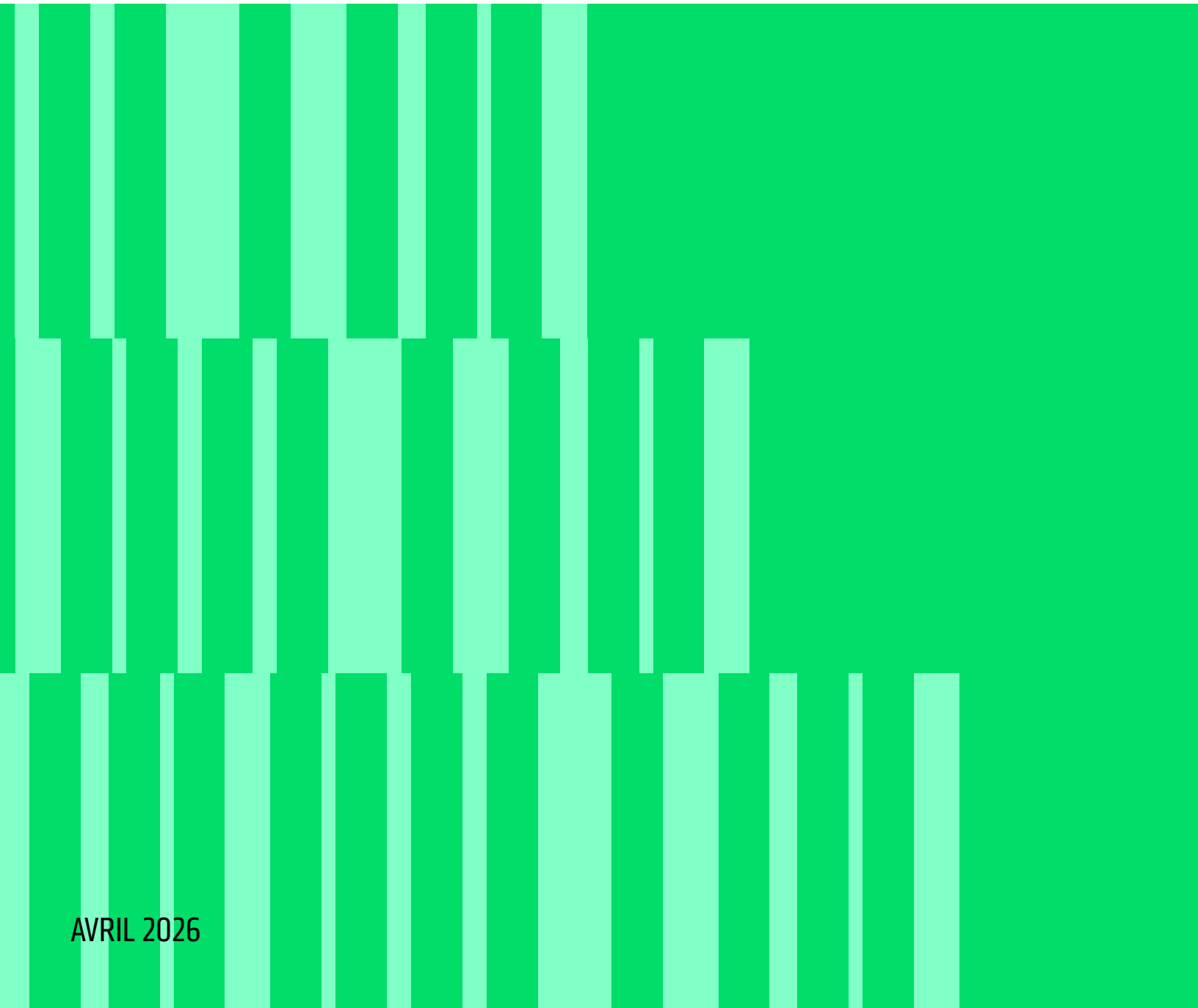
COHESITY

RAPPORT SUR LA CYBER-RÉSILIENCE

Être préparé aux risques ou y être exposé :
Cyber-résilience : les services financiers face à un déficit critique



AVRIL 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, 390 provenaient du secteur des services financiers. Leurs réponses révèlent une fracture croissante en matière de résilience entre les acteurs des services financiers prêts à faire face au risque, capables d'assurer une restauration rapide et maîtrisée, et leurs homologues plus exposés, qui demeurent vulnérables à des interruptions prolongées ainsi qu'aux conséquences financières qui en découlent.

