisir du sujet puisqu'en immense partie, près de 95 %, REMPAR25 a été pour eux l'occasion de mettre en place des actions sur les volets gestion de crise et/ou SSI.

Près de 80 % des répondants ont indiqué instancier ou mettre à jour leur dispositif de gestion de crise d'origine cyber, plus de 60 % veulent rédiger un plan de continuité d'activité ou intégrer un volet cyber à un PCA existant et près de la moitié des organisations souhaitent mettre en place des mesures de sécurité complémentaires.

Au-delà des actions relatives à l'organisation, la méthodologie ou la documentation, le sujet du budget alloué à la SSI reste une marche compliquée à franchir pour la grande majorité des organisations.

ACTIONS RECENSÉES DANS LES RETEX DES PARTICIPANTS



Pour aller plus loin

Un kit d'exercice mis à la disposition de tous pour faciliter l'organisation d'exercice de crise d'origine cyber

Dans une volonté de faciliter la mise en œuvre par toutes les organisations de REMPAR25, l'ANSSI met à disposition l'ensemble des documents et supports nécessaires sur son site.

Le kit « REMPAR25 » est composé des éléments suivants :

- ⟶ Webinaires de mise en œuvre et d'adaptation de l'exercice ;
- ⟶ Scénario détaillant la chaine de compromission et les chronogrammes associés ;
  - → Chronogramme principal avec plusieurs teintes sectorielles ;
  - → Chronogramme à destination des CSIRT territoriaux et sectoriels ;
  - → Chronogramme à destination des préfectures (Centres Opérationnels Départementaux – COD)
- ⟶ Pièces jointes associées aux stimuli des chronogrammes ;
- ⟶ Boites à outils : annuaire de crise, main courante, grille d'observation ;
- ⟶ Documents de *briefing* pour les animateurs et les observateurs ;
- ⟶ Dossier de mise en situation ;
- ⟶ Documents pour l'organisation et la réalisation du retour d'expérience (RETEX).

L'ANSSI encourage les organisations à se saisir de ce retour d'expérience et du kit prêt à l'emploi pour le déployer. Les exercices de crise sont un outil efficace pour disposer d'une compréhension partagée des enjeux par des équipes pluridisciplinaires. La meilleure manière de gérer une crise d'origine cyber, c'est de s'y préparer.

ANNEXE
LISTE DES PARTENAIRES

RÉGION	PARTENAIRE
Auvergne-Rhône-Alpes	Campus Région du numérique
Bourgogne-Franche-Compté	Préfecture de la région Bourgogne-Franche-Comté Direction régionale de l'économie, de l'emploi, du travail et des solidarités (DREETS)
Bretagne	Agence régionale de santé Bretagne / e-Santé Bretagne
	Breizh Cyber
	Bretagne Cyber Alliance
	CLUSIR Bretagne
	Cyber place
	École des hautes études en santé publique
	European Digital Innovation Hub Bretagne
	GACYB Bretagne
	Le Poool
	Pôle d'excellence Cyber
	Préfecture d'Ille-et-Vilaine
Centre-Val de Loire	CybeRéponse
	Ministère de l'économie, des finances et de la Souveraineté industrielle Service de l'information stratégique et sécurité économiques
	Service départemental d'incendie et de secours du Loiret
Corse	Agence de développement économique de la Corse
	CAPA Paesi d'Aiacciu (Communauté d'agglomération du Pays Ajaccien)
	CLUSIR Corsica
	Collectivité de Corse
	CSIRT CyberCorsica
	Préfecture de Corse
Grand Est	Grand Reims
	Numica
Hauts-de-France	Campus Cyber Hauts-de-France Lille Métropole
	CLUSIR Nord de France
Île-de-France	Campus Cyber
	Club de la continuité d'activité
	CESIN
	CLUSIF
	Métropole du Grand Paris
La Réunion	Cyber Réunion
Normandie	Agence de développement pour la Normandie
Nouvelle-Aquitaine	Campus régional de cybersécurité et de confiance numérique de Nouvelle-Aquitaine
Occitanie	Cyber'Occ
Pays de la Loire	Nantes Digital Week
	Nantes Métropole
Polynésie française	Haut-commissariat de la République en Polynésie française
Provence-Alpes-Côte d'Azur (site de Marseille)	Campus Cyber Région Sud / Euromed
	CCI Aix-Marseille-Provence
	Métropole Aix-Marseille-Provence
Provence-Alpes-Côte d'Azur (site de Sophia Antipolis)	Campus Cyber Région Sud / Sophia Antipolis
	CCI Nice Côte d'Azur
	CLUSIR Sud – PACA
	Communauté d'agglomération Sophia Antipolis
	Entreprise Europe Network
	Sictiam
	Telecom Valley
	Urgence Cyber région Sud
	Région de gendarmerie de Provence-Alpes-Côte d'Azur
National	Campus Cyber
	Club de la continuité d'activité

Version 1.0 – Décembre 2025

Licence Ouverte/Open Licence (Etalab — v2.0)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr