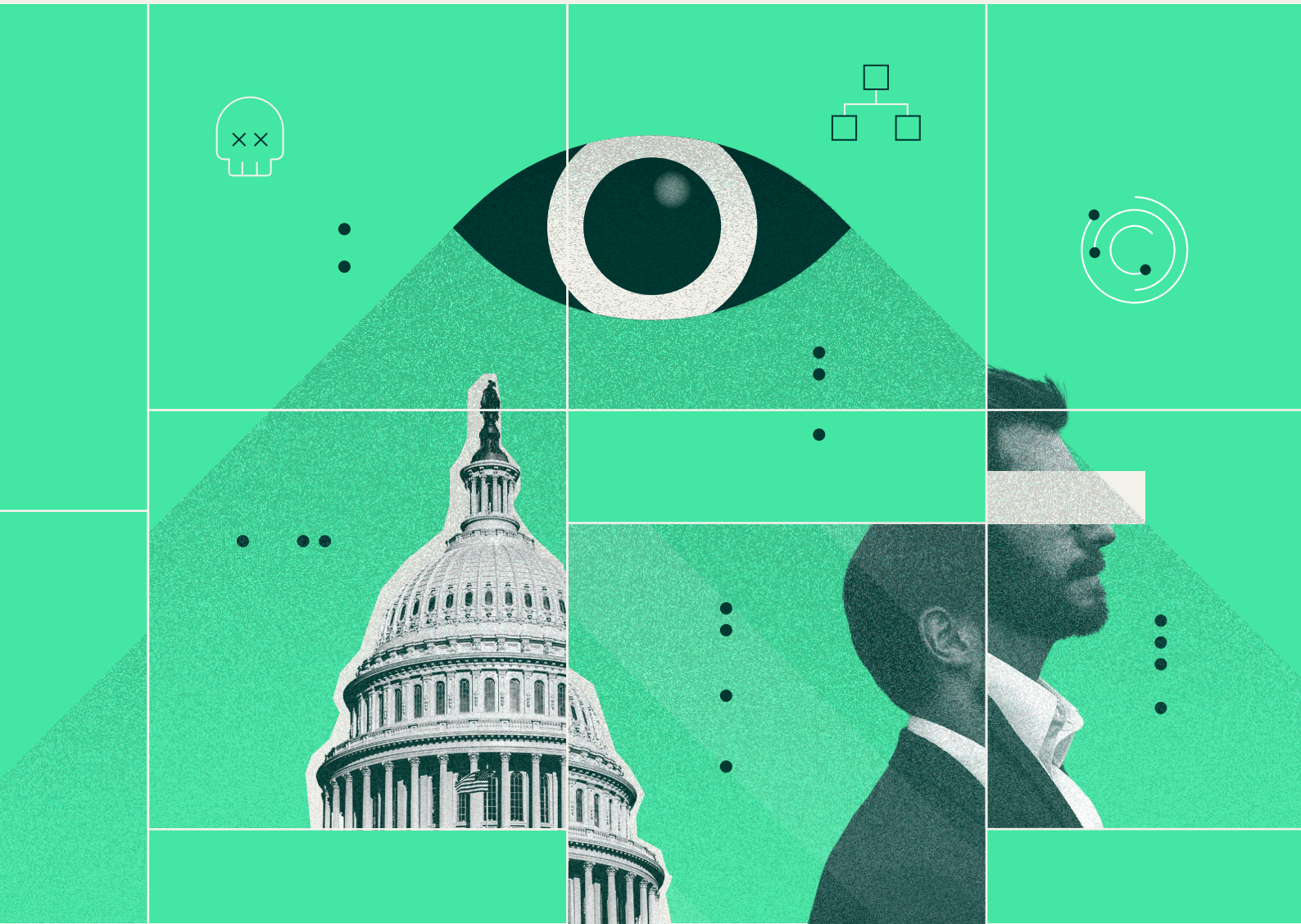
Rubrik Zero Labs

LIVRE BLANC

Point sur la sécurité des données

L'impact humain de la cybercriminalité



Sommaire

Introduction p3

Répartition des personnes interrogées p5

1.0 Contexte p6

1.1 Le nombre de cyberattaques et leurs conséquences continuent d'augmenter
1.2 Les organisations se sentent impuissantes face aux attaques
1.3 Les menaces connues restent le principal problème

2.0 Réalité p10

2.1 Les responsables informatiques et de la cybersécurité recherchent toujours des ressources pour sécuriser leurs données
2.2 La cybercriminalité fait des ravages
2.3 Les dirigeants peinent à mettre en œuvre les stratégies de sécurité

3.0 Solution p14

3.1 Quelles sont les prochaines étapes pour les responsables informatiques et de la cybersécurité ?
3.2 Bonnes pratiques

Résumé p19

Ce rapport aborde le sujet des données et les risques encourus lorsqu'elles sont menacées. Il s'intéresse également aux personnes : celles qui ont besoin des données pour leur travail, les criminels qui les menaces et les équipes qui les protègent.

