COHESITY

Rapport 2023 sur l'état de la sécurité et de la gestion des données

Juillet 2023

En bref

Le deuxième rapport annuel sur l'état de la sécurité et de la gestion des données repose sur une enquête commandée en 2023 par Cohesity, Tenable et BigID, et menée par Censuswide auprès de plus de 3 400 décideurs des domaines de l'informatique et de la sécurité (SecOps) (répartis presque à parts égales entre les deux groupes). Celle-ci a été réalisée auprès d'entreprises basées en Australie, en France, en Allemagne, au Japon, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis en avril 2023.[1]

Face à l'aggravation et à la multiplication des cyberattaques, trois constats s'imposent :

- **La plupart des entreprises n'ont pas les stratégies de cyber-résilience ou les capacités de sécurité des données nécessaires pour faire face aux menaces et assurer la continuité de leurs activités.**
- **Le nombre de personnes interrogées qui pensent que leur entreprise peut récupérer rapidement leurs données après une attaque est moins élevé qu'en 2022.**
- **Il est de plus en plus difficile d'obtenir une cyber-assurance.**

L'augmentation des cyberattaques entretient les inquiétudes à propos des ransomwares

Lorsque nous avons publié notre premier rapport sur l'état de la sécurité et de la gestion des données en 2022, les menaces de ransomwares figuraient en tête des préoccupations. En fait, 74 % des personnes interrogées l'an dernier ont déclaré avoir l'impression que la menace d'attaques par ransomware dans leur secteur d'activité avait augmenté cette année-là.

Nous avons posé la même question dans l'enquête de cette année, et le pourcentage a considérablement augmenté. Pas moins de 93 % des personnes interrogées ont déclaré que la menace d'attaques par ransomware avait augmenté cette année par rapport à la même période l'année dernière.

Et ce ne sont pas seulement les menaces qui inquiètent. Ce sont les attaques réelles. Pour la deuxième année consécutive, près de la moitié des personnes interrogées ont déclaré que leur entreprise avait été victime d'une attaque par ransomware au cours des six derniers mois.

1. Censuwide respecte et emploie des membres de la Market Research Society, qui repose sur les principes ESOMAR.

Vous vous demandez si les ransomwares et autres cyberattaques représentent toujours une menace réelle pour votre entreprise, et pour les entreprises du monde entier ? À en croire cette enquête mondiale, la réponse est oui.

Ont déclaré avoir l'impression que la menace d'attaques par ransomware qui pèse sur leur secteur d'activité s'est accrue en 2023.

Ont déclaré que leur entreprise avait été victime d'une attaque par ransomware au cours des six derniers mois.

Problème 1

La plupart des entreprises n'ont pas de stratégies de cyber-résilience solides ou de capacités de sécurité des données qui leur permettent de faire face aux menaces et d'assurer la continuité de leurs activités.

Les menaces se multiplient, le pourcentage de personnes interrogées qui travaillent dans une entreprise victime d'une attaque récente est élevé, et pourtant le nombre de mesures stratégiques destinées à renforcer la cyber-résilience n'augmente pas. En fait, près de quatre personnes interrogées sur cinq ne sont pas totalement convaincues que leur entreprise possède une stratégie de cyber-résilience conçue pour faire face au nombre croissant de défis et de menaces liés à la cybersécurité.

Et ce n'est pas qu'une question de confiance. Les entreprises ont également besoin de capacités de cyber-résilience et de sécurité des données en place pour pouvoir récupérer leurs données et restaurer leurs opérations rapidement.

Les entreprises citent souvent le cadre de cybersécurité du NIST comme leur cadre de référence en matière de cybersécurité et de cyber-récupération. Le cadre simplifie la hiérarchisation des investissements en fonction des risques et des priorités opérationnelles grâce à ses fonctions d'identification, de protection, de détection, de réponse et de récupération. S'aligner sur les normes présente plusieurs avantages. En effet, ces cadres guident le déploiement de contrôles et de processus appropriés, et créent un point de référence commun qui permet aux entreprises d'harmoniser leur sécurité, leur informatique et leurs activités.

80 % des personnes interrogées se sont dites préoccupées par la stratégie de cyber-résilience de leur entreprise et par sa capacité à faire face aux défis et aux menaces actuels liés à la cybersécurité.

(Cette définition de la cyber-résilience du NIST a été communiquée aux personnes interrogées au début de l'enquête).

