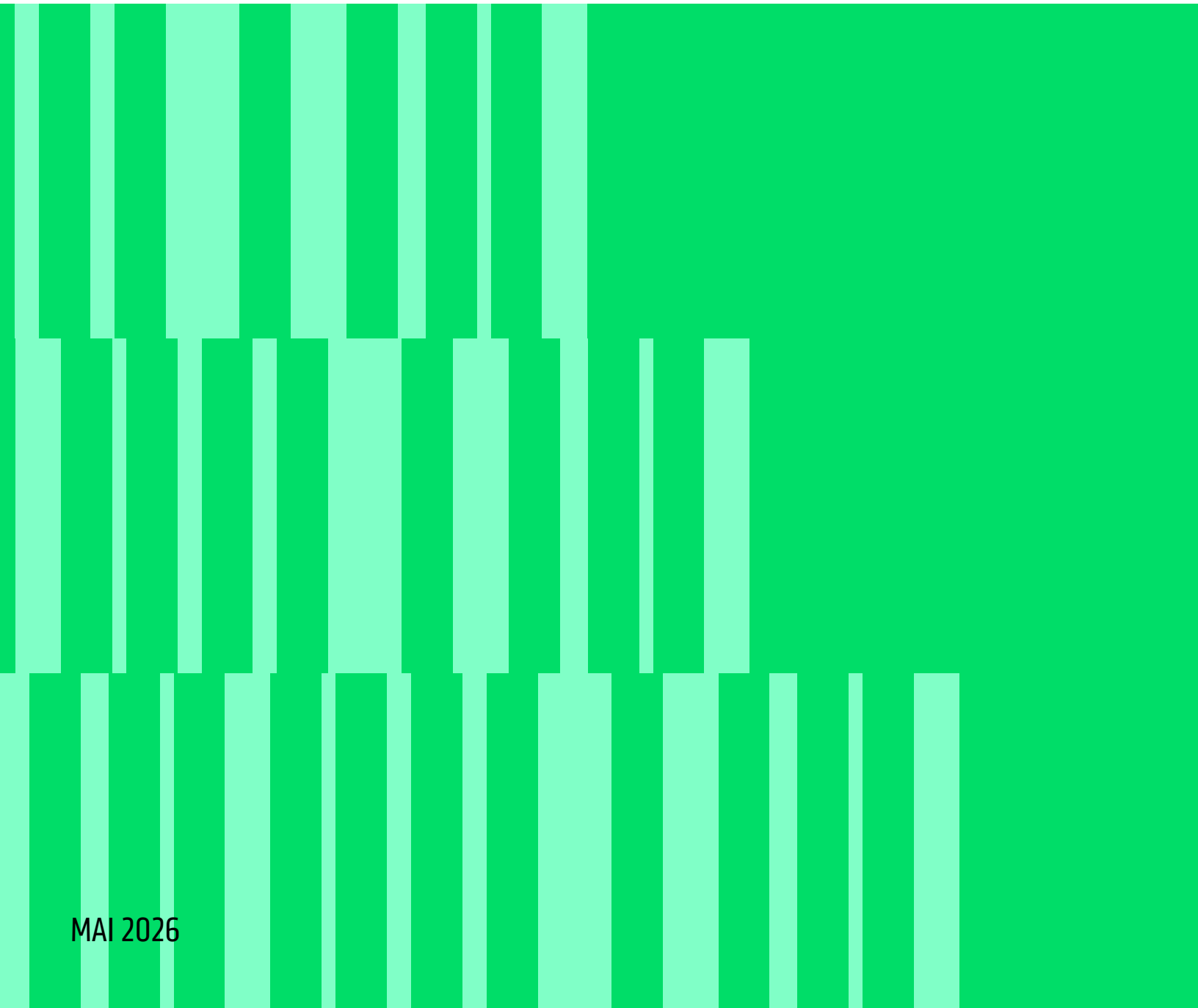
COHESITY

RAPPORT SUR LA CYBER-RÉSILIENCE

Être préparé aux risques ou y être exposé : Le fossé de la cyber-résilience dans le secteur public