Dans le cadre de ce premier rapport commandité par Rubrik et mené par Wakefield Research, Rubrik Zero Labs a également étudié l'impact humain de la sécurisation des données du point de vue des spécialistes.

Rubrik Zero Labs a pour mission de fournir des informations exploitables et indépendantes des fournisseurs afin de réduire les risques liés à la sécurité des données. Nous améliorons les résultats en matière de sécurité des données Zero Trust en nous appuyant sur l'évaluation des cybermenaces dans le monde réel et sur les bonnes pratiques en matière de cyber-résilience. Notre travail repose sur trois principes fondamentaux :

1

Exploiter les constats négatifs sur le plan opérationnel
Élaboration de décisions proactives et exploitables à partir d'observations et d'analyses de tendances fondées sur des données.

2

Réduire les risques
Réduction et limitation des options de menace par la recherche, la sensibilisation du public, les partenariats et les changements techniques apportés aux technologies ou aux techniques et méthodes de base en matière de sécurité des données.

3

Améliorer les conditions de notre communauté
Intervention en tant que conseiller de confiance dans le domaine de la sécurité des données, via des recherches approfondies sur des sujets liés à la sécurité, des modèles et des publications externes.

« Écoutez d'abord, parlez ensuite. »

Peter Drucker, pionnier du management moderne, a dit : « Écoutez d'abord, parlez ensuite. » Dans cet esprit, nous voulions inaugurer Rubrik Zero Labs en écoutant les personnes chargées de la protection contre les menaces et de la gestion de la cybercriminalité au quotidien.

Afin d'obtenir une vision complète et impartiale, nous avons interrogé des personnes extérieures à notre clientèle. Pour cela, nous avons demandé à plus de 1 600 responsables informatiques et de la cybersécurité (dont la moitié sont des DSI et RSSI), dans 10 pays, de nous donner leur avis sur l'état de la sécurité des données. Nous avons ensuite partagé nos découvertes à un panel d'éminents spécialistes du domaine pour obtenir leurs conseils afin d'aider les organisations à mieux sécuriser leurs données. Informations sur l'étude :

+ de 1 600
responsables informatiques et de la cybersécurité

819
DSI et RSSI

10
pays dans le monde

Répartition des personnes interrogées

L'enquête mondiale a été commanditée par Rubrik et menée par Wakefield Research auprès de 1 625 décideurs du secteur de l'informatique et de la sécurité (directeurs, vice-présidents, DSI et RSSI), dans des entreprises de 500 employés ou plus. L'étude a été réalisée aux États-Unis, au Royaume-Uni, en France, en Allemagne, en Italie, aux Pays-Bas, au Japon, en Australie, à Singapour et en Inde entre le 18 et le 27 juillet 2022.

Poste	241 Vice-président	565 Directeur	408 RSSI	411 DSI
Région	500 USA	625 EMEA	500 APAC	
Taille de l'entreprise	366 + de 2 500	505 1 000-2 499	754 500-999	

1.0 Contexte

1.1 Le nombre de cyberattaques et leurs conséquences continuent d'augmenter

1.2 Les organisations se sentent impuissantes face aux attaques

1.3 Les menaces connues restent le principal problème

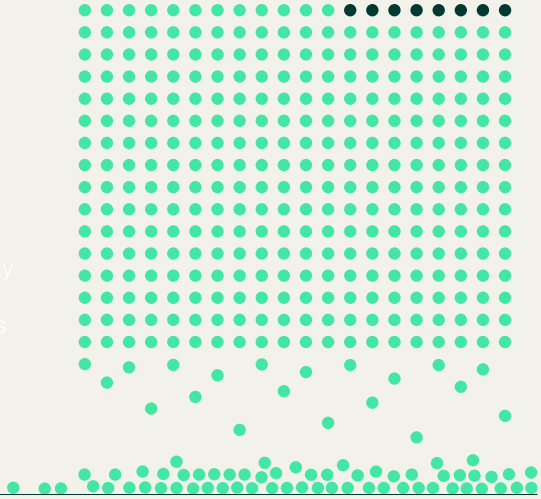
1.1

Le nombre de cyberattaques et leurs conséquences continuent d'augmenter

Malgré des décennies d'efforts et d'investissements dans la cybersécurité, les cybermenaces ne faiblissent pas. En fait, la situation s'aggrave.

98 %

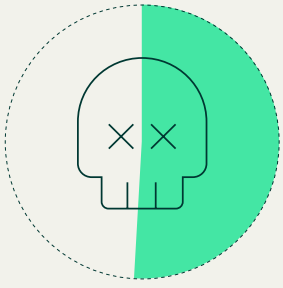
des responsables informatiques et de la cybersécurité ont identifié au moins une cyberattaque au cours de l'année dernière.