« Pour devenir cyber-résilient, il faut commencer par maîtriser les fondamentaux, notamment en ce qui concerne les données. Il est essentiel de savoir où se trouvent vos données sensibles, quelle est leur nature, qui y a accès et quels sont les risques associés. Notre communauté de la sécurité doit placer ses données au cœur de sa stratégie de sécurité. »

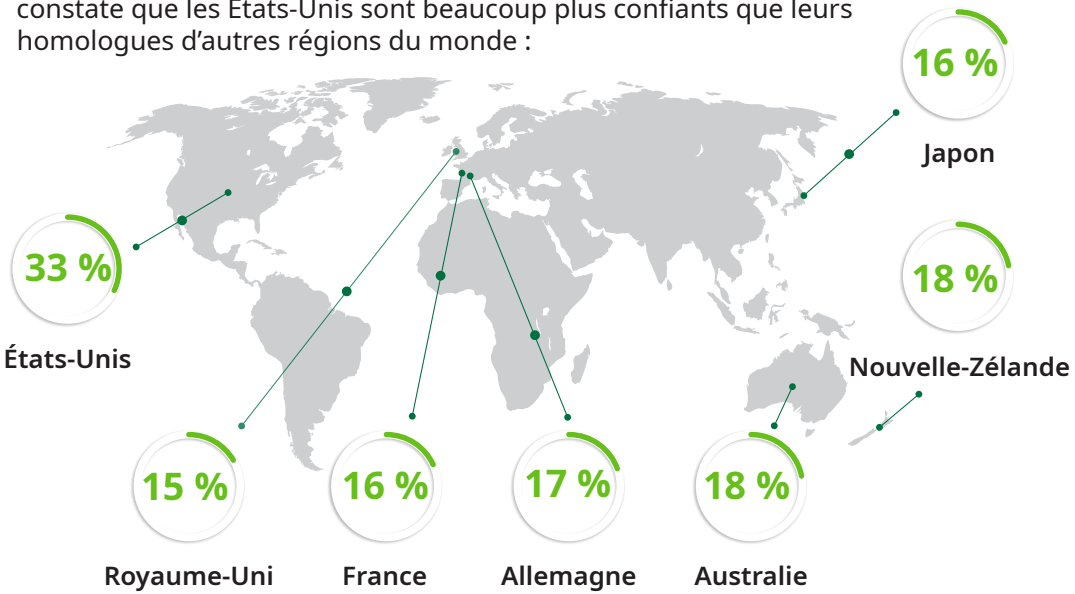
TYLER YOUNG, RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, BIGID

Problème 2

Les personnes interrogées craignent que leur entreprise ne puisse pas récupérer après une attaque.

À la question portant sur la menace des ransomwares, 40 % des personnes interrogées l'an dernier ont répondu que « l'impossibilité de récupérer les données » les inquiétait, même si elles étaient sauvegardées. Cette année, 67 % des personnes interrogées ne sont pas totalement convaincues que leur entreprise pourrait récupérer ses données et ses principaux processus métier en cas de cyberattaque à l'échelle du système.

Au niveau mondial, sur le faible pourcentage (21 %) de personnes ayant répondu qu'elles étaient « absolument certaines » de pouvoir restaurer leurs données après une cyberattaque sans risquer d'être réinfectées par des logiciels malveillants, on constate que les États-Unis sont beaucoup plus confiants que leurs homologues d'autres régions du monde :



Quels sont les obstacles à la reprise de l'activité ? L'enquête révèle que les trois principaux défis à relever sont les suivants :

34 % Absence d'intégration entre les systèmes informatiques et de sécurité

Absence de coordination entre les professionnels de l'informatique et de la sécurité **33 %**

32 % Systèmes de sauvegarde et de récupération obsolètes

...et lorsque la récupération est possible, elle n'est pas nécessairement rapide.

Une récupération lente introduit de l'incertitude et nuit à l'activité. Elle soulève également de nombreuses questions.

Quand vos machines virtuelles, vos bases de données et vos données NAS seront-elles à nouveau en ligne et accessibles ? Seront-elles propres, ou les récupérer réintroduira des logiciels malveillants et réinfectera vos systèmes ? Pouvez-vous récupérer des données stratégiques à grande échelle à n'importe quel point dans le temps et à n'importe quel emplacement ? Si oui, quand ? Si non, que se passe-t-il alors ?