Notre étude examine les impacts concrets des cyberattaques majeures, la manière dont les acteurs des services financiers ont évalué leur cyber-résilience au regard des bonnes pratiques, ainsi que les mesures qu'ils ont mises en place pour détecter ces incidents, y répondre et restaurer leurs activités. 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. Pour de nombreux acteurs des services financiers, gérer des tentatives de phishing, des incursions malveillantes ou des interruptions système fait presque partie du quotidien. 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 SERVICES FINANCIERS, CES ATTAQUES LOURDES EN CONSÉQUENCES NE SONT PLUS L'EXCEPTION : ELLES S'INSCRIVENT DÉSORMAIS DANS UNE DYNAMIQUE RÉCURRENTE.

77 %

des répondants ont été confrontés à au moins une cyberattaque majeure

57 %

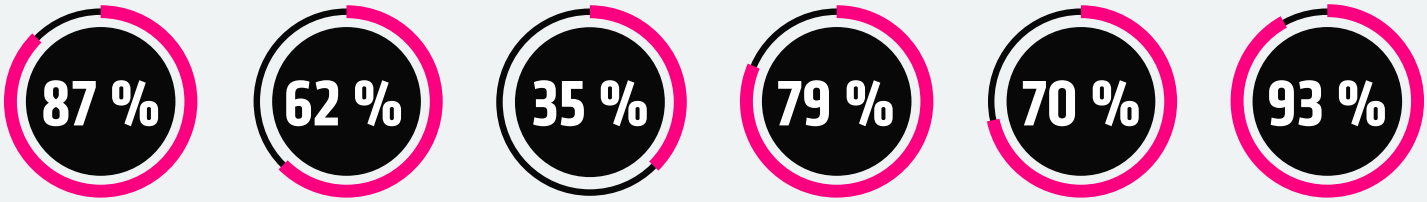
en ont subi une au cours des 12 derniers mois

27 %

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 DE SERVICES FINANCIERS 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 (51 %) et des actions en justice/recours collectifs (41 %)

[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

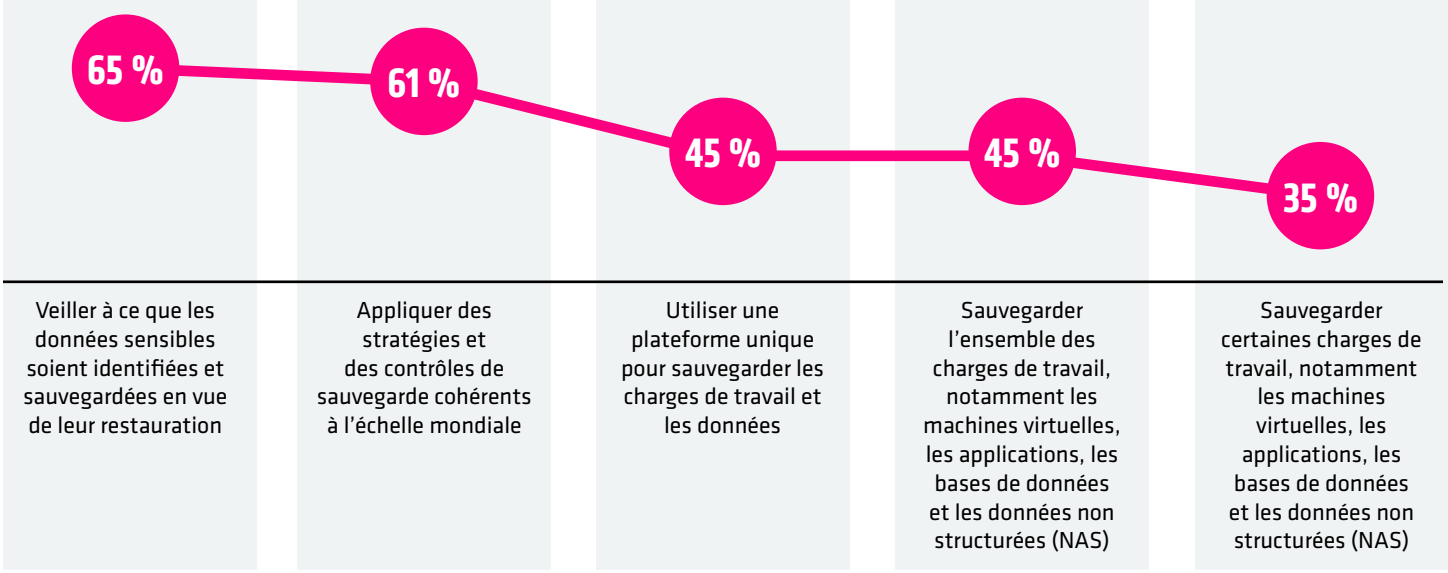
Compte tenu de l'ampleur des répercussions financières et opérationnelles révélées par notre étude, on pourrait s'attendre à ce que la résilience organisationnelle soit un sujet de préoccupation très répandu. Près de la moitié des personnes interrogées (46 %) se sont dites totalement convaincues que 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 ?