En moyenne, ils déclarent avoir eu connaissance de 47 cyberattaques sur l'année.

52 %

ont été confrontés à une violation des données.



51 %

ont eu affaire à un ransomware sur la même période.

> Les intrusions ne relèvent plus seulement de la compétence de petites équipes internes. Les hauts dirigeants, les organisations entières et le grand public sont désormais conscients de ces événements et en subissent les conséquences.

1.2

Les organisations se sentent impuissantes face aux attaques

Face à l'élargissement du périmètre des attaques, à la sophistication des cybercriminels et à la médiatisation des attaques, les responsables informatiques et de la cybersécurité ainsi que les équipes de direction semblent douter de leur capacité à combattre les menaces.

---

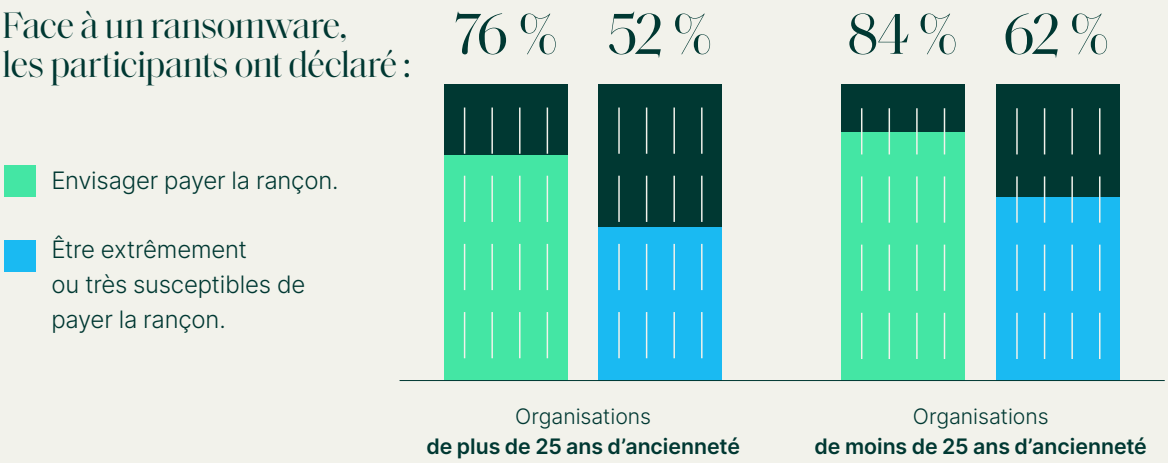
33 %

des responsables informatiques et de la cybersécurité estiment que leur conseil d'administration et leur direction n'ont que peu ou pas confiance dans la capacité de récupérer les données et les applications métier essentielles en cas de cyberattaque.

92 %

craignent de ne pas pouvoir assurer la continuité des activités s'ils subissent une cyberattaque.

Face à un ransomware, les participants ont déclaré :



Quel est le degré de confiance de votre conseil d'administration/direction dans la capacité de l'organisation à restaurer les données critiques et les applications métier dans l'éventualité d'une cyberattaque ?

27 %

Confiance totale

40 %

Confiance générale, mais surveillance occasionnelle

33 %

Confiance faible ou nulle

1.3 Les menaces connues restent le principal problème

Même si les attaques 0-day font l'objet d'une attention particulière de la part du secteur de la cybersécurité, seul un tiers des participants a déclaré avoir subi une attaque de ce type au cours de l'année dernière et ils sont peu nombreux à les considérer comme leur principale menace pour l'année à venir.

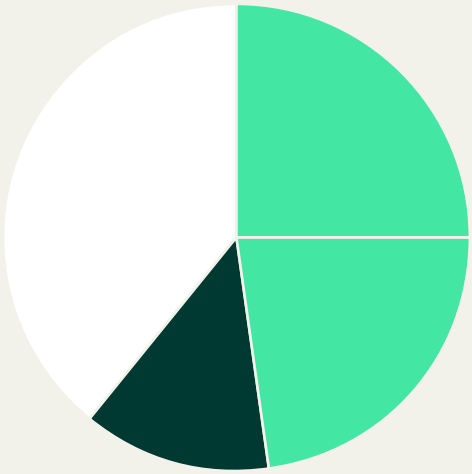
Seulement **39 %**

des cyberattaques relevant de la compétence des responsables informatiques et de la cybersécurité étaient de type 0-day l'année dernière, ce qui signifie que près de deux tiers des événements s'appuyaient sur des vulnérabilités bien connues.

11 %

des responsables informatiques et de la cybersécurité ont déclaré ne pas avoir remédié correctement aux vulnérabilités identifiées lors d'événements antérieurs.

