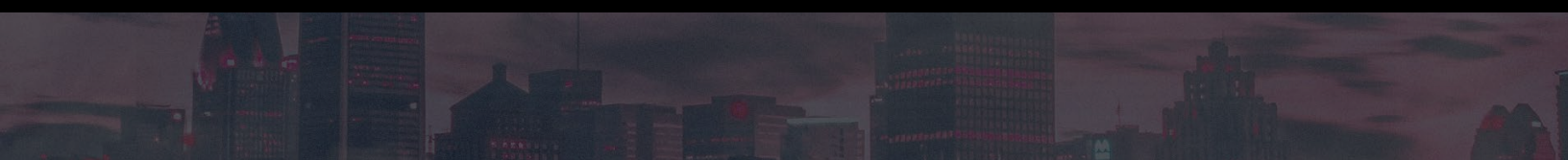
RAPPORT SUR L'ÉTAT DE PRÉPARATION À LA CYBER-RÉCUPÉRATION

2024

Commvault®

In partnership with GIGAOM



Chère lectrice, cher lecteur,

Bienvenue à un moment charnière dans l'évolution de la cyber-résilience. Depuis la création de The Collaborative au début de l'année 2024, notre mission est claire : forger des partenariats solides avec des analystes, des leaders du secteur et des visionnaires comme vous, afin d'explorer en profondeur et d'améliorer la cyber-résilience au sein de différentes organisations. Notre rapport fondateur, « Seven Emerging Trends in Cyber Resilience » (Sept tendances émergentes en matière de cyber-résilience), a déjà établi le programme de cette année, en abordant des domaines critiques face à la menace croissante des ransomwares.

Nous sommes heureux d'annoncer la publication du Rapport 2024 sur l'état de préparation à la cyber-récupération, une collaboration entre Commvault et GigaOm. Votre leadership et votre expertise en matière d'informatique et de sécurité sont essentiels pour orienter l'avenir vers une cyber-résilience accrue. Ce rapport est conçu pour vous fournir des informations et des données essentielles qui permettront à votre organisation de garder une longueur d'avance dans un cyberpaysage de plus en plus instable.

Les informations que nous partageons sont issues d'une enquête approfondie menée auprès de 1 000 responsables mondiaux de la cybersécurité et des technologies de l'information. Ce rapport offre non seulement une vision mondiale des défis à relever, mais il met également en évidence les stratégies efficaces qui sont essentielles à la préparation à la cyber-récupération. Il souligne la nécessité de mettre en place des stratégies globales de reprise des activités informatiques qui dépassent les plans traditionnels de récupération après sinistre.

Principales conclusions :

- Avec un chiffre stupéfiant, 83 % des organisations ont récemment subi une violation matérielle de la sécurité, et plus de la moitié au cours de la seule année écoulée, ce qui souligne la nécessité impérieuse d'une préparation avancée et de stratégies de réponse efficaces.

- Les organisations les plus résilientes partagent des pratiques communes qui améliorent considérablement leur préparation à la reprise. Notre analyse révèle que les organisations les mieux préparées présentent au moins quatre des cinq marqueurs clés de maturité.

- Il existe une corrélation évidente entre la cybermaturité et la vitesse de récupération. Les organisations dont le niveau de cybermaturité est le plus élevé se remettent des violations 41 % plus rapidement que celles qui sont moins bien préparées.

- Les tests réguliers des plans de cyber-récupération ne sont pas seulement bénéfiques : ils sont essentiels. Nos données montrent une différence prononcée dans la fréquence des tests entre les organisations qui ont subi des violations et celles qui n'enont pas subi.

Recommandations :

1. Testez et améliorez régulièrement vos plans de récupération. Des exercices et des mises à jour fréquents permettent à votre organisation de réagir rapidement et efficacement à tout cyberincident.

2. Donnez la priorité au renforcement de la cybermaturité en adoptant les marqueurs identifiés de l'état de préparation à la cyber-récupération. Cela permet non seulement d'atténuer les risques, mais aussi de réduire considérablement l'impact des violations potentielles.

3. Élaborez une stratégie holistique de cyber-récupération, qui va au-delà de la simple sauvegarde de données et englobe la reprise complète du système, afin d'assurer la continuité de l'activité globale de l'entreprise.

Nous vous invitons à vous plonger dans le rapport et à intégrer ces idées et recommandations dans votre planification stratégique. Notre objectif n'est pas seulement d'informer, mais d'inspirer une action décisive qui renforcera fermement votre organisation contre les cybermenaces futures.

Nous sommes là pour vous soutenir dans votre démarche vers une préparation inégalée à la cyber-récupération.

Bien cordialement,

The Collaborative

TABLE DES MATIÈRES

UNE VIOLATION PEUT DONNER UNE LEÇON

L'expérience d'une violation a un impact significatif sur la manière dont une organisation aborde la résilience.

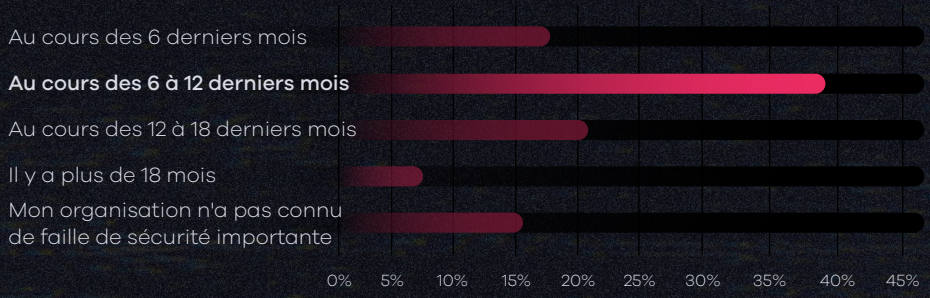
Malheureusement, les violations sont beaucoup trop fréquentes et touchent des entreprises de toutes tailles et de tous secteurs. Comme toute expérience dramatique, la lutte contre une violation modifie le comportement d'une organisation et la façon dont elle fixe les priorités en ce qui concerne ses actions. C'est l'une des conclusions de notre premier Rapport sur l'état de préparation à la cyber-récupération, un effort conjoint de Commvault et de GigaOm.