Près des deux tiers des acteurs des services financiers veillent à ce que les données sensibles soient identifiées et sauvegardées en vue de leur restauration, tandis qu'une proportion légèrement inférieure applique des politiques de sauvegarde cohérentes à l'échelle mondiale. Moins de la moitié sauvegardent l'ensemble des charges de travail ou s'appuient sur une plateforme unique. Près d'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

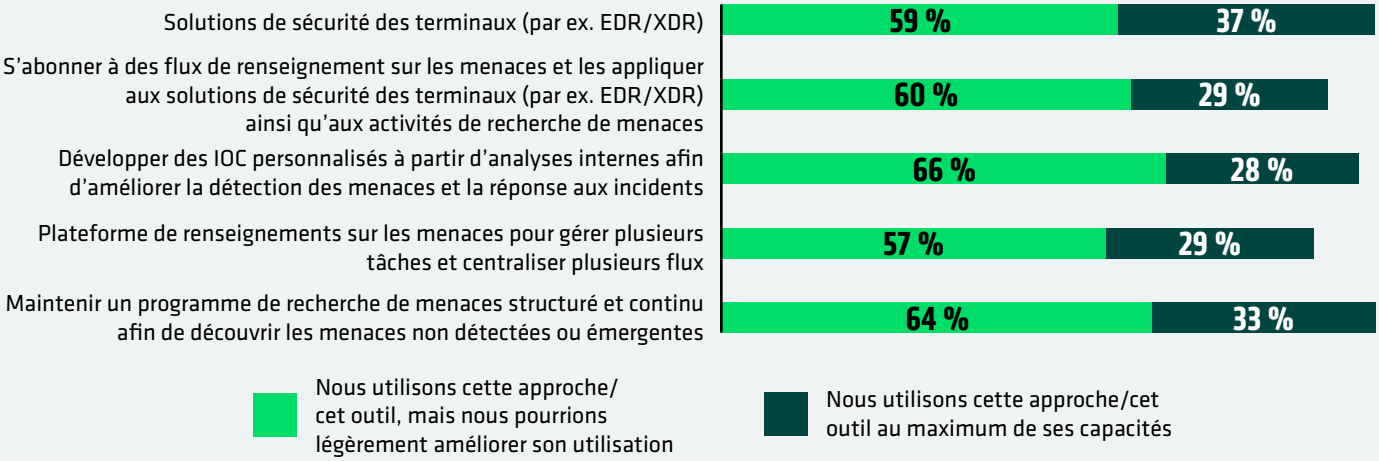
Que fait votre entreprise pour garantir la capacité de récupération de ses données ?