À la question de savoir combien de temps, en moyenne, leur entreprise mettrait à restaurer ses données et ses processus métier en cas de cyberattaque :

Ont répondu plus de 24 heures

Ont répondu plus de 4 jours

Ont répondu plus d'une semaine

Et en cas d'attaque par ransomware, chaque minute compte. Le risque d'impacts graves, et souvent immédiats, en aval est d'autant plus grand que l'entreprise reste longtemps à l'arrêt sans pouvoir accéder à ses données.

« Les entreprises ne peuvent pas se permettre d'être déconnectées et incapables d'assurer leurs opérations, en particulier pendant plus d'une journée. Pourtant, force est de constater que nombre d'entre elles sont vulnérables face aux cybercriminels parce qu'elles sont incapables de récupérer rapidement leurs données et leurs processus métier le cas échéant. »

BRIAN SPANSWICK, RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION ET DIRECTEUR INFORMATIQUE, COHESITY

Lorsque 95 % des entreprises ne peuvent pas récupérer leurs données et leurs processus métier dans les 24 heures, elles sont non seulement vulnérables, mais aussi plus enclines à faire des choix susceptibles de favoriser de futures attaques de l'industrie. Par exemple, payer une rançon.

La plupart envisagerait de payer une rançon

Payer une rançon est généralement la dernière chose à faire. Pourtant, 90 % des personnes interrogées dans le monde pensent que leur entreprise envisagerait (certaines sans équivoque, d'autres en fonction du coût) d'en payer une si cela leur permettait de récupérer leurs données et leurs processus métier, ou de les récupérer plus rapidement. Parmi les pays les plus susceptibles de choisir cette option, citons :

- **L'Australie et la Nouvelle Zélande (95 %)**
- **Les États-Unis (94 %)**
- **La France (93 %)**
- **Le Royaume-Uni (91 %)**

L'Allemagne **(87 %)** et le Japon **(78 %)** sont encore susceptibles d'envisager de payer, mais moins dans l'ensemble.

Bien entendu, quand on traite avec des cybercriminels, on ne traite pas avec des acteurs de bonne foi. Souvenez-vous que payer une rançon ne garantit pas que vous récupérerez vos données, ni qu'elles seront propres et exemptes de logiciels malveillants si vous les récupérez.

Problème 3

Il est de plus en plus difficile d'obtenir une cyber-assurance.

Le coût de la cybercriminalité dans le monde est estimé à 8 000 milliards d'euros par an (10 500 milliards d'euros d'ici 2025). De plus en plus d'entreprises tentent donc de sécuriser une protection financière contre les pertes liées aux cyberattaques, aux violations de données et à d'autres incidents de cybersécurité. Une des stratégies de protection consiste à souscrire une cyber-assurance.

Cette année, 74 % des personnes interrogées ont déclaré que leur entreprise possédait actuellement une cyber-assurance. (Au Japon, ce chiffre s'élève seulement à 61 %.) Il n'est toutefois pas facile de sécuriser une stratégie. Selon presque la moitié (46 %) des personnes interrogées, cela devient même de plus en plus difficile. Ceux-ci déclarent en effet qu'il est plus difficile d'obtenir une cyber-assurance aujourd'hui qu'il y a trois ans.

Les personnes interrogées ont dressé une longue liste de technologies et de capacités considérées comme essentielles pour les entreprises qui tentent de sécuriser leur cyber-assurance. Elle comprend :

- 40 % — Chiffrement solide
- 38 % — Capacité à vérifier l'intégrité de la sauvegarde
- 37 % — Authentification multifacteur (MFA)
- 34 % — Détection d'anomalies
- 33 % — Isolation des données / air-gapping
- 29 % — Immuabilité

Garantir des capacités critiques peut non seulement permettre de sécuriser des stratégies de cyber-assurance difficiles à obtenir, mais aussi de faire baisser les primes.

La cyber-assurance vient enrichir une approche multicouche de la sécurité destinée à lutter contre les ransomwares, et plus largement contre les cyberattaques.

Les problèmes sont nombreux. Mais les solutions aussi.

Il *est* possible de renforcer la cyber-résilience.

La gravité des problèmes abordés dans ce rapport n'empêche pas les entreprises de renforcer leur cyber-résilience pour lutter contre des menaces de plus en plus nombreuses, qu'il s'agisse de ransomwares et d'autres cyber-incidents (comme évoqué dans ce document), ou de catastrophes telles que des tremblements de terre, des inondations, des défaillances système ou des erreurs humaines.