48 % des responsables informatiques et de la cybersécurité considèrent que la principale menace l'an prochain sera :



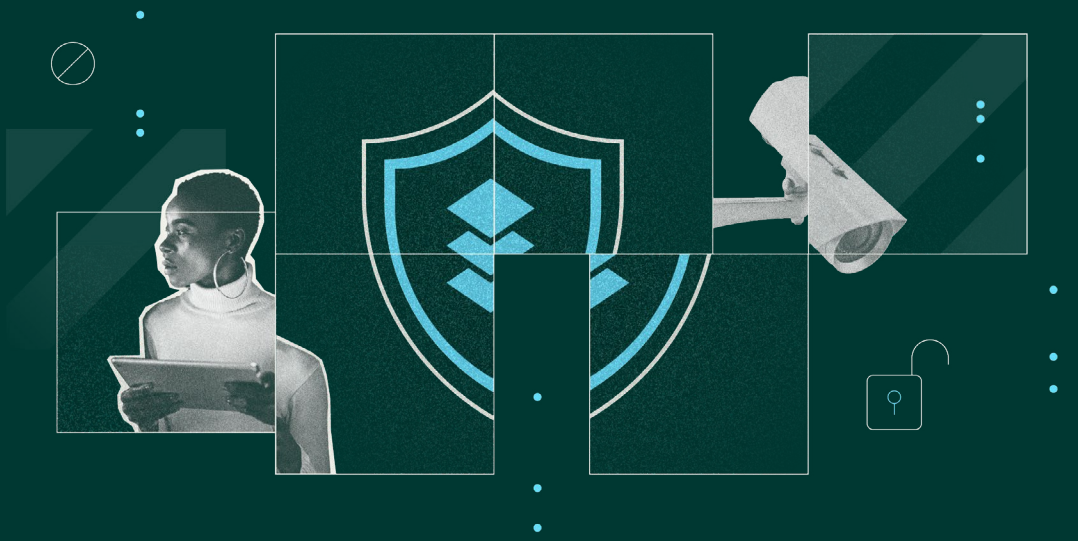
25 %
Violations de données

23 %
Attaques de ransomware

contre seulement **13 %**
Attaques 0-day

> L'augmentation du nombre et de l'importance des cyberattaques, les menaces émergentes et les difficultés à résoudre les problèmes connus augmentent considérablement la sollicitation des équipes IT et cybersécurité.

2.0 Réalité



2.1
Les responsables informatiques et de la cybersécurité recherchent toujours des ressources pour sécuriser leurs données

2.2
La cybercriminalité fait des ravages

2.3
Les dirigeants peinent à mettre en œuvre les stratégies de sécurité

2.1

Les responsables informatiques et de la cybersécurité recherchent toujours des ressources pour sécuriser leurs données

Depuis des années, le secteur de la cybersécurité connaît une pénurie de talents criante. Le nombre de postes à pourvoir dans le domaine de la cybersécurité a augmenté de 350 %, passant d'un million d'offres en 2013 à 3,5 millions en 2021, selon Cybersecurity Ventures. Sans surprise, les personnes interrogées dans le cadre de l'enquête Rubrik Zero Labs ont placé le recrutement de talents en tête des défis à relever pour protéger leur organisation, devant les outils, le budget et le soutien des dirigeants ou du conseil d'administration.

Quels sont les cinq principaux défis à relever pour protéger votre organisation des cyberattaques ?

1

Manque de talents au sein des équipes informatiques ou SecOps

2

Manque d'outils et de solutions de cybersécurité

3

Budget insuffisant pour assurer la sécurité des données

4

Les dirigeants/le conseil d'administration ne donnent pas la priorité à la sécurité des données

5

Les différentes équipes ne parviennent pas à se mettre d'accord sur la manière de protéger l'organisation des cyberattaques

Historiquement,

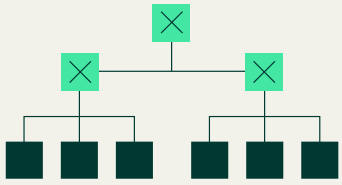
les pénuries de ressources sont plus accentuées dans les petites organisations. Les petites entités ont la charge supplémentaire de combattre les mêmes menaces, mais avec moins de personnel et des budgets limités.

2.2 La cybercriminalité fait des ravages

Des années de pression croissante combinées et un manque de ressources semblent avoir fait des ravages non seulement auprès des responsables informatiques et de la cybersécurité et de leurs équipes, mais aussi dans l'ensemble des organisations.

---

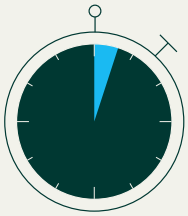
96 %



des responsables informatiques et de la cybersécurité ont fait état d'un impact émotionnel ou psychologique important, allant des inquiétudes au sujet de la sécurité de l'emploi à la perte de confiance de leurs collègues ou de leur organisation envers eux.