64 %	Exiger une autorisation supplémentaire pour les tâches administratives à risque élevé associées aux solutions de sauvegarde et de restauration
61 %	Authentification multifacteur sur notre solution de sauvegarde
48 %	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)
45 %	Protéger les données critiques grâce à l'immuabilité
41 %	Appliquer le principe du moindre privilège aux charges de travail sauvegardées

De nombreux acteurs des services financiers ont renforcé les contrôles d'accès autour des environnements de sauvegarde : près des deux tiers exigent une autorisation administrative supplémentaire pour les tâches à risque élevé, et un peu plus de la moitié imposent l'authentification multifacteur (MFA). Près de la moitié respectent la règle 3-2-1 et un pourcentage légèrement inférieur protège les données critiques via des sauvegardes immuables. En revanche, une part plus limitée met en œuvre des droits d'accès conformes au moindre privilège. 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'ANALYSE 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 acteurs des services financiers ont recours à des solutions de sécurité des terminaux, à des flux de renseignement sur les menaces et à des programmes structurés de recherche proactive de menaces. Pourtant, seule une minorité en tire pleinement parti. L'adoption de capacités avancées telles que des indicateurs de compromission (IOC) personnalisés et des plateformes de renseignement sur les menaces reste particulièrement limitée. 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 ?

64 % 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.

61 % Identifier et corriger les failles des contrôles de sécurité avant de restaurer les systèmes en production

60 % Créer un référentiel en ligne et sécurisé des systèmes et informations critiques pour soutenir la réponse aux incidents et la restauration

51 % Utiliser un environnement isolé pour enquêter sur les incidents, les corriger et restaurer de manière sécurisée

39 % Garantir l'immuabilité de toutes les données de sauvegarde

L'approche des services financiers en matière de résilience des applications progresse, mais des lacunes subsistent. Un peu plus de la moitié identifient les lacunes des contrôles de sécurité avant toute restauration des systèmes, tandis que près des deux tiers procèdent chaque année à des exercices de reprise des activités. Environ six sur dix disposent de référentiels en ligne protégés par un dispositif d'isolation des données, tandis qu'un peu plus de la moitié s'appuient sur des environnements isolés pour procéder à des enquêtes sécurisées et à une restauration/reprise. Moins de la moitié mettent en œuvre l'immuabilité sur l'ensemble des 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 ?

67 %

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

62 %

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

59 %

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

56 %

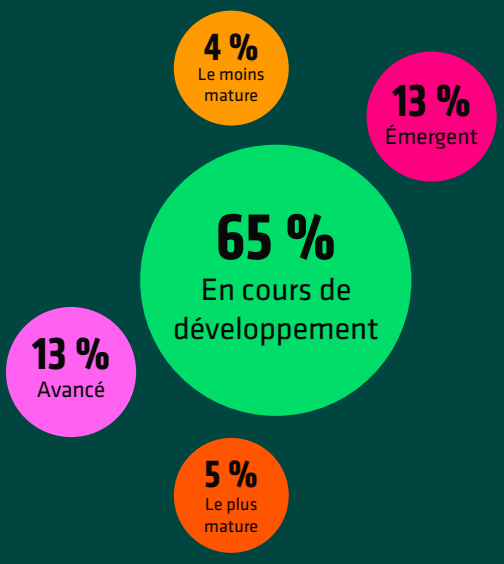
Identifier et hiérarchiser les systèmes pour la sauvegarde

Les acteurs des services financiers utilisent de manière plus stratégique la découverte et la classification des données pour renforcer la conformité, la réponse aux incidents et la restauration. Près des deux tiers gèrent les violations de confidentialité et de sécurité et utilisent la classification des données pour guider les démarches de conformité pendant une attaque. En revanche, ils sont moins nombreux à définir en amont l'importance d'un incident ou à hiérarchiser les sauvegardes selon le risque. Ces lacunes 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 services financiers développent (ou peinent à développer) leur résilience opérationnelle. Si la majorité des entreprises en sont encore au stade du développement, seules 5 % 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 RÉSILIENCE CYBER



Le moins mature (4 %) : 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 (13 %) : 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.