Nous avons interrogé 1 000 responsables de la cybersécurité et de l'informatique dans le monde entier afin de mieux comprendre l'état global de préparation à la cyber-récupération et d'avoir une compréhension précise de la manière dont les organisations restent résilientes face au chaos et aux dommages causés par les violations. Pour plus de détails sur notre méthodologie et les personnes interrogées, se reporter à la page 17.

Notre enquête a confirmé la prévalence des infractions, 83 % des personnes interrogées ayant signalé une faille cruciale de la sécurité : plus de 50 % d'entre elles sont intervenues au cours de l'année écoulée et plus de 75 % au cours des 18 derniers mois (Figure 1). Les violations coûtant jusqu'à **12 millions de dollars par jour**, la capacité à se rétablir rapidement est de ¹ère importance.

Figure 1

À quand remonte la dernière violation importante de la sécurité de votre organisation?



83% de notre échantillon ont fait état d'une violation importante de la sécurité, dont plus de **50%** de celles-ci au cours de **l'année écoulée.**

1 SolarWinds : Pingdom Team, Average Cost of Downtime per Industry, 9 janvier 2023.

L'une des principales conclusions de l'ensemble des données est qu'il y a de nombreux enseignements à tirer du fait d'avoir subi une violation.

Les organisations acquièrent une expérience qui modifie leurs perspectives, leurs priorités et, souvent, leur maturité. À titre d'exemple, les organisations qui ont subi une violation sont près de 2,5 fois plus susceptibles de classer la compréhension du profil de risque des données, la classification des données et le niveau relatif de risque comme une priorité absolue de leur stratégie de cyber-récupération, par rapport aux organisations qui n'ont pas subi de violation (Figure 2).

Figure 2

En réponse aux incidents de sécurité, quelles sont les priorités de votre organisation en ce qui concerne sa stratégie de cyber-récupération ?

Organisations ayant subi une faille cruciale de la sécurité par rapport à l'ensemble des répondants

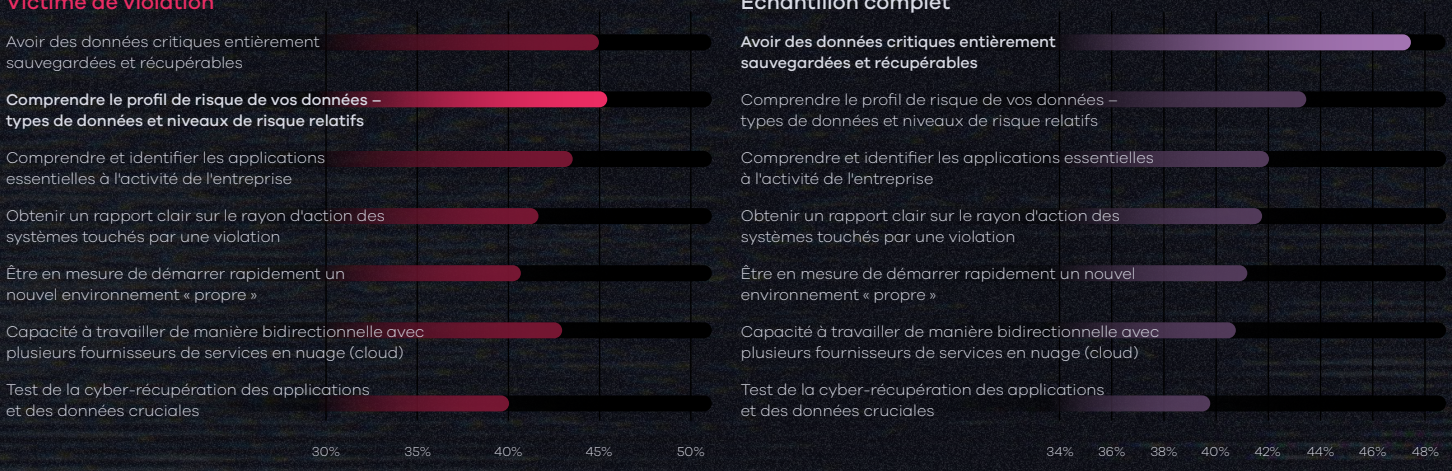
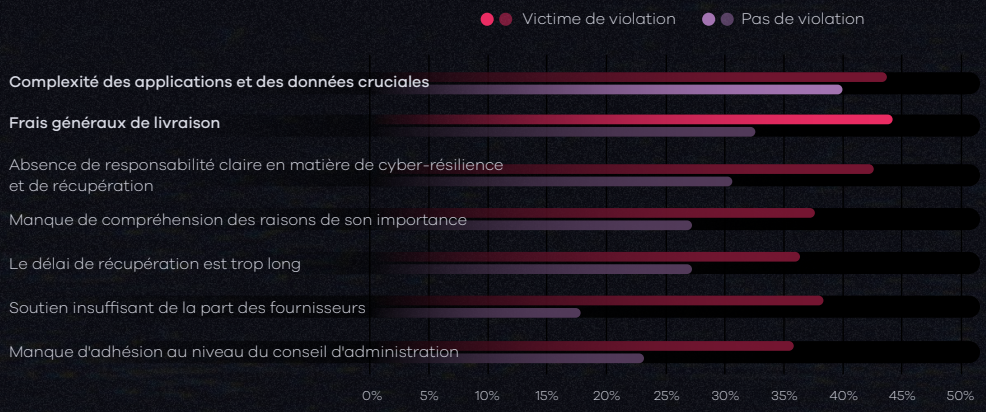


Figure 3

Selon vous, quels sont les défis d'ensemble à relever en matière de cyber-résilience ?

Répartition des données: Avez-vous été victime d'une violation?



Dans l'ensemble, les organisations qui n'ont pas été victimes d'une violation ont une vision plus étroite, citant la nécessité d'avoir des données critiques entièrement sauvegardées et récupérables comme l'un des trois premiers choix dans près de 60 % des cas (Figure 3). Les organisations qui ont été victimes d'une violation accordent une importance supérieure à un ensemble plus large de pratiques, en commençant par la compréhension de leur profil de risque en matière de donnéeset les classifications.