36 %

des organisations de l'étude ont changé de direction au cours de l'année écoulée en raison d'une cyberattaque et de la réponse apportée.



Seulement 5 %

des organisations ont pu assurer la continuité des activités ou reprendre un fonctionnement normal dans l'heure qui a suivi la découverte d'une cyberattaque.

96 % des organisations participantes ont subi des conséquences négatives suite à une cyberattaque survenue l'année dernière. Quelles sont les conséquences subies par votre organisation suite à une cyberattaque ?

42 %	41 %	40 %	36 %	5 %
Mauvaise presse et/ou atteinte à la réputation	Perte de clients	Perte de revenus	Changement forcé de direction	Impact négatif sur les actions

> L'épuisement des ressources humaines, la complexité croissante et la diversité des menaces exercent une pression considérable sur les opérations et sur un vivier de talents très demandé, mais peu dense. De plus en plus d'intrusions étant rendues publiques, les répercussions négatives d'une seule violation se font sentir à l'échelle de toute l'organisation.

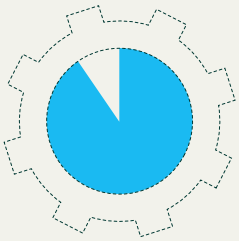
2.3 Les dirigeants peinent à mettre en œuvre les stratégies de sécurité

Les responsables informatiques et de la cybersécurité ont souligné l'importance de mieux aligner les équipes informatiques et SecOps afin de réagir efficacement aux événements et d'apporter des améliorations proactives. Les leaders du secteur ont également souhaité des partenariats entre le public et le privé pour aider à résoudre les problèmes de cybersécurité dans le monde. Mais les données de Rubrik Zero Labs montrent qu'il est plus difficile de faire aboutir ces propositions dans la pratique.

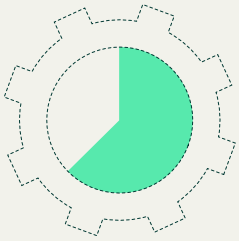
---

31 % des dirigeants interrogés ont déclaré que leurs équipes informatiques et SecOps éprouvaient des difficultés à s'accorder, ou n'y parvenaient pas du tout, lorsqu'il s'agissait de défendre leur organisation.

Les participants pensent que les partenariats entre les secteurs public et privé sont

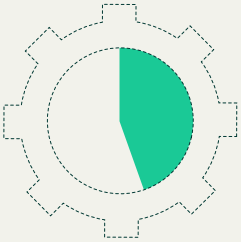


89 %
Bénéfiques



64 %
Extrêmement bénéfiques

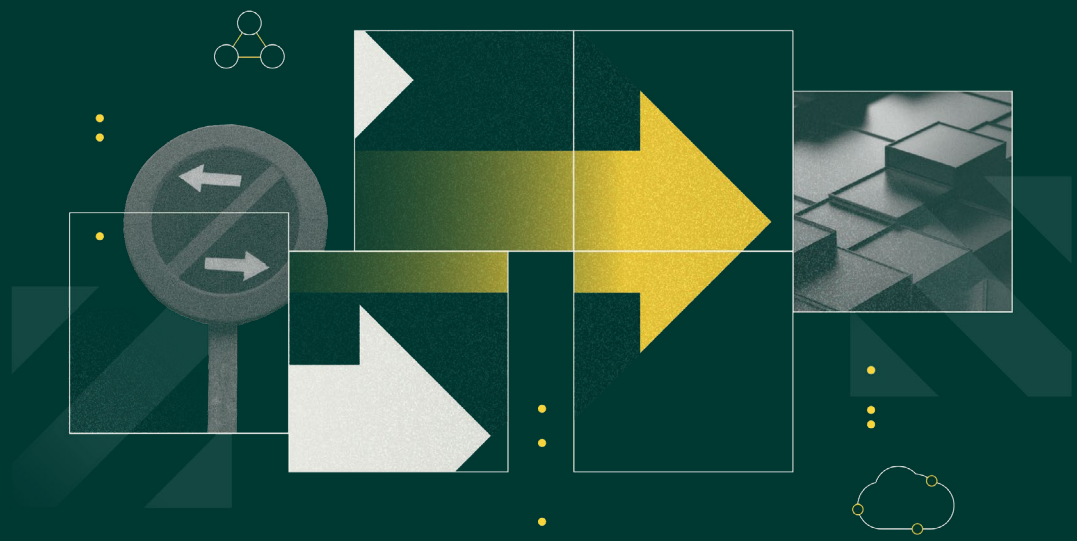
Cependant, moins de la moitié ont déclaré participer à des partenariats entre le secteur privé et le secteur public en faveur de la cybersécurité.