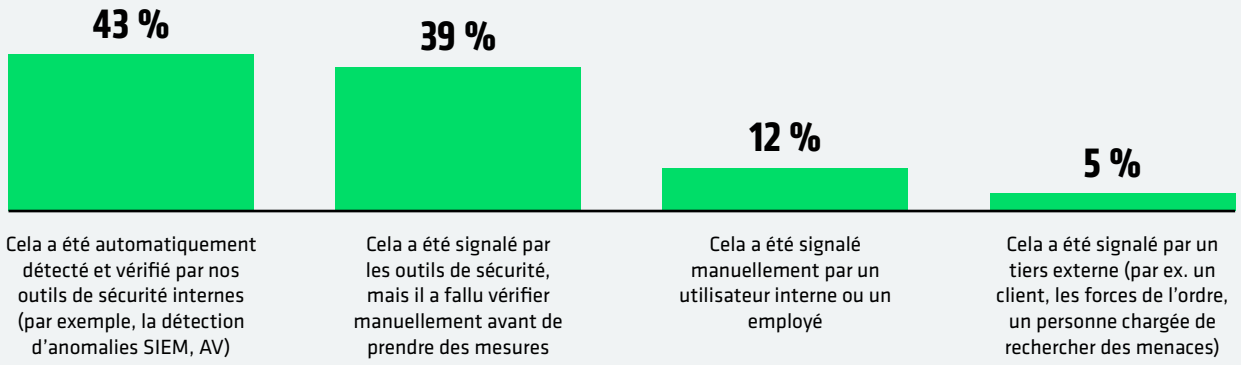
En cours de développement (65 %) : Les pratiques fondamentales, notamment les sauvegardes, les contrôles administrateurs et les renseignement sur les menaces, sont plus courantes, mais restent inégales. Les environnements de restauration, les contrôles de conformité et la correction des failles de sécurité sont appliqués de manière sporadique, ce qui limite l'efficacité des efforts en matière de résilience.

Avancé (13 %) : 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 (5 %) : 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.