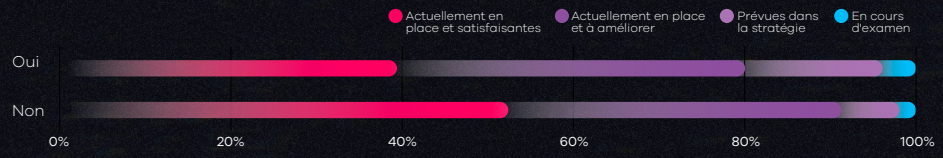
Cela signifie qu'une fois qu'une organisation a été victime d'une violation et qu'elle a compris les implications des actions à entreprendre pour y répondre, ses priorités changent. Ces organisations ont appris qu'il y a des domaines clés à intégrer, qui peuvent être moins évidents pour ceux qui n'ont pas été victimes d'une violation comme : la communication avec les parties prenantes, la collaboration avec les fournisseurs, l'appropriation claire et la répartition des responsabilités. Ceux qui n'ont pas été victimes de violations se concentrent principalement sur la seule vitesse.

Les organisations ayant subi une violation sont également moins satisfaites de l'état de leurs outils d'alerte précoce que celles qui n'ont pas signalé de violation (Figure 4), ce qui suggère un certain degré d'autosatisfaction dans le groupe des organisations n'ayant pas subi de violation.

Figure 4

Dans quelle mesure votre organisation dispose-t-elle des capacités suivantes pour la reprise après un incident de sécurité ?

Mesures spécifiques visant à montrer l'état de préparation à la cyber-récupération des activités informatiques et le risque par rapport à la violation.

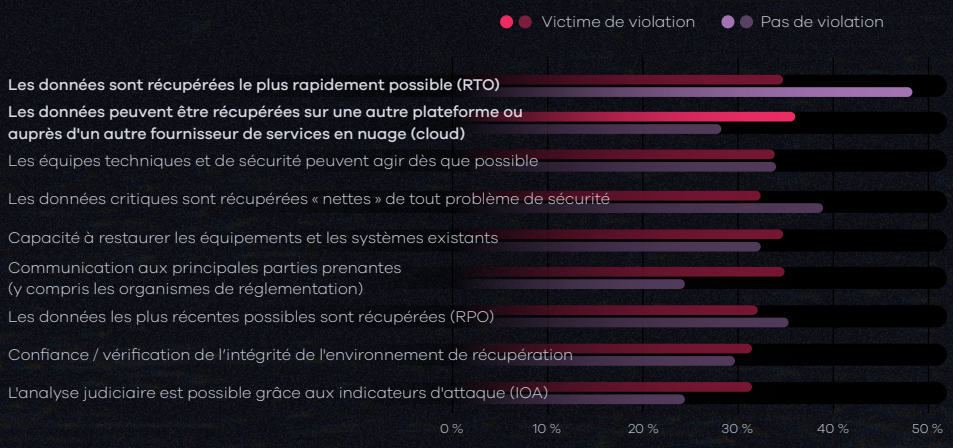


Dans l'ensemble, celles qui ont été victimes d'une violation se préparent de manière plus complète – elles sont plus susceptibles d'avoir des plans, et elles les testent plus fréquemment. En réponse à une violation, elles donnent la même priorité à l'augmentation des capacités et des activités plutôt qu'à l'amélioration des performances de quelques éléments (Figure 5).

Figure 5

À la suite d'un incident de sécurité, quelles sont selon vous les cinq principales priorités de votre organisation ?

Combinaison des réponses classées en première, deuxième et troisième position



LES CYBERDÉFIS À SURMONTER

Dans un paysage de risques qui évolue rapidement, les organisations accordent la priorité à la protection des données.

Pour les professionnels de la sécurité et de l'informatique, le paysage des risques est en constante évolution : ils sont particulièrement préoccupés par les menaces externes, et les organisations doivent assumer les violations. Les organisations réalisent que la question n'est pas de savoir *si* ou *quand* elles seront victimes d'une violation, mais plutôt de savoir quand elles découvriront *qu'elles ont déjà* été victimes d'une violation.

Face à cette réalité, les professionnels de la sécurité et de l'informatique sont confrontés à une série de défis redoutables. Pour les répondants, les principaux défis à relever en matière de sécurité sont les suivants : des hackers et des types d'attaques de plus en plus sophistiqués, l'utilisation de l'intelligence artificielle par les cybercriminels, une surface d'attaque plus large grâce au cloud et au SaaS, et l'adoption de technologies basées sur l'IA dans l'ensemble des outils de sécurité (Figure 6).

Figure 6

Quels sont, selon vous, les plus grands défis à relever pour assurer la cybersécurité de votre organisation?

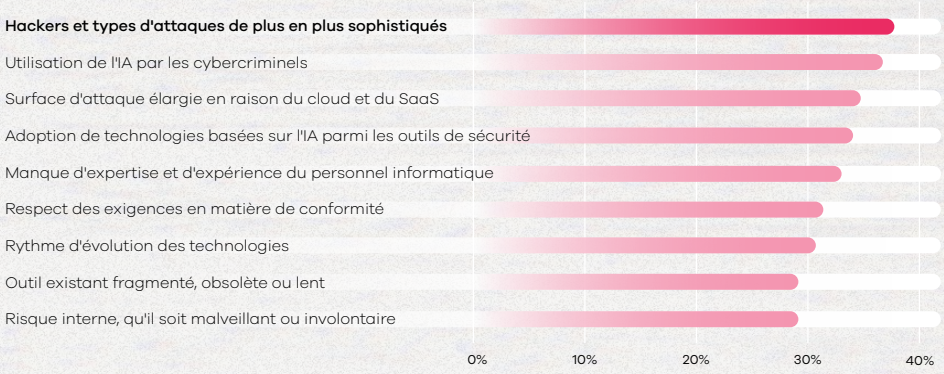
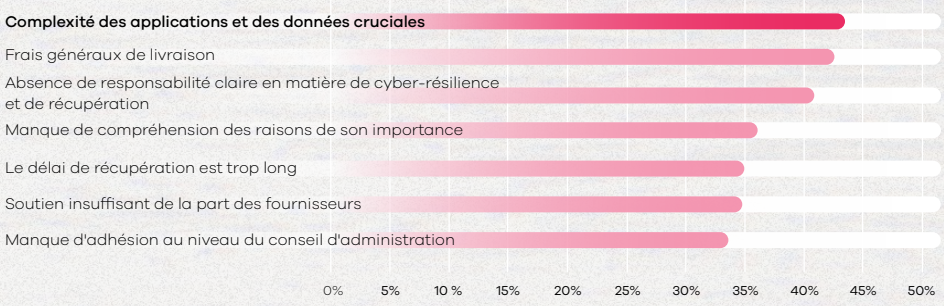