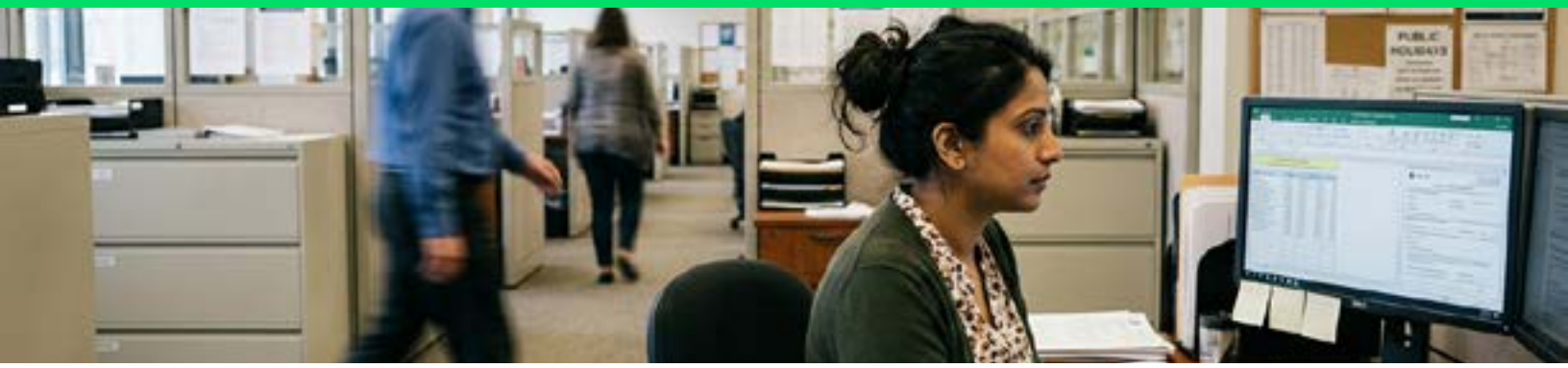


MAI 2026

On parle beaucoup de détection et de prévention des cyberattaques, mais la réalité est tout autre. Il ne suffit plus de prévenir et de détecter. Même les entreprises les plus avancées sont victimes de perturbations paralysantes dont les répercussions s'étendent des opérations informatiques à la salle du conseil, et au-delà.

Afin de comprendre les causes de cette situation et ce qui distingue les entreprises résilientes de celles qui restent en difficulté, Cohesity a interrogé 3 200 décideurs en charge des opérations informatiques et de sécurité, dans 11 pays. Parmi les répondants, 399 provenaient d'entreprises du secteur public. Leurs réponses révèlent une fracture croissante en matière de résilience entre les entreprises prêtes à faire face au risque, capables d'assurer une restauration rapide et maîtrisée, et leurs homologues plus exposées, qui demeurent vulnérables à des interruptions prolongées ainsi qu'aux conséquences financières qui en découlent.

Nos recherches examinent les impacts concrets des cyberattaques majeures, la manière dont les entreprises du secteur public ont auto-évalué leur cyber-résilience par rapport aux bonnes pratiques, et les mesures qu'elles ont prises pour détecter ces incidents, y répondre et restaurer leur activité. Elle met également en évidence les enseignements qu'elles en ont tirés, et la manière dont elles se tournent vers l'IA et l'automatisation pour accélérer leur résilience et combler le fossé.



CYBERATTAQUES MAJEURES : **LA NOUVELLE RÉALITÉ DES ENTREPRISES MODERNES**

Tous les cyber incidents ne se valent pas. De nombreuses entreprises gèrent quasi-quotidiennement des tentatives de phishing, des scans de logiciels malveillants ou des pannes système. Mais les cyberattaques majeures sont différentes. Notre enquête définit une cyberattaque majeure comme un incident ayant causé un impact mesurable financier, réputationnel, opérationnel ou en matière de perte de clients.

DANS LES ENTREPRISES DU SECTEUR PUBLIC, CES ATTAQUES LOURDES EN CONSÉQUENCES NE SONT PLUS L'EXCEPTION : ELLES S'INSCRIVENT DÉSORMAIS DANS UNE DYNAMIQUE RÉCURRENTE.

67 %

des répondants ont été confrontés à au moins une cyberattaque majeure

49 %

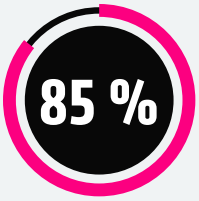
en ont subi une au cours des 12 derniers mois

26 %

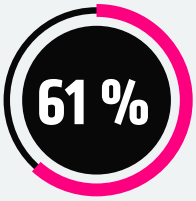
ont subi plusieurs incidents sur cette période de 12 mois

LE VÉRITABLE COÛT DES CYBERATTAQUES MAJEURES

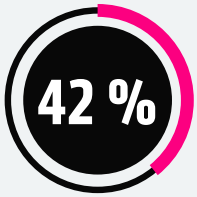
LES PRESSIONS FINANCIÈRES ET RÉGLEMENTAIRES SE SONT FAIT RESSENTIR DANS L'ENSEMBLE DES ENTREPRISES DU SECTEUR PUBLIC QUE NOUS AVONS INTERROGÉES :



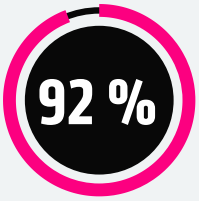
ont déclaré avoir subi une perte de chiffre d'affaires



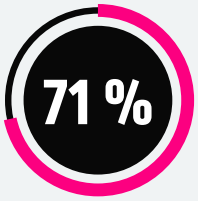
des entreprises cotées en bourse ont déclaré avoir révisé leurs prévisions financières[1]



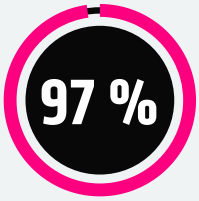
ont perdu des clients



ont payé une rançon, d'un montant moyen de 1,3 million d'euros par incident



des entreprises non cotées ont réaffecté une partie de leur budget au détriment de projets visant à stimuler la croissance



ont été confrontés à des répercussions juridiques ou réglementaires, notamment des sanctions financières (45 %) et des actions en justice/recours collectifs (40 %)

[1] Bien que relativement peu d'entreprises cotées en bourse aient officiellement annoncé avoir révisé leurs résultats suite à un cyber incident, ces conclusions suggèrent que les répercussions financières et opérationnelles vont bien au-delà de ce que révèlent les documents publics.