Il existe deux moyens concrets de favoriser la cyber-résilience : renforcer la collaboration et approfondir ses connaissances.

Renforcer la collaboration

87 % des personnes interrogées pensent que les fournisseurs de données et de cybersécurité doivent collaborer pour proposer des solutions anti-ransomware complètes et intégrées.[2] Les entreprises tirent profit des efforts communs déployés par les fournisseurs pour vaincre les ransomwares et créer des solutions intégrées qui soutiennent les efforts de récupération propre. Renforcer la cyber-résilience bénéficie aux entreprises, à leurs clients et à leur secteur d'activité. Les États-nations commettent de plus en plus de cybercrimes. Déjouer ces attaques et renforcer la résilience est donc également bénéfique pour le monde entier.

Approfondir ses connaissances

Au-delà des avantages d'une collaboration entre fournisseurs, 90 % des personnes interrogées estiment que leur entreprise tirerait profit d'une plateforme de sécurité et de gestion des données qui fournit des informations sur leur posture de sécurité globale et leur cyber-résilience. Ces connaissances permettent aux entreprises de réduire le risque de perturbations opérationnelles et d'améliorer leur capacité à résister aux cyberattaques. Ces informations permettent en outre d'accélérer et de faciliter les audits de conformité aux réglementations relatives à l'industrie et à la confidentialité.

2. Ces statistiques combinent les résultats des personnes interrogées ayant sélectionné « Extrêmement important » ou « Assez important ».

« Dans un paysage de cybermenaces aussi sophistiqué que celui d'aujourd'hui, s'appuyer sur des systèmes de sauvegarde et de récupération traditionnels, dépourvus de capacités modernes de sécurité des données, c'est courir au désastre. Les entreprises devraient plutôt chercher des plateformes de sécurité et de gestion des données qui s'intègrent à leurs solutions de cybersécurité existantes, qui offrent une visibilité sur leur posture de sécurité et qui améliorent leur cyber-résilience. »

BRIAN SPANSWICK, RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION ET DIRECTEUR INFORMATIQUE, COHESITY

« La seule façon de devenir cyber-résilient est de privilégier des mesures de sécurité proactives qui permettront avant tout d'éviter les cyber-attaques. Cette approche devrait également s'étendre aux mesures de sauvegarde et de récupération pour assurer la continuité des activités en cas d'incident de cybersécurité. Les entreprises doivent donc non seulement gérer leur cyber-risque, mais aussi mieux comprendre leur exposition au risque en exploitant les données relatives aux vulnérabilités et à l'exposition pour prendre des décisions éclairées sur leurs efforts de correction. »

RAY KOMAR, VICE-PRÉSIDENT DE LA TECHNOLOGIE ET DES ALLIANCES CLOUD, TENABLE

Conclusion

Lorsqu'une entreprise est victime d'un ransomware et que ses données sont volées, effacées, infectées ou compromises, elle ne peut pas fonctionner correctement tant que ses données, processus, opérations et applications n'ont pas été restaurés. Il est essentiel pour la résilience de l'entreprise de s'assurer que cette récupération est propre et rapide.

Face à cette réalité, la meilleure défense contre des menaces mondiales persistantes consiste à adopter une approche globale de la sécurité et de la gestion des données.

Voilà ce que révèle l'enquête mondiale de cette année :

1. **La plupart des entreprises n'ont toujours pas les stratégies de cyber-résilience ou les capacités de sécurité des données nécessaires pour faire face à ces menaces et assurer la continuité de leurs activités.**
2. **Les professionnels de l'informatique et des SecOps sont moins nombreux à penser que leur propre entreprise peut récupérer efficacement (et rapidement) après une cyberattaque.**
3. **Bien que la cyber-assurance soit en plein essor, elle est plus difficile à obtenir et la liste des technologies et des capacités essentielles nécessaires pour y prétendre est longue.**

En fin de compte, les entreprises qui travaillent avec des fournisseurs qui collaborent, s'associent et intègrent leurs solutions de cybersécurité, de gestion et de sécurité des données, pourront mieux résister aux cyber-incidents, récupérer en cas de besoin, et réduire leurs risques opérationnels globaux. De plus, les entreprises dotées de plateformes de sécurité et de gestion des données capables de leur fournir des informations sur leur posture de sécurité globale sauront mieux résister aux menaces et récupérer sereinement.

Les entreprises d'aujourd'hui ne peuvent pas se permettre de ne pas être préparées.

COHESITY