Figure 7

Selon vous, quels sont les défis d'ensemble à relever en matière de cyber-récupération?



La **complexité des applications et des données cruciales** est le principal défi en matière de cyber-récupération cité par 44% des répondants, suivie par le coût.

Un nombre important d'organisations **(42 %)** ne savent pas précisément qui est responsable de la conduite des stratégies et de l'exécution de la cyber-résilience et de la reprise des activités (Figure 7).

Adoption de plusieurs capacités générales de sécurité – gestion de l'identité et de l'accès ; protection contre les intrusions, détection et réaction ; prévention / protection contre la perte de données ; et gestion de la posture de sécurité – située dans la fourchette comprise entre **75 % et 80 %**, la solution actuellement en place étant soit satisfaisante, soit à améliorer (Figure 8).

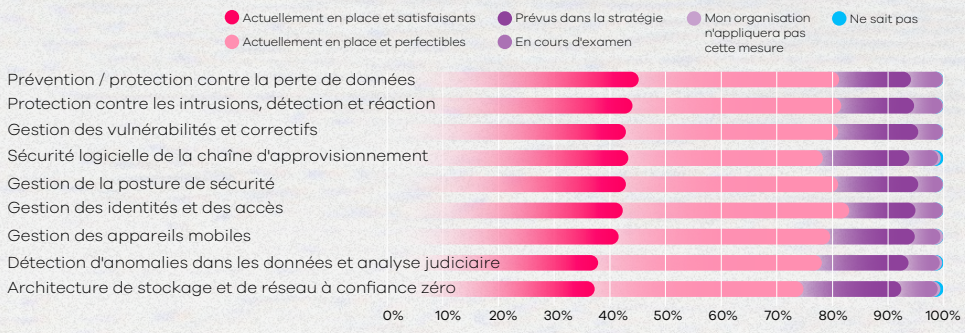
Toutefois, si l'on dresse un constat global,

42% des personnes interrogées sont **satisfaites** de leur cybersécurité générale, tandis que

38% considèrent qu'il **est nécessaire d'améliorer** leurs mesures de cybersécurité.

Figure 8

Dans quelle mesure les principaux éléments suivants de l'architecture de cybersécurité de votre organisation ont-ils été adoptés et / ou mis en œuvre?



MARQUEURS DE CYBERMATURITÉ

Les pratiques et capacités clés marquent la maturité d'une organisation en matière de cyber-résilience.

Bien que les organisations puissent citer des mesures spécifiques comme priorités, c'est la manière dont elles se comportent qui importe vraiment. En analysant les organisations les plus résilientes, nous avons constaté qu'elles utilisaient de nombreuses mesures, mais que cinq pratiques étaient les plus importantes pour déterminer leur véritable état de préparation. Nous appelons ces pratiques des marqueurs de maturité (voir 5 marqueurs de l'état de préparation à la cyber-récupération, page 9).

Les organisations présentant quatre ou cinq marqueurs sont considérées comme matures sur le plan cybernétique. Ces entreprises déclarent subir moins de violations et se rétablir plus rapidement lorsqu'elles en sont victimes.

Cependant, notre enquête a révélé que seulement 4 % des organisations ont déployé les cinq marqueurs, et que seulement 13 % d'entre elles en pratiquent au moins quatre. Au bas de la courbe de maturité, 14 % des entreprises n'ont pas du tout mis en place de marqueurs clés (Figure 9).

Alors que moins de la moitié des organisations ont confiance en leurs plans de récupération (Figure 10), plus de la moitié des organisations ayant atteint la maturité cybernétique (54 %) sont beaucoup plus confiantes dans leur capacité à récupérer les systèmes et les données critiques après un incident majeur (Figure 13, page 11).

Figure 9

Quel est l'état de préparation de votre organisation à la reprise après un incident de sécurité, sur la base de l'utilisation de capacités spécifiques ?

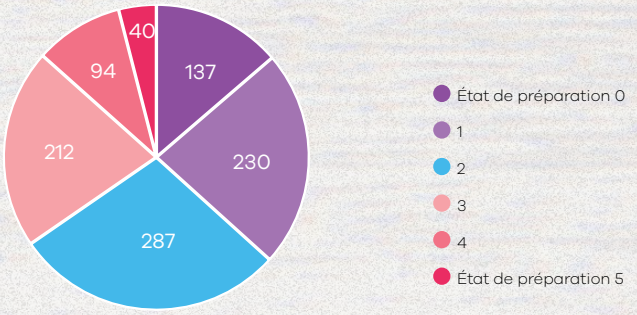
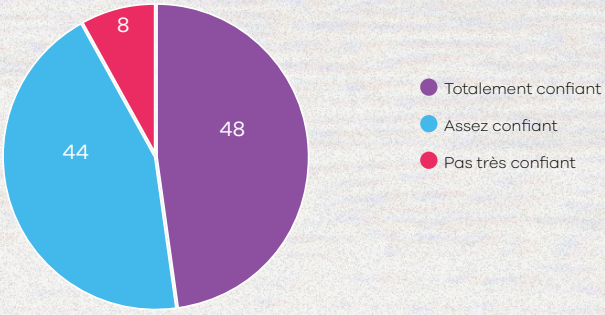


Figure 10

Dans quelle mesure êtes-vous convaincu d'avoir mis en place un plan de récupération solide, spécifique aux menaces liées à la cybersécurité ?