44 %
impliqués dans des partenariats entre secteur privé et secteur public

> En dépit d'efforts et d'investissements importants, les organisations peinent à mettre les choses en pratique. Les changements fondamentaux au niveau de l'architecture et des processus sont les plus rentables, mais souvent difficiles à réaliser.

3.0 Solution



3.1 Quelles sont les prochaines étapes pour les responsables informatiques et de la cybersécurité ?

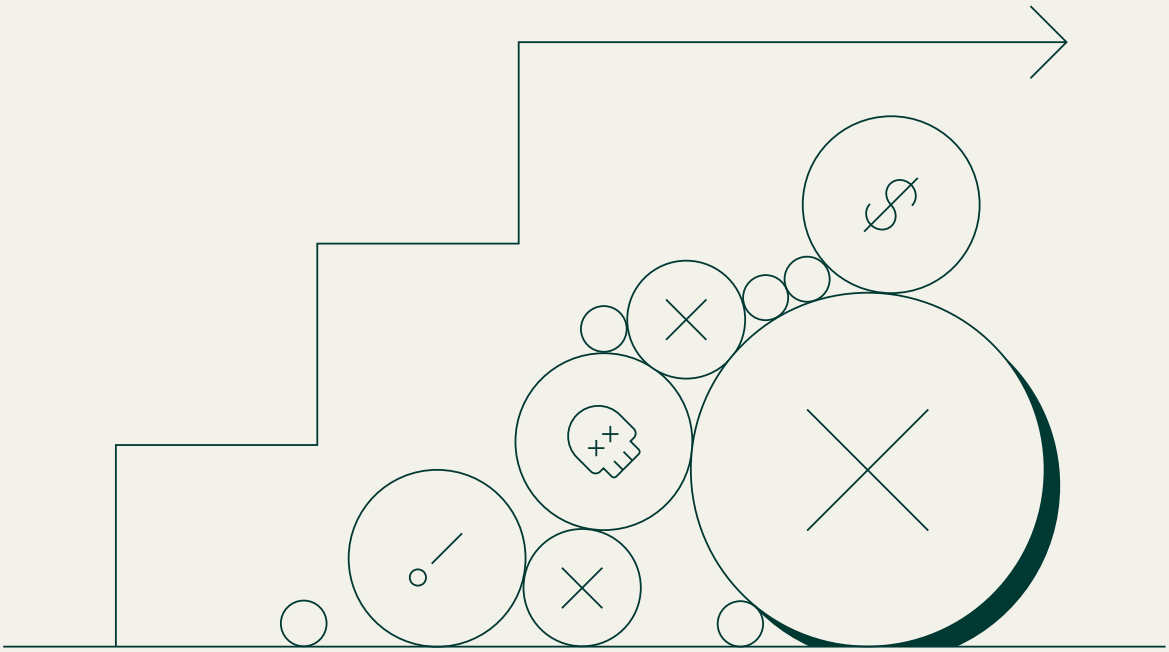
3.2 Bonnes pratiques

3.1 Quelles sont les prochaines étapes pour les responsables informatiques et de la cybersécurité ?

L'étude menée par Rubrik Zero Labs montre que les responsables informatiques et de la cybersécurité continuent de se heurter à une liste croissante de défis lorsqu'il s'agit de protéger les données de leur entreprise contre les cyberattaques.

Que peuvent-ils faire pour surmonter les difficultés ?

Des pionniers et grands noms de la cybersécurité ont formulé des recommandations d'experts pour les aider à faire face à ces réalités décourageantes. Ils ont confirmé la gravité de la situation et proposé trois bonnes pratiques que les organisations peuvent mettre en œuvre pour se protéger et protéger leurs données.



3.2 Bonnes pratiques

1 Les mesures de lutte contre la violation des données doivent résister aux intrusions *hebdomadaires*

Les participants ont déclaré en moyenne avoir été informé de 47 cyberattaques contre leur organisation au cours de l'année passée. Cela représente près d'une attaque par semaine. Comme il est peu probable que cette fréquence ralentisse, ils doivent disposer d'une capacité hebdomadaire pour faire face à ces événements. Après chaque incident, les organisations doivent rapidement mettre à jour leurs plans de préparation et de gestion de crise afin d'améliorer leur cyber-résilience à long terme. Ces améliorations permettront aux équipes d'être mieux armées pour rétablir les opérations plus rapidement, en toute confiance, et réduire l'impact de chaque violation ultérieure.

La création d'un processus collaboratif, où chaque tentative de violation permet de mieux anticiper et contrer la suivante, nécessitera l'implication d'autres personnes que les équipes informatiques et de sécurité. Les équipes juridiques, RH et communication, pour n'en citer que quelques-unes, devront consacrer du temps et des efforts à ce type de collaboration pour qu'elle fonctionne.