DE LA CONFIANCE MALGRÉ LES CONSÉQUENCES

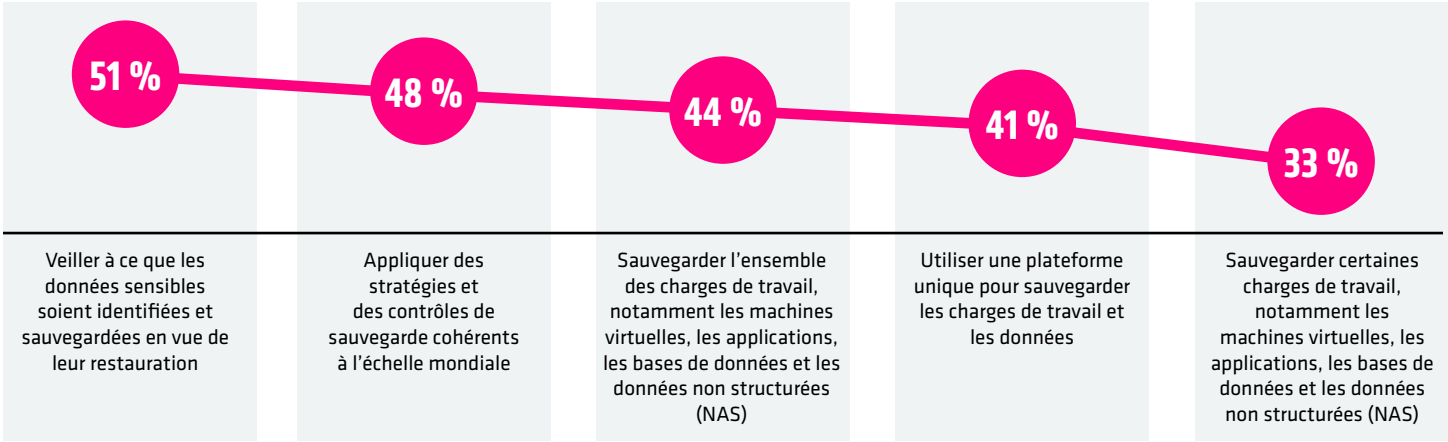
Compte tenu de l'ampleur des répercussions financières et opérationnelles révélées par notre étude, on pourrait s'attendre à ce que la résilience organisationnelle soit un sujet de préoccupation très répandu. La majorité des personnes interrogées (54 %) se sont dites totalement convaincues que leur stratégie de cyber-résilience pouvait résister aux menaces actuelles. Ce niveau de confiance contraste fortement avec les impacts majeurs subis par bon nombre de ces mêmes entreprises.

CE QUE LES ENTREPRISES FONT (ET NE FONT PAS)

Nous avons voulu aller plus loin et identifier les lacunes en matière de résilience. Pour ce faire, nous avons demandé aux personnes interrogées de décrire leur approche concernant certaines pratiques et capacités clés associées aux cinq dimensions fondamentales de la cyber-résilience : **la protection des données, la restauration des données, la détection et l'investigation des menaces, la résilience des applications et l'optimisation de la posture des risques liés aux données.**

LA PROTECTION DES DONNÉES RESTE FRAGMENTÉE DANS LES ENVIRONNEMENTS HYBRIDES ET MULTI-CLOUD

Laquelle des mesures suivantes votre entreprise met-elle en œuvre pour protéger toutes ses données dans des environnements hybrides et/ou multi-cloud ?



Un peu plus de la moitié des entreprises du secteur public veillent à identifier et à sauvegarder leurs données sensibles afin de pouvoir les restaurer, et près de la moitié d'entre elles appliquent des stratégies de sauvegarde cohérentes à l'échelle mondiale. Moins de la moitié sauvegardent toutes les charges de travail ou utilisent une plateforme unique pour protéger les charges de travail et les données. Un tiers ne protège par sauvegarde qu'une partie des charges de travail. Cette fragmentation limite la visibilité et la cohérence entre les environnements. La maturité en cyber-résilience dépend de la convergence de la sauvegarde et de la restauration/reprise au sein d'une plateforme unique, intelligente, et sécurisée par une approche fondée sur les principes du Zero Trust.