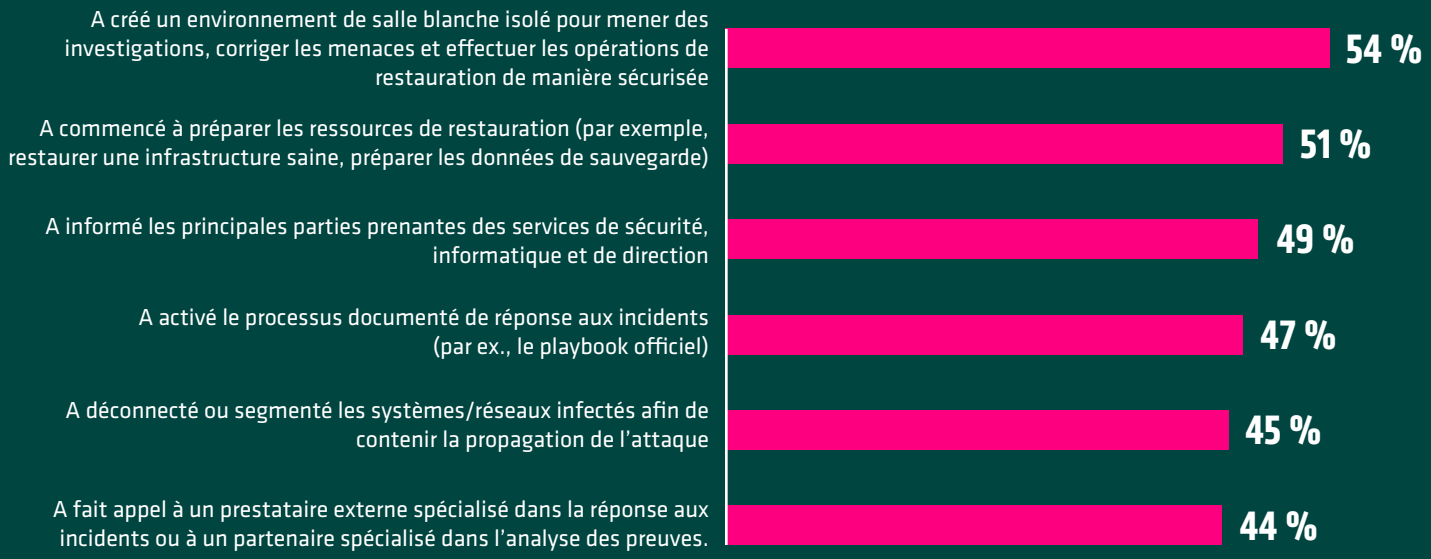
LA RÉSILIENCE DANS L'ADVERSITÉ

COMMENT LES ÉQUIPES ONT IDENTIFIÉ L'ATTAQUE



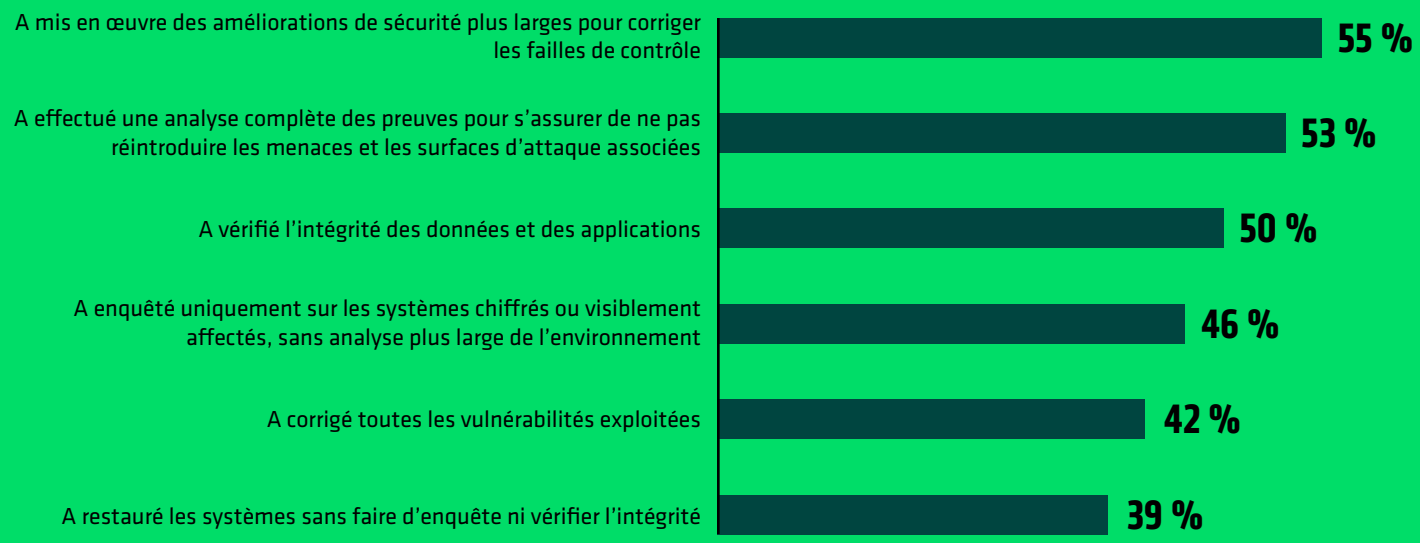
La plupart des services financiers qui sont victimes d'une cyberattaque détectent les incidents via leurs dispositifs internes. Près de la moitié des acteurs du secteur financier ont indiqué que les attaques étaient automatiquement identifiées et vérifiées par leurs propres outils de sécurité, tandis que plus d'un tiers ont signalé qu'elles étaient détectées par des outils mais nécessitaient une vérification manuelle avant toute action. Seule une faible proportion des incidents a été signalée par des rapports de tiers. Ainsi, la détection repose principalement sur des dispositifs internes, mais nécessite toujours une confirmation humaine.