5 MARQUEURS DE PRÉPARATION À LA CYBER-RÉCUPÉRATION

Le niveau de cybermaturité d'une organisation peut être mesuré par la présence de cinq marqueurs. Les organisations les plus matures et les mieux cyberpréparées présentent quatre ou cinq de ces caractéristiques :

1

Outils de sécurité permettant une alerte précoce en cas de risque, y compris le risque interne.

Les outils de sécurité d'alerte précoce sont des technologies et des systèmes conçus pour détecter les cybermenaces potentielles avant qu'elles ne causent des dommages importants. Ces outils visent à identifier les risques le plus tôt possible, ce qui permet aux organisations de réagir de manière proactive plutôt que réactive. Les exemples incluent les systèmes de détection d'intrusion, la technologie de déception, les systèmes de prévention d'intrusion, la gestion des informations et des événements de sécurité, l'analyse du comportement des utilisateurs et des entités, ainsi que la détection et la réponse des points d'extrémité.

2

Un site sombre connu et propre ou un système secondaire en place.

Maintien d'un environnement de récupération isolé, préconfiguré ou dynamique (par exemple, une salle blanche) qui n'est pas affecté par les cyberincidents survenant sur le site principal. Ce site secondaire peut être rapidement activé pour assurer la continuité des activités et l'intégrité des données en cas de cyberattaque ou de panne majeure. Il améliore la cyber-résilience en fournissant une option de basculement sécurisée, minimisant les temps d'arrêt et la complexité du basculement.

3

Un environnement isolé pour stocker une copie immuable des données.

Il s'agit de conserver une copie séparée et à l'écart du réseau (c'est-à-dire immuable et indélébile) des données sécurisées derrière l'infrastructure d'un tiers. Les données demeurent inchangées et protégées contre les cybermenaces, y compris les ransomwares et les actions internes malveillantes. Il améliore l'intégrité et la disponibilité des données, offrant une option de récupération fiable en cas de corruption ou de perte de données.

4

Définition de runbooks, de rôles et de processus pour la réponse aux incidents.

Une capacité essentielle à la cyber-résilience pour une réponse structurée et efficace face aux cyber-incidents. Des runbooks testés fournissent des instructions étape par étape pour traiter différents types d'incidents, réduisant ainsi la confusion et le temps de réponse. Des rôles et des processus clairement définis garantissent que chaque membre de l'équipe connaît ses responsabilités, ce qui favorise la coordination des efforts. Cette préparation accélère la récupération et aide à maintenir la continuité opérationnelle pendant et après les cyberévénements.

5

Mesures spécifiques visant à montrer l'état de préparation à la cyber-récupération et les risques.

Mesures et tests qui démontrent la capacité d'une organisation à se remettre d'un cyberincident et à évaluer les risques associés. Ces mesures, telles que des exercices de récupération réguliers et des évaluations des risques, permettent d'évaluer l'efficacité des plans de reprise et d'identifier les vulnérabilités potentielles. Elles sont importantes pour la cyber-résilience en particulier, ainsi que pour l'état de préparation, la validation des stratégies de récupération et la mise en évidence des domaines à améliorer.

NE PAS PRENDRE DE RACCOURCIS

Les organisations prêtes pour le cyberespace ne prennent pas de raccourcis lorsqu'il s'agit de cyber-résilience et de préparation.

Pour de nombreuses organisations, la stratégie de cyber-récupération est encore en cours d'élaboration. Là encore, 38 % des personnes interrogées reconnaissent que leurs efforts pourraient être améliorés.

Celles qui souhaitent s'améliorer devraient s'inspirer de leurs homologues plus matures, qui accordent la priorité à un plus grand nombre de pratiques plutôt qu'à quelques-unes seulement et qui, par conséquent, ont une posture plus solide face à une violation.

Elles donnent la priorité aux tests et à la sauvegarde des données critiques, mais accordent une importance presque égale à la capacité de travailler avec plusieurs fournisseurs de services en nuage (cloud), à la compréhension et à l'identification des applications critiques pour l'entreprise et à la mise en place rapide d'un environnement propre (Figure 11).

Il en résulte une posture de sécurité plus forte et une meilleure cyber-résilience. Dans l'ensemble, elles sont environ deux fois moins susceptibles de subir une violation que les entreprises moins matures (Figure 12).

Figure 11

En réponse aux incidents de sécurité, quelles sont les priorités de votre organisation en ce qui concerne sa stratégie de cyber-récupération?

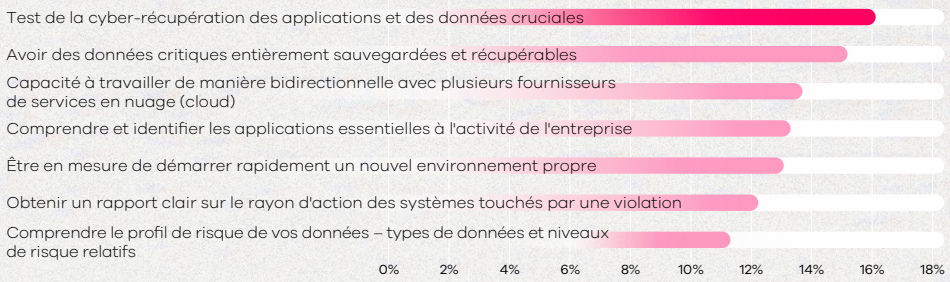
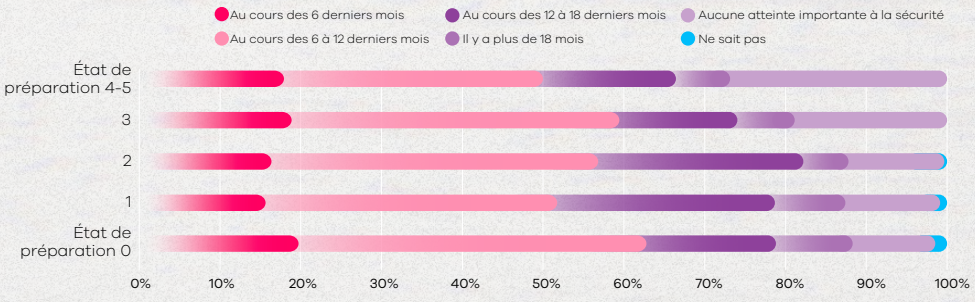


Figure 12

À quand remonte la dernière violation importante de la sécurité de votre organisation ?