LES MESURES DE CAPACITÉ DE RÉCUPÉRATION DES DONNÉES SONT COURANTES, MAIS LEUR MATURITÉ VARIE

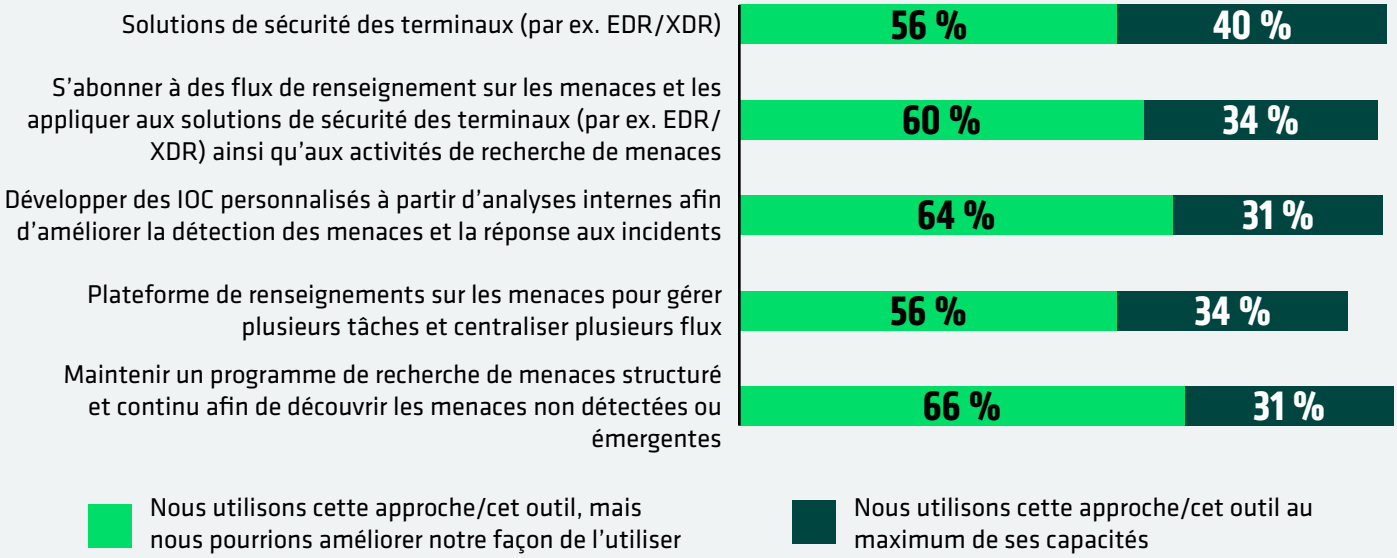
Que fait votre entreprise pour garantir la capacité de récupération de ses données ?

50 %	Exiger une autorisation supplémentaire pour les tâches administratives à risque élevé associées aux solutions de sauvegarde et de restauration
47 %	Suivre la règle de sauvegarde « 3-2-1 » (trois copies des données, stockées sur deux types de supports différents, dont une copie conservée hors site)
46 %	Authentification multifacteur sur notre solution de sauvegarde
46 %	Appliquer le principe du moindre privilège aux charges de travail sauvegardées
38 %	Protéger les données critiques grâce à l'immuabilité

De nombreuses organisations du secteur public ont renforcé les contrôles d'accès autour des environnements de sauvegarde, la moitié nécessitant une autorisation administrative supplémentaire pour les tâches à risque élevé. Environ la moitié applique l'authentification multifacteur, suit la règle de sauvegarde 3-2-1 et applique des droits d'accès selon le principe du moindre privilège. Peu d'entre elles protègent les données critiques grâce à l'immuabilité Ces lacunes ne permettent pas de garantir une restauration complète. Une cyber-résilience mature repose sur des copies de restauration vérifiées, isolées et infalsifiables.

LES OUTILS DE DÉTECTION ET D'INVESTIGATION DES MENACES SONT SOUS-UTILISÉS

Dans quelle mesure votre entreprise utilise-t-elle chacun des outils ou méthodes suivants pour détecter et enquêter sur les menaces ?



Les solutions de détection et d'analyse des menaces sont largement mises en place, mais restent fréquemment sous-utilisées. La plupart des entreprises du secteur public ont recours à des solutions de sécurité des endpoints, à des flux de renseignement sur les menaces, à des indicateurs de compromission personnalisés, à des plateformes de renseignements sur les menaces et à des programmes structurés de recherche proactive de menaces. Pourtant, seule une minorité en tire pleinement parti. Une cyber-résilience mature repose sur l'intégration de ces outils dans une boucle continue de renseignement, afin d'améliorer la visibilité, la détection et la réponse.

LES ENTREPRISES SONT SUSCEPTIBLES D'ÊTRE RÉINFECTÉES

Que fait ou ferait votre entreprise pour garantir la résilience des applications face aux cyberattaques ?

57 % Faire des simulations annuelles de bout en bout impliquant une équipe transversale composée de parties prenantes des services techniques, juridiques, stratégiques, exécutifs et de communication.

52 % Créer un référentiel en ligne et sécurisé des systèmes et informations critiques pour soutenir la réponse aux incidents et la restauration

48 % Identifier et corriger les failles des contrôles de sécurité avant de restaurer les systèmes en production

43 % Utiliser un environnement isolé pour enquêter sur les incidents, les corriger et restaurer de manière sécurisée

36 % Garantir l'immuabilité de toutes les données de sauvegarde

L'approche des entreprises du secteur public en matière de résilience des applications progresse, mais des lacunes subsistent. Près de la moitié identifient les lacunes des contrôles de sécurité avant de restaurer les systèmes et plus de la moitié organisent des exercices annuels de restauration. Un peu plus de la moitié disposent de référentiels en ligne protégés par un dispositif d'isolation des données, tandis qu'un peu moins s'appuient sur des environnements isolés pour procéder à des enquêtes sécurisées et à une restauration/reprise. Un pourcentage encore plus faible applique l'immuabilité à toutes les données de sauvegarde. Ces lacunes rendent les processus de restauration vulnérables à la réinfection ou à la perte de données. Une cyber-résilience mature associe la préparation à des zones de restauration sécurisées et vérifiables.