MESURES PRISES PAR LES ÉQUIPES APRÈS CONFIRMATION DE L'ATTAQUE



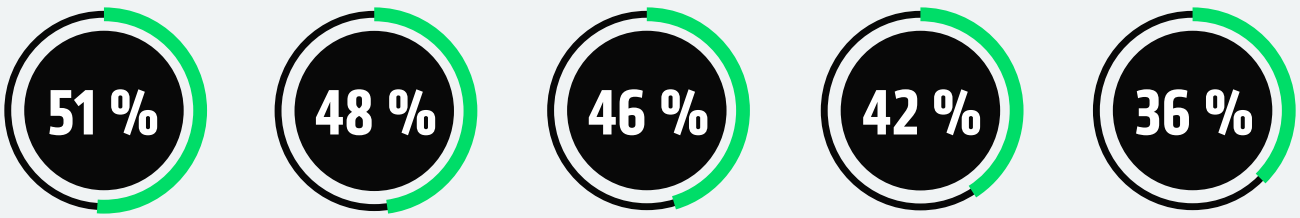
Après confirmation d'une attaque, les acteurs des services financiers ont entrepris diverses actions pour assurer la restauration. Un peu plus de la moitié ont initié la restauration d'une infrastructure intègre ou la mise en quarantaine de données de sauvegarde, tandis qu'un pourcentage légèrement supérieur disposait déjà d'environnements isolés et sécurisés dédiés aux enquêtes et à la restauration. Une proportion plus faible a informé les parties prenantes clés, isolé les systèmes infectés, activé des procédures formelles de réponse ou fait appel à des experts externes en réponse à incident ou en analyse post-incident. Ces variations indiquent que les actions de réponse ne sont pas encore pleinement standardisées pour les étapes critiques.

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



Avant de remettre les systèmes en ligne, les acteurs des services financiers ont mené un ensemble d'actions d'analyse post-incident et de remédiation. Plus de la moitié ont déployé des mesures de sécurité renforcées à plus grande échelle ou conduit une analyse de preuves complète. La moitié a par ailleurs contrôlé l'intégrité des données et des applications. En revanche, ils sont moins nombreux à avoir étendu l'enquête au-delà des systèmes manifestement impactés ou à avoir appliqué des correctifs sur les vulnérabilités exploitées. Plus d'un tiers ont restauré les systèmes sans investigation complète ni vérification d'intégrité, laissant des failles propices à la réinfection et à des risques résiduels.

DIFFICULTÉS RENCONTRÉES PAR LES ÉQUIPES PENDANT L'ATTAQUE



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)

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

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

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

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

Les équipes ont signalé d'importants défis tout au long du processus. Beaucoup ont rencontré des difficultés de communication ou de coordination pendant que les systèmes critiques étaient hors ligne. Près de la moitié ont subi une pression pour restaurer les opérations avant la fin des mesures correctives. L'évasion des outils de sécurité, la réinfection et l'absence de points de reprise propres ont aggravé les difficultés, soulignant la nécessité de mesures de résilience plus robustes.

LES LACUNES PERSISTANTES DES INVESTISSEMENTS DANS LA RÉSILIENCE

Même les services financiers bien préparés 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 services financiers 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 de la boîte montre la proportion des investissements en cyberrésilience de la plus grande à la plus petite

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

Les résultats montrent également que les acteurs des services financiers voient dans l'IA un puissant facteur d'amélioration de la cyber-résilience, notamment pour renforcer la rapidité de la détection et la précision de la réponse. 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. Cinquante-six pour cent des services financiers 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. 49 % 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. 39 % 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 acteurs des services financiers enregistrent des progrès mesurables en matière de cyber-résilience, beaucoup disposent encore de marges de progression dans la réponse, la restauration et la validation de leur état de préparation à la suite d'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 pour les services financiers.

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

2000083-001-FR 5-2026