LES ORGANISATIONS PRÊTES À AFFRONTER LE CYBERESPACE RÉCUPÈRENT PLUS RAPIDEMENT

Les organisations qui ont le plus de marqueurs de maturité sont prêtes à réagir.

Mieux préparées, les organisations matures sont mieux placées pour récupérer d'une cyberattaque. Sans surprise, ces entreprises sont plus confiantes dans leur capacité à se redresser, 54 % d'entre elles étant tout à fait confiantes (Figure 13).

Cette confiance est justifiée : **Ces organisations matures se rétablissent 41 % plus rapidement que les répondants ayant seulement zéro ou un marqueur, et 24 % plus rapidement que les répondants ayant deux ou trois marqueurs** (Figure 14).

Le fait d'être hors ligne coûte de l'argent et peut nuire à la réputation d'une entreprise et à la confiance des clients, c'est pourquoi chaque minute compte. Plus vite les organisations pourront reprendre leurs activités normales, mieux ce sera.

Figure 13

Dans quelle mesure avez-vous confiance dans le fait que votre organisation puisse récupérer les systèmes et les données critiques à la suite d'un incident majeur?

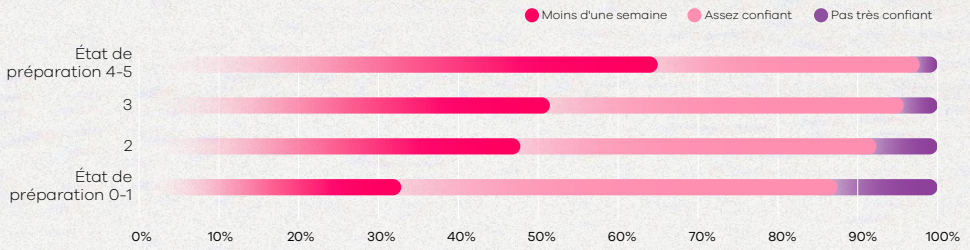
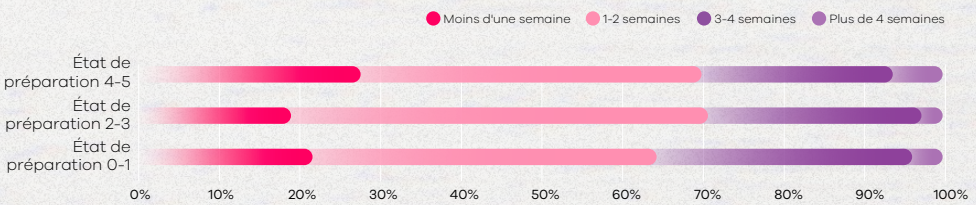


Figure 14

Combien de temps a-t-il fallu à votre organisation pour reprendre ses activités normales après la violation?



LA CYBER-RÉCUPÉRATION VA AU-DELÀ DE LA RÉCUPÉRATION APRÈS SINISTRE

La récupération après sinistre classique ne suffit pas lorsqu'il s'agit de récupérer d'un cyberincident.

Il est important de noter que si certaines entreprises se préparent à la cyber-récupération en tant qu'élément d'un plan global de récupération après sinistre, la **cyber-récupération n'est pas la même chose que la récupération après sinistre**.

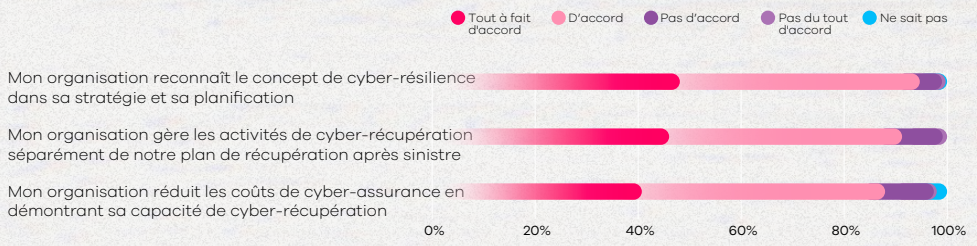
Les plans de récupération après sinistre sont créés en prévision d'événements plus prévisibles tels que les pannes de matériel ou les catastrophes naturelles comme les incendies et les inondations. Bien que ce type d'événement soit certainement dévastateur, les entreprises sont généralement en mesure de se remettre en ligne plus rapidement parce qu'elles suivent les étapes d'un plan prédéfini. Il est important de noter qu'en cas de catastrophe naturelle, les données peuvent être fiables. Ainsi, la récupération après sinistre peut se concentrer sur l'intégrité des données, la rapidité de la reprise et la réalisation des objectifs de reprise établis.

Les cyberévénements sont différents. En cas de cyberattaque, les données ne sont pas fiables. Les plans de récupération doivent donc inclure les éléments importants d'une récupération propre et fiable, afin que la récupération n'aggrave pas la situation. Les plans de récupération des activités informatiques doivent comprendre des mécanismes de récupération avec Confiance Zéro.

Les personnes interrogées reconnaissent cette différence importante. Dans notre enquête, **plus de 90 % des personnes interrogées** déclarent que leur organisation **gère la reprise après sinistre séparément de la cyber-récupération** (Figure 15), ce qui est un signe que la plupart des entreprises reconnaissent les différences et s'y préparent en conséquence.

Figure 15

Dans quelle mesure êtes-vous d'accord ou non avec les affirmations suivantes?



L'ÉTAT DE PRÉPARATION À LA RÉCUPÉRATION NÉCESSITE DES CAPACITÉS, DES COMPÉTENCES ET UNE CULTURE

Les organisations prêtes pour le cyberespace optimisent leur personnel, leurs processus et leur technologie afin d'être prêtes pour la récupération.