LA CLASSIFICATION DES DONNÉES S'IMPOSE PROGRESSIVEMENT, MAIS L'APPROCHE PILOTÉE PAR LE RISQUE RESTE À RENFORCER

Comment votre entreprise utilise-t-elle les approches/outils de découverte et de classification des données pour minimiser l'exposition aux risques liés aux données dans l'ensemble de son patrimoine de données ?

58 %

Identifier et corriger les violations de confidentialité et de sécurité des sauvegardes afin d'assurer la conformité

57 %

En cas de cyberattaque, nous utilisons la classification des données de sauvegarde pour déterminer les obligations de conformité liées aux données impactées

53 %

Identifier et hiérarchiser les systèmes pour la sauvegarde

51 %

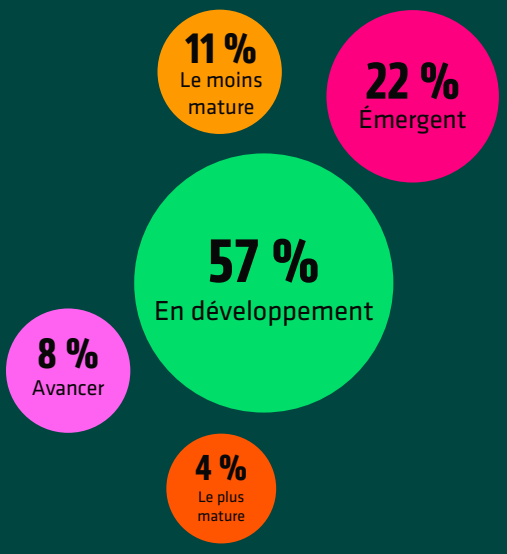
Définir et comprendre l'importance d'une cyberattaque avant qu'un incident ne survienne

Les entreprises du secteur public utilisent la découverte et la classification des données de manière plus stratégique pour la conformité, la réponse et la restauration. Plus de la moitié gèrent les violations de confidentialité et de sécurité et un peu plus de la moitié utilisent la classification des données pour guider les démarches de conformité pendant une attaque et définir en amont l'importance d'un incident. Une part similaire donne la priorité aux sauvegardes en fonction du risque. Ces modèles suggèrent que l'utilisation de la classification fondée sur le risque est encore en évolution. Une cyber-résilience mature transforme la classification en une approche systématique permettant d'optimiser l'exposition au risque liée aux données et d'éclairer les stratégies de protection, de réponse et de restauration.

UNE VISION PLUS CLAIRE DE LA MATURITÉ DE LA RÉSILIENCE

Une fois compilées, les réponses des personnes interrogées ont permis d'établir un baromètre de haut niveau de la maturité de la cyber-résilience. Elles ont révélé des tendances claires dans la manière dont les entreprises du secteur public construisent (ou peinent à construire) leur résilience dans la pratique. Si la majorité des entreprises en sont encore au stade du développement, seules 4 % d'entre elles possèdent les capacités intégrées les plus matures qui caractérisent les entreprises préparées à faire face aux risques.

LA COURBE DE MATURITÉ DE LA CYBER-RÉSILIENCE



Le moins mature (11 %) : Les sauvegardes, les stratégies et les mesures de sécurité sont souvent inexistantes ou incohérentes. La MFA et les contrôles administrateurs sont rarement appliqués, la restauration n'est souvent pas isolée et les évaluations de conformité ou d'importance sont généralement négligées.

Émergent (22 %) : Certaines pratiques de résilience sont en place, mais de manière incohérente. Les entreprises peuvent sauvegarder les données sensibles, appliquer des stratégies globales ou utiliser la MFA, mais rarement de manière combinée. Des efforts sont faits en matière de renseignement sur les menaces et de conformité, mais ils restent immatures et fragmentés.

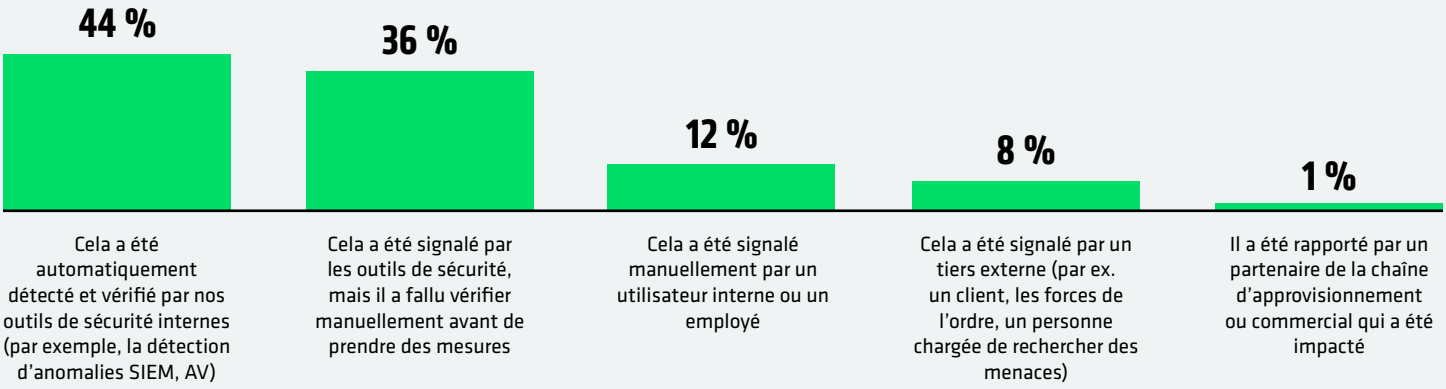
En cours de développement (57 %) : Les pratiques fondamentales, notamment les sauvegardes, les contrôles administrateurs et les renseignement sur les menaces, sont plus courantes, mais restent inégales. Les environnements de restauration, les contrôles de conformité et la correction des failles de sécurité sont appliqués de manière sporadique, ce qui limite l'efficacité des efforts en matière de résilience.