> « La question n'est plus de savoir si, mais quand votre organisation sera victime d'une cyberattaque. La préparation peut être votre arme secrète. Les dirigeants doivent non seulement élaborer une stratégie de remédiation, mais également la mettre en pratique afin de disposer de l'équipe, des solutions et des processus adaptés pour restaurer rapidement les activités en cas d'attaque. »
>
> **John W. Thompson**
> Ancien président du conseil d'administration de Microsoft et PDG de Symantec

> « Pour répondre à une cyberattaque, les équipes chargées de l'informatique et de la sécurité doivent collaborer avec les responsables de tous les départements. La préparation exige non seulement une bonne collaboration, mais aussi une formation et une pratique constantes. Il est essentiel de vous assurer que vous disposez d'un plan de sécurité et de restauration des données bien pensé pour garantir la résilience de l'entreprise et la continuité effective des opérations. »
>
> **Michael Mestrovich**
> Responsable de la sécurité informatique chez Rubrik, ancien RSSI de la CIA

3.2 Bonnes pratiques

2 Les responsables doivent *exiger davantage* de leurs données

Lors d'une cyberattaque, les données sont souvent considérées comme des victimes passives. Toutefois, en ayant recours aux technologies d'observabilité, les organisations peuvent utiliser les ressources de données pour réduire les cyber-risques et accélérer les délais de réponse aux incidents.

Les responsables informatiques et de la cybersécurité devraient se poser les questions de base suivantes :

- Quelle quantité de données mon organisation crée-t-elle et gère-t-elle ?
- Quelles données sont sensibles ou contiennent des informations personnelles identifiables ?
- Où se trouvent ces données ?
- Qui peut y accéder ?
- Quelles données ont le plus d'impact sur les activités ?
- Mon organisation dispose-t-elle des technologies et des processus adéquats pour mettre en œuvre des politiques basées sur le volume, l'importance, la sensibilité et l'accès des données ?
- Quels systèmes de support sont essentiels pour maintenir l'accès à ces données et dans quel ordre fonctionnent-ils ?
- À quelle vitesse pouvez-vous trouver des réponses à vos questions sur les données ?

Il peut être difficile de répondre à ces questions, car les employés restent à distance et les organisations continuent d'évoluer vers des environnements hybrides. Néanmoins, elles aideront également les organisations à contrer les intrusions et à améliorer la résilience dans diverses situations, notamment face aux catastrophes, aux menaces internes et aux fuites de données accidentelles.

> « Pour se défendre contre les cybermenaces modernes, les responsables informatiques et de la cybersécurité doivent avoir une compréhension approfondie de leurs données - c'est-à-dire savoir qui y a accès, où elles résident, si elles contiennent des informations sensibles. Les acteurs malveillants se spécialisent dans l'exploitation des angles morts et les équipes IT et cybersécurité ont la responsabilité envers leurs clients de garder une longueur d'avance. »
>
> **Asheem Chandna**
> Partenaire, Greylock Partners

> « La protection de votre organisation et de ses données se résume à une résilience fondamentale. Et la résilience s'obtient par la sécurisation de vos données. Dans le cas où une cyberattaque se fraye un chemin à travers les lignes défenses traditionnelles, si vos données sont sécurisées, vous avez la possibilité de relancer rapidement votre activité et de vous en sortir. »
>
> **Shay Reddy**
> RSSI, Hanna Andersson

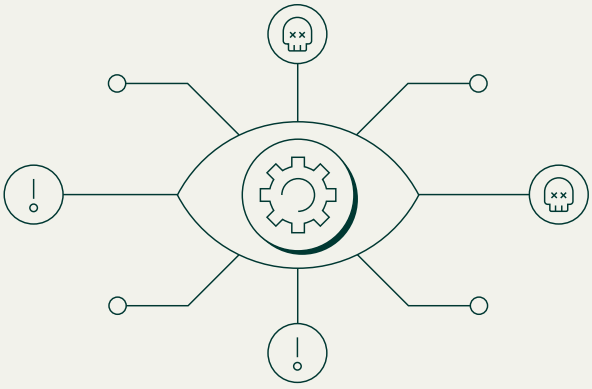
3.2 Bonnes pratiques

3 Partage *inter-équipe* des informations stratégiques sur les cyberrisques et les menaces

Les données recueillies par Rubrik Zero Labs révèlent que la majorité des participants s'attendent à une diminution de leurs ressources à l'avenir en raison d'une série de facteurs, notamment l'incertitude économique, le rétrécissement des budgets, les priorités concurrentes et des facteurs géopolitiques plus importants.

Ces facteurs de stress croissants font qu'il est plus important que jamais pour les équipes de travailler de manière transversale et avec une vue partagée de leurs données. Une meilleure collaboration, favorisée par une visibilité partagée, est particulièrement importante lors des incidents de sécurité, qui nécessitent une réponse et une restauration plus rapides pour assurer la continuité des activités, mais elle facilitera également l'exécution des tâches de routine.