Il est important de reconnaître que la **technologie seule ne peut pas améliorer la résilience et la préparation**. Notre recherche valide le paradigme qui a fait ses preuves : la technologie est un outil au service des personnes et des processus.

La plupart des entreprises reconnaissent que la préparation à la cyber-récupération nécessite une approche complète qui justifie
les ressources dont dispose leur entreprise et la manière dont leurs employés les mettent en œuvre.

Capacités : les outils et les systèmes mis en place par une organisation pour se rétablir après une violation.

Compétences : la capacité et l'aptitude d'une organisation à exploiter ses capacités de manière efficace et efficiente.

La culture : les valeurs d'une organisation et sa capacité à les mettre en pratique.

Si les capacités sont les « hard skills » (compétences techniques) d'une entreprise, la culture englobe ses « soft skills » (compétences comportementales). Quelle est la fréquence des tests ? Quelle valeur est accordée à l'investissement dans les deux outils et au temps nécessaire pour les tester ? Dans quelle mesure les employés collaborent-ils et communiquent-ils pour mettre en œuvre un régime de test rigoureux ? Tous ces facteurs influencent le degré de préparation d'une entreprise face aux cybermenaces.

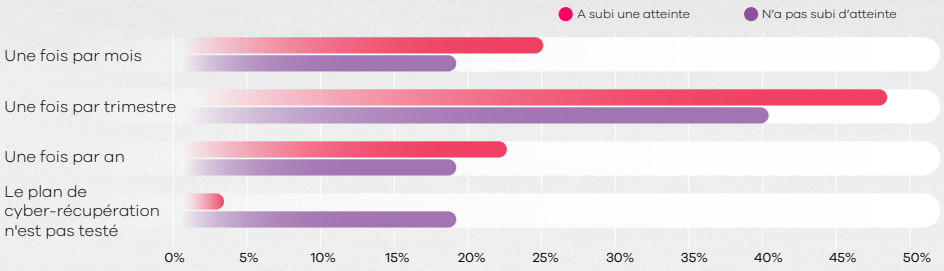
LES TESTS SONT ESSENTIELS À LA RÉSILIENCE ET À LA PRÉPARATION CYBER

Des tests fréquents de récupération après sinistre sont indispensables pour améliorer l'état de préparation.

En l'absence de tests dans un scénario réel, les organisations n'ont aucun moyen de savoir comment leurs plans de récupération des activités informatiques fonctionneront. C'est ce que l'on constate en comparant les stratégies de test des organisations qui ont été victimes d'une violation à celles des organisations qui ne l'ont pas été. Vingt pour cent des organisations qui n'ont pas subi de violation déclarent ne pas tester ***du tout*** leur plan de récupération d'activité (Figure 16). Ce chiffre tombe à seulement 2 % pour les organisations qui ont été victimes d'une violation.

Figure 16

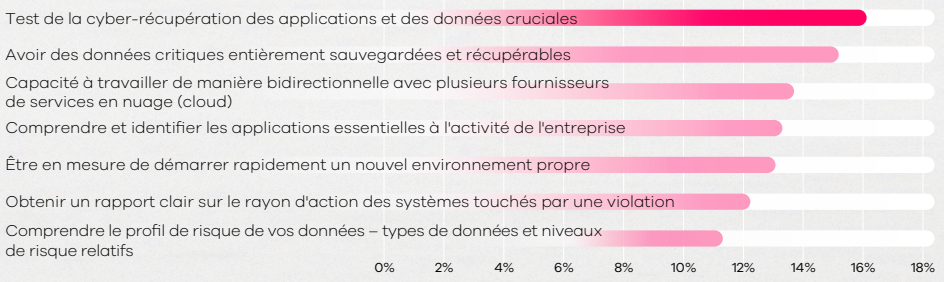
À quelle fréquence le plan de cyber-récupération de votre organisation est-il testé?



En outre, nous avons constaté que les **organisations les plus matures donnent la priorité aux tests** plutôt qu'à d'autres mesures lors de la planification de leur stratégie de cyber-récupération (Figure 17). Soixante-dix pour cent des organisations les plus matures testent leurs plans tous les trimestres, alors que 43 % seulement de celles qui n'ont qu'un ou zéro marqueur de maturité le font (Figure 18).

Figure 17

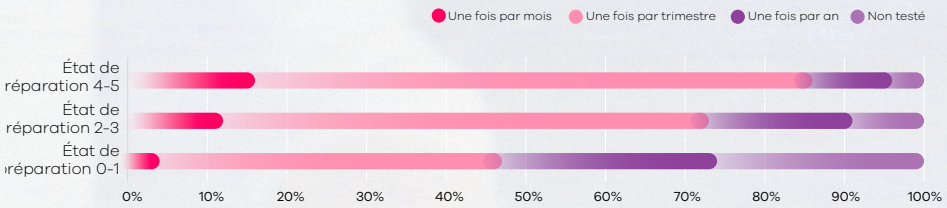
En réponse aux incidents de sécurité, quelles sont les priorités de votre organisation en ce qui concerne sa stratégie de cyber-récupération?



Remarque : Organisations avec 4 ou 5 marqueurs de maturité

Figure 18

À quelle fréquence votre organisation teste-t-elle son plan de cyber-récupération ?



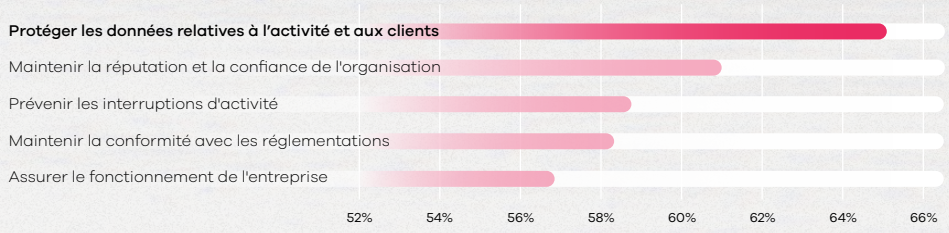
POURQUOI LA PRÉPARATION EST IMPORTANTE – ATTÉNUER L'IMPACT D'UNE VIOLATION

L'état de préparation donne aux organisations la confiance nécessaire pour rester résilientes en cas d'attaque.