Avancé (8 %) : La plupart des pratiques clés sont systématiquement appliquées, notamment les stratégies de sauvegarde globales, les approbations des administrateurs et la correction avant la restauration. Les renseignements sur les menaces sont utilisés, mais ne sont pas pleinement optimisés, et il subsiste certaines lacunes en matière de restauration isolée et de couverture complète de la conformité.

Le plus mature (4 %) : La résilience est systématique et complète. Les données sensibles sont sauvegardées à l'échelle mondiale, la MFA et les contrôles administrateurs sont standard, les renseignement sur les menaces sont optimisés, la restauration est sécurisée grâce à la correction et les mesures de conformité sont systématiquement respectées.

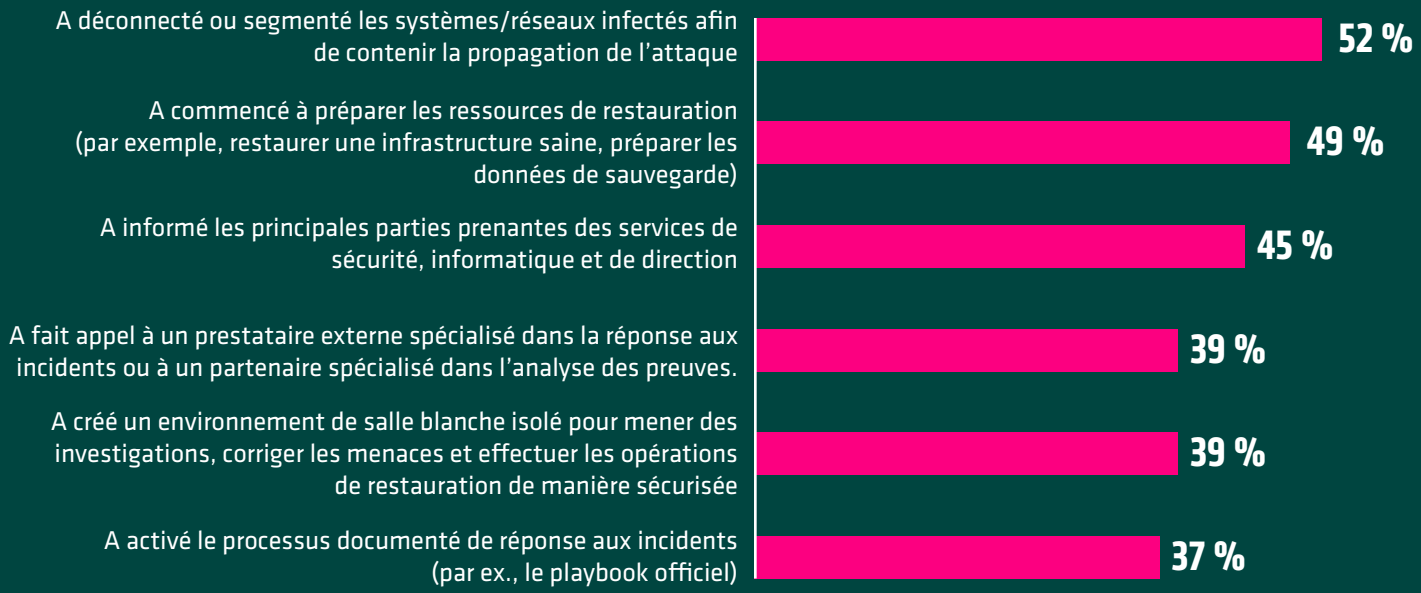
LA RÉSILIENCE DANS L'ADVERSITÉ

COMMENT LES ÉQUIPES ONT IDENTIFIÉ L'ATTAQUE



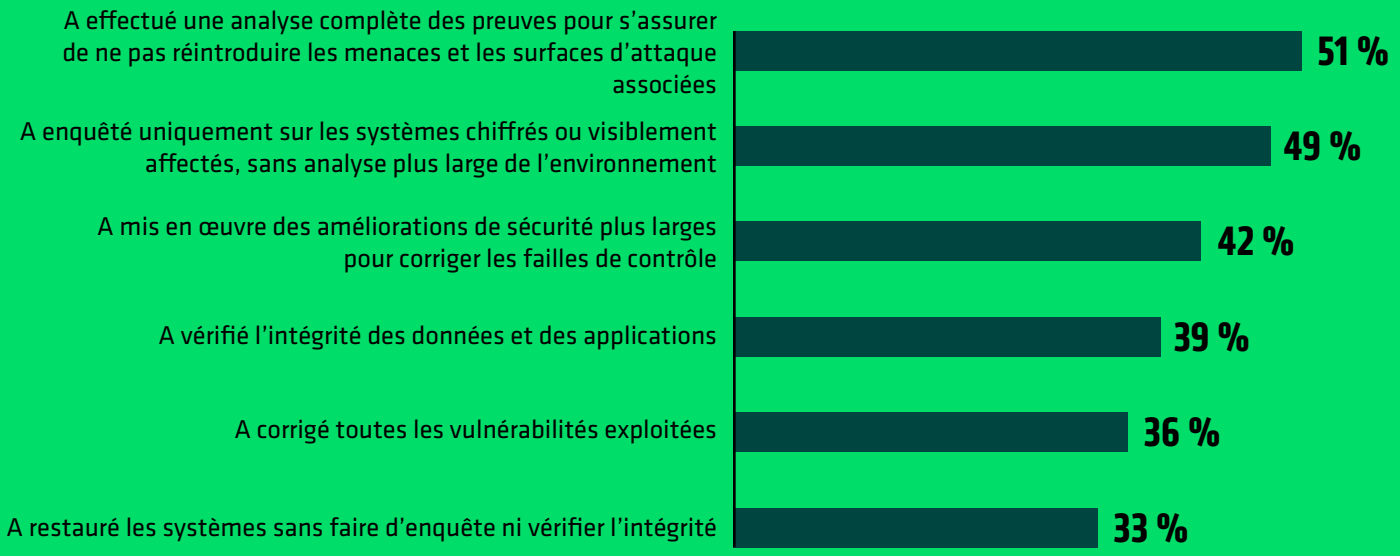
La plupart des entreprises du secteur public qui sont victimes d'une cyberattaque détectent les incidents via leurs dispositifs internes. La plus grande part des incidents est automatiquement identifiée et vérifiée par des outils de sécurité, tandis que beaucoup d'autres sont signalés par des outils, mais nécessitent une vérification manuelle. Beaucoup moins d'incidents sont signalés par les employés ou les parties externes. La détection est largement axée sur les outils, bien que la validation humaine joue toujours un rôle important.

MESURES PRISES PAR LES ÉQUIPES APRÈS CONFIRMATION DE L'ATTAQUE



Après avoir confirmé une attaque, les entreprises du secteur public ont pris des mesures variées pour contenir la menace et commencer la restauration. Environ la moitié ont déconnecté des systèmes infectés ou ont commencé à préparer des ressources de restauration propres, tandis que beaucoup ont informé des parties prenantes clés. Une plus petite part a créé des environnements de salle blanche isolés, activé des manuels d'intervention formels ou engagé des partenaires externes d'intervention en cas d'incident. Ces différences suggèrent que les efforts de réponse ne sont pas encore systématiquement standardisés entre les actions critiques.

MESURES PRISES AVANT DE REMETTRE LES SYSTÈMES ET LES DONNÉES EN LIGNE