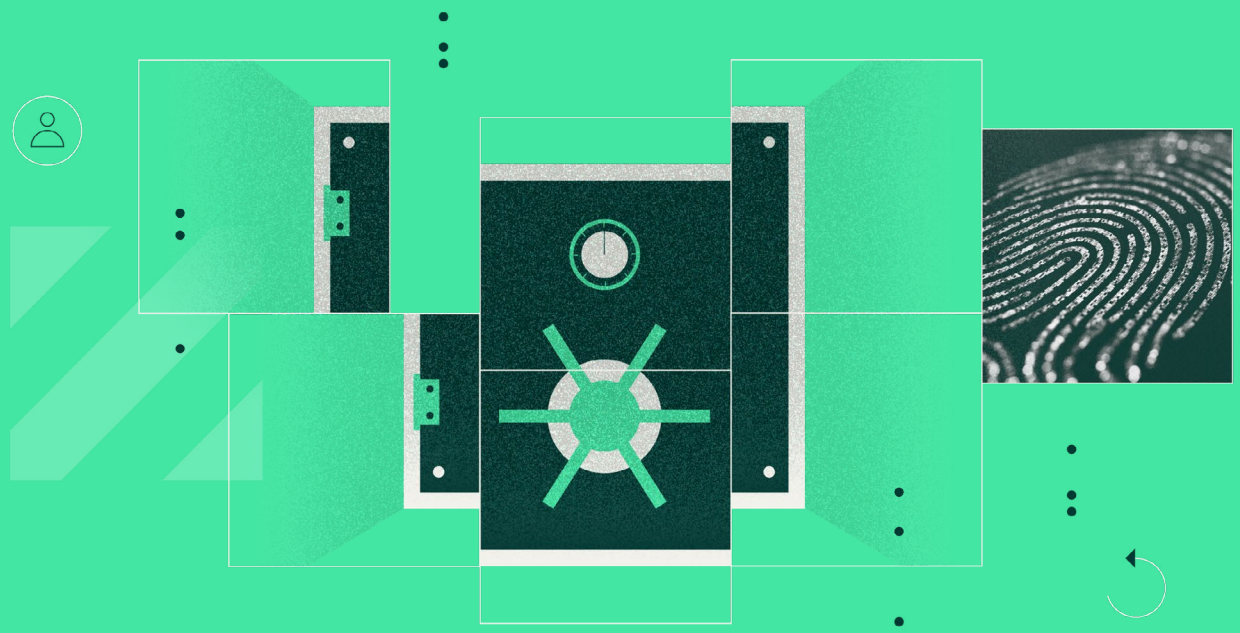
Plus les équipes seront nombreuses à utiliser les mêmes outils, les mêmes processus et la même visibilité dans l'ensemble de l'organisation, plus il sera facile de prendre ces décisions et de les appliquer à grande échelle.



« Nous omettons souvent la dimension psychologique des cyberattaques et le chaos qui a tendance à suivre après la découverte d'un incident. Les attaquants l'ont certainement compris, puisqu'ils essaient de générer des réactions émotionnelles lorsqu'ils attaquent, comme en témoigne l'augmentation des efforts d'extorsion criminelle et des campagnes de piratage et de fuite. En fin de compte, les responsables informatiques et de la cybersécurité ont tendance à porter la responsabilité de ces cyberattaques. L'une des techniques les plus efficaces que j'ai vues pour se préparer à ces types d'attaques est d'accepter que vous allez passer une mauvaise journée à un moment donné, et votre travail consiste à vous assurer que cela ne devienne pas votre « pire journée ». C'est pourquoi nous avons besoin que des défenseurs de tous les horizons se réunissent - partageant les bonnes pratiques, les enseignements tirés des attaques, les simulations, les cadres - afin que nous renforcions collectivement nos défenses et minimisions l'impact psychologique provoqué par une attaque. »

Chris Krebs
Ancien directeur de CISA et associé fondateur du groupe Krebs Stamos

Résumé



Sécuriser vos données dans la **lutte contre la cybercriminalité**

La cybercriminalité continue de menacer de nombreuses organisations, malgré le temps et les ressources considérables consacrés à la protection des données, des applications et de l'infrastructure. Les responsables informatiques et de la cybersécurité ont besoin de soutien, notamment de l'attention et de l'implication des dirigeants, d'un budget et de talents.

Cependant, ces ressources seules ne suffiront pas. Dans leur lutte contre les cybercriminels, les organisations doivent tirer parti de leurs propres données, afin de les rendre exploitables, de les sécuriser et de les restaurer d'une façon plus simple, plus fiable et plus rapide.

Rubrik Zero Labs