Les violations sont non seulement fréquentes, mais elles menacent également les ressources et la marque d'une entreprise. Grâce à l'enquête, nous avons appris que la priorité absolue des organisations en matière de sécurité est la protection et des données relatives à l'activité et aux clients, suivies par le maintien de la réputation et de la confiance en l'organisation (Figure 19).

Figure 19

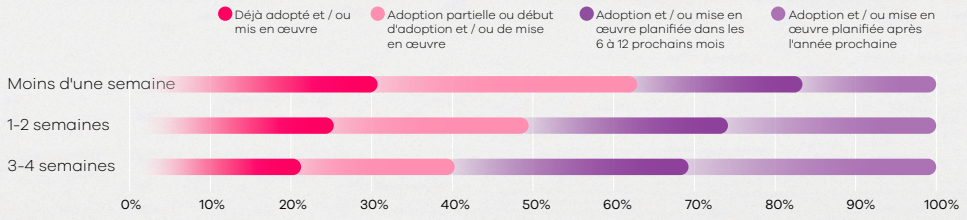
Quelles sont les principales priorités de votre organisation en matière de sécurité, du point de vue de l'entreprise?



Ces attaques ont un impact évident sur le cours normal des affaires. Nous avons constaté que **celles qui avaient déjà adopté totalement ou partiellement un plan de récupération se rétablissent** généralement **41 % plus vite** que celles qui n'ont pas de plan (Figure 20).

Figure 20

Combien de temps a-t-il fallu à votre organisation pour reprendre ses activités normales après la violation?



C'est pourquoi la confiance dans la préparation à la cyber-récupération est de la plus haute importance. Celles qui possèdent le plus grand nombre de marqueurs de maturité sont presque deux fois plus confiantes dans leur posture de cyber-résilience que celles qui n'ont que zéro ou un seul marqueur de maturité (Figure 13, page 11). C'est cette préparation qui permet aux organisations matures de se remettre plus rapidement d'une violation et d'en subir moins dans l'ensemble.

RÉSUMÉ

L'état de préparation à la cyber-récupération

Les résultats de notre enquête montrent clairement qu'il **existe une différence de perspective entre ceux qui ont subi une violation et ceux qui n'en ont pas encore subi**. Mais il est important de se rappeler que les actes sont plus éloquents que les mots. Il ne suffit pas de dire que l'on se comportera différemment. Les organisations devront modifier leurs comportements afin d'améliorer leurs chances de réussir à surmonter une violation et à restaurer leurs systèmes et leurs données.

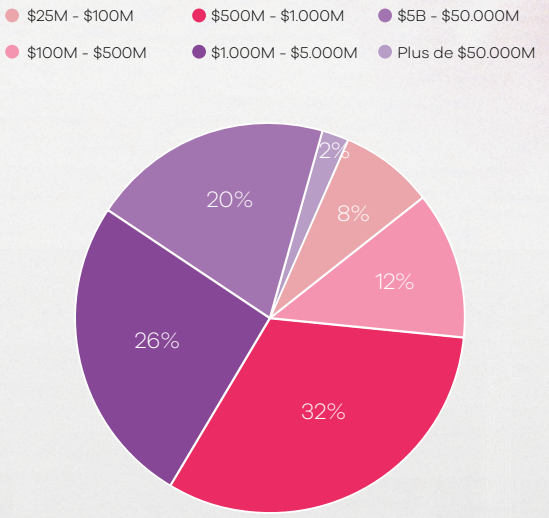
Si vous faites partie des **38 % qui estiment que leurs mesures de cybersécurité pourraient être améliorées** ou si vous faites partie de la majorité de ceux qui n'ont **pas pleinement confiance en leur capacité à se remettre d'une violation**, il y a des mesures que vous pouvez prendre.

En veillant à ce que votre organisation dispose d'un plan pour **atteindre les cinq marqueurs de la cyber-résilience**, vous serez mieux préparés. En investissant dans un programme de tests et en veillant à ce que chacun comprenne son rôle au sein de ce dernier, vous augmenterez vos chances de surmonter une cyberattaque avec succès.

Vous ne pouvez pas vous reposer sur vos lauriers et vous croire à l'abri du danger. **En comprenant et en reconnaissant les risques, vous êtes en mesure de passer outre une violation en gardant vos données – et votre réputation – intactes.**

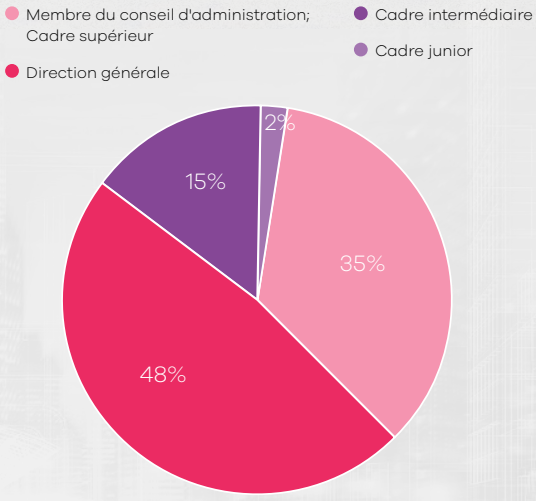
DÉMOGRAPHIE

Figure 1



GigaOm a mené cette étude auprès de 1 000 personnes interrogées à travers 11 pays en avril 2024.

Les personnes interrogées appartenaient à des entreprises qui gagnaient au moins 10 millions de dollars de revenus annuels, la **majorité d'entre elles atteignant 500 millions de dollars ou plus**.



Trente-cinq pour cent des personnes interrogées étaient des membres du conseil d'administration ou des cadres supérieurs, **48 % appartenaient à la direction** et les 17 % restants étaient des cadres intermédiaires ou junior.