Avant de remettre les systèmes et les données en ligne, les entreprises du secteur public ont pris une série de mesures d'analyse des preuves et de remédiation. Environ la moitié d'entre elles ont effectué des analyses de preuves complètes ou se sont concentrées uniquement sur les systèmes visiblement affectés, tandis qu'un nombre moindre a mis en œuvre des améliorations de sécurité plus larges, vérifié l'intégrité ou corrigé des vulnérabilités exploitées. Notamment, environ un tiers a restauré des systèmes sans investigation ni vérification, laissant des lacunes potentielles qui pourraient augmenter le risque de réinfection ou d'exposition résiduelle.

DIFFICULTÉS RENCONTRÉES PAR LES ÉQUIPES PENDANT L'ATTAQUE

54 %

Incapacité à communiquer ou à se coordonner au sein de notre équipe en raison de la panne des systèmes critiques (par ex., e-mail, applications collaboratives, système de tickets)

45 %

Pression de la direction pour restaurer les systèmes avant que l'attaque ne soit corrigée

42 %

Nous avons restauré, mais avons ensuite été réinfectés, car les menaces n'étaient pas entièrement éliminées

40 %

Les outils de sécurité ont été contournés et les sauvegardes ont été attaquées

39 %

Manque d'accès à des points de restauration sains et validés

Les équipes ont été confrontées à des défis opérationnels et techniques importants pendant l'attaque. Beaucoup ont eu du mal à communiquer alors que les systèmes critiques étaient hors ligne et ont ressenti une pression pour restaurer les systèmes avant que la correction ne soit terminée. D'autres ont signalé une évasion des outils de sécurité, des sauvegardes attaquées, un manque de points de récupération propres, voire une réinfection après la restauration. Ces difficultés mettent en évidence des lacunes dans l'état de préparation qui peuvent compliquer la réponse et prolonger la perturbation.

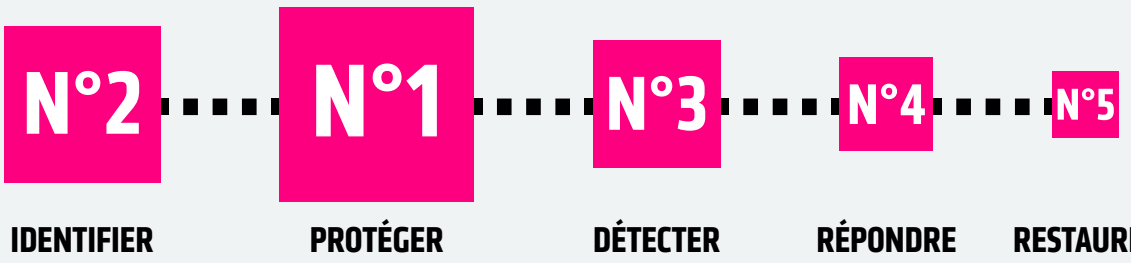
LES LACUNES PERSISTANTES DES INVESTISSEMENTS DANS LA RÉSILIENCE

Même les entreprises bien préparées peinent à maintenir leur résilience en cas d'attaque. Plus la pression opérationnelle augmente, plus les failles de coordination, les corrections incomplètes et les risques de réinfection révèlent à quel point la restauration peut être fragile sans processus unifiés ni assurance continue.

Ces tendances reflètent la manière dont les entreprises du secteur public allouent actuellement leurs budgets de cyber-résilience. Nous avons demandé aux répondants comment ils répartissaient leurs dépenses entre les cinq fonctions clés du Cadre de cybersécurité du NIST : Identifier, Protéger, Détecter, Répondre et Restaurer. La plupart continuent d'investir fortement dans la prévention, la protection et la détection, tandis que des financements comparativement moindres soutiennent la réponse et la restauration vérifiée. La courbe de maturité reste donc davantage axée sur la défense que sur la restauration, mettant en évidence une opportunité inexploitée de renforcer la résilience là où elle compte le plus : après l'attaque.

CADRE DE CYBERSÉCURITÉ DU NIST

La taille des cases indique la proportion des investissements en matière de cyber-résilience, de la plus élevée à la plus faible.



L'IA ET L'AUTOMATISATION S'IMPOSENT COMME DES MULTIPLICATEURS DE RÉSILIENCE

Les résultats montrent également que les entreprises du secteur public considèrent l'IA comme un puissant catalyseur de la cyber-résilience, notamment pour améliorer la rapidité de détection et la précision des réponses. Presque toutes les personnes interrogées ont jugé que des outils tels que la détection d'anomalies, l'analyse du comportement des utilisateurs, ainsi que l'investigation et la réponse aux menaces pilotées par l'IA étaient efficaces pour renforcer leur posture de sécurité.

Même les assistants basés sur l'IA générative plus récents, qui sont capables de traiter des requêtes en langage naturel et d'effectuer des analyses contextuelles, gagnent en popularité car ils permettent de simplifier et d'accélérer la prise de décision. 56 % des entreprises du secteur public victimes d'une cyberattaque ont déclaré avoir notamment appris qu'il était primordial de renforcer l'automatisation des processus de détection, de réponse et de restauration. Cela reflète la demande croissante de plateformes intégrées d'automatisation et d'orchestration, sur lesquelles l'IA agit comme un multiplicateur de force et permet d'améliorer l'efficacité, la cohérence et la performance de ces processus.

Si l'on se projette dans l'avenir, la plupart des personnes interrogées s'attendent à ce que l'IA joue un rôle de plus en plus stratégique dans la cyber-défense d'ici fin 2026. 43 % estiment que l'IA soutiendra la prise de décision humaine en renforçant les capacités d'analyse et de recommandation, l'humain conservant la maîtrise des décisions et des actions finales. 42 % s'attendent à ce que l'IA devienne un élément central des processus de détection et de réponse, voire qu'elle prenne certaines décisions de manière autonome. Cela indique une trajectoire claire : l'IA passe du statut d'assistant à celui de pilier opérationnel de la cyber-résilience, et s'apprête à améliorer la rapidité, la précision et la confiance dans les domaines de la détection, de la réponse et de la restauration.

L'AVENIR DE LA RÉSILIENCE COMMENCE MAINTENANT

Bien que les entreprises du secteur public fassent des progrès notables en matière de cyber-résilience, beaucoup d'entre elles ont encore du chemin à parcourir pour améliorer leur réponse, leur restauration et la validation de leur niveau de préparation après une attaque. La cyber-résilience représente un avantage concurrentiel considérable. L'avenir appartient aux entreprises qui investissent dans les personnes, les produits et les processus nécessaires pour restaurer plus rapidement, conserver la confiance de leurs clients et maintenir leur activité lorsque d'autres n'y arrivent pas. Lorsqu'il est pratiquement impossible d'éviter une perturbation, la résilience n'est pas seulement une protection, c'est un véritable levier de performance.

Renforcez votre résilience avant d'être confronté à une crise :

- Réservez un atelier sur la résilience face aux ransomwares.
- Passez au niveau supérieur grâce à un plan d'action en cinq étapes pour renforcer votre cyber-résilience.
- En savoir plus sur les solutions de cyber-résilience de Cohesity
  - Secteur public
  - État, collectivités locales et éducation

MÉTHODOLOGIE

COHESITY

En septembre 2025, Cohesity a chargé Vanson Bourne d'interroger 3 200 décideurs informatiques et responsables de la sécurité. Cette enquête a permis d'établir les conclusions présentées ici. Les personnes interrogées représentent des entreprises aux États-Unis (500), au Brésil (200), au Royaume-Uni (400), en Allemagne (400), en France (400), aux Émirats arabes unis (100), en Australie (200), en Corée du Sud (200), au Japon (400), en Inde (200) et à Singapour (200). Ces entreprises comptaient au moins 1 000 employés et provenaient de divers secteurs publics et privés, notamment les services financiers, le secteur public et la santé.

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000090-001 FR 6-2026