SOPHOS
Cybersecurity delivered.

L'état des ransomwares 2022

Résultats d'une enquête indépendante et agnostique menée auprès de 5 600 professionnels de l'informatique travaillant dans des organisations de taille moyenne dans 31 pays.

Un livre blanc Sophos. Avril 2022

Introduction

L'enquête annuelle de Sophos, qui étudie les expériences réelles des professionnels de l'informatique face aux ransomwares, a révélé un environnement d'attaque de plus en plus complexe associé à une plus forte pression financière et opérationnelle sur les victimes. L'enquête jette également un nouvel éclairage sur le lien entre ransomware et cyberassurance, et sur le rôle joué par l'assurance dans l'évolution des cyberdéfenses.

À propos de l'enquête

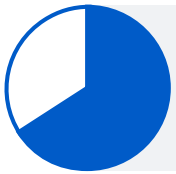
Sophos a demandé à l'organisme de recherche Vanson Bourne de mener une enquête indépendante et agnostique auprès de 5 600 décideurs informatiques dans des organisations de taille moyenne (100 à 5 000 employés) dans 31 pays. Cette enquête s'est déroulée entre janvier et février 2022, et les répondants ont été invités à répondre sur la base de leurs expériences vécues en 2021.

Les attaques se multiplient, leur complexité et leur impact augmentent

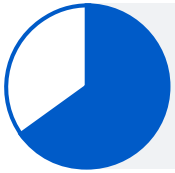
66 % des organisations ont été touchées par un ransomware en 2021, une hausse de 37 % par rapport à 2020. C'est une augmentation de 78 % en un an. Ce résultat montre que les adversaires sont devenus capables d'exécuter des attaques bien plus importantes à grande échelle. Cela reflète aussi le succès croissant du modèle de Ransomware-as-a-Service (RaaS) qui étend considérablement la portée des ransomwares en réduisant le niveau de compétence requis pour déployer une attaque. [Remarque : « touché par un ransomware » a été défini comme un ou plusieurs appareils impactés par une attaque, sans impliquer nécessairement de chiffrement].

Les adversaires parviennent aussi plus souvent à chiffrer les données dans leurs attaques. En 2021, les attaquants ont réussi à chiffrer des données dans 65 % des attaques, soit une augmentation par rapport aux 54 % signalés en 2020. Cependant, le pourcentage de victimes ayant subi une attaque d'extorsion seule, c'est-à-dire où les données n'ont pas été chiffrées mais où l'organisation a été rançonnée avec la menace d'exposer les données, a diminué, passant de 7 à 4 %.

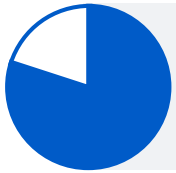
La hausse du nombre d'attaques de ransomware réussies s'inscrit dans un environnement de menaces de plus en plus complexe : en 2021, 57 % des organisations ont constaté une augmentation du volume global de cyberattaques, 59 % ont vu la complexité des attaques augmenter et 53 % ont déclaré que leur impact avait augmenté. 72 % ont constaté une augmentation dans au moins un de ces domaines.



66 %
touchés par un ransomware au cours de l'année passée



65 %
attaques parviennent à chiffrer les données



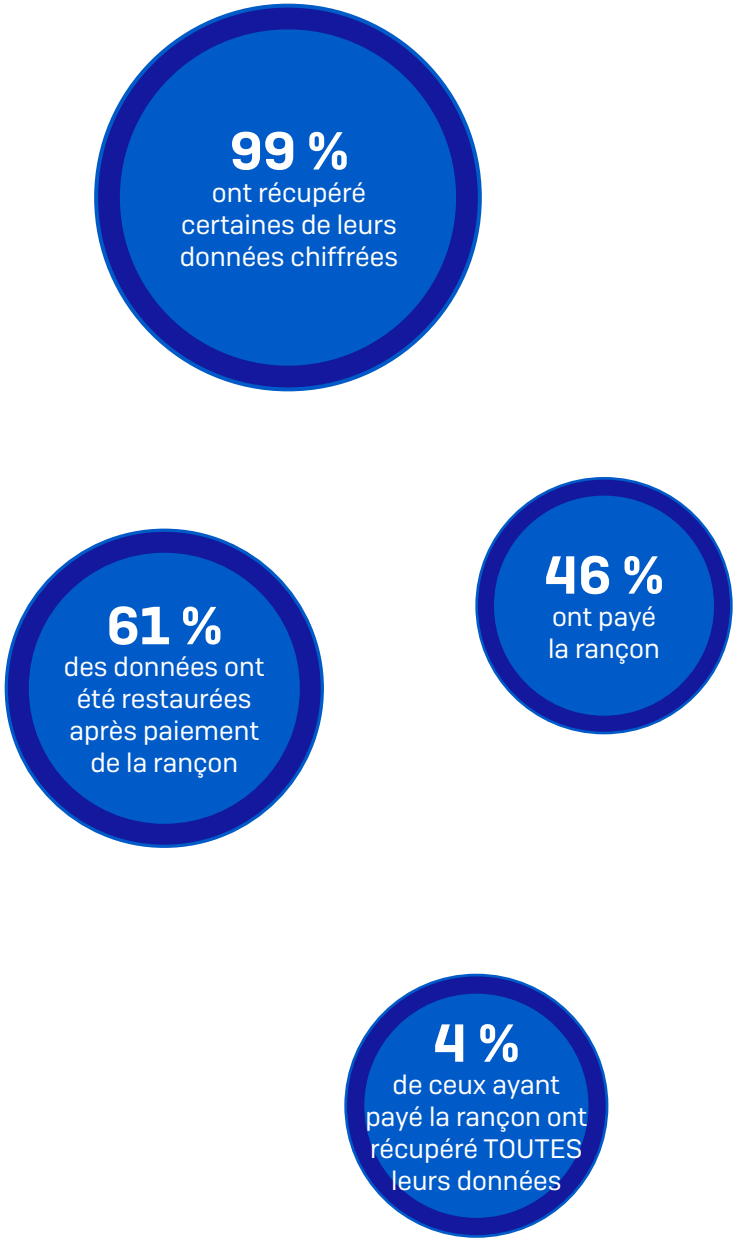
72 %
ont connu une augmentation du volume/de la complexité/de l'impact des cyberattaques

Les organisations se sont améliorées dans la restauration des données après une attaque

Les ransomwares étant de plus en plus répandus, les organisations sont de mieux en mieux armées pour faire face aux conséquences d'une attaque. Presque toutes les organisations touchées par un ransomware en 2021 (99 %) parviennent à récupérer des données chiffrées, soit une légère augmentation par rapport aux 96 % de l'année précédente.

Les sauvegardes sont la première méthode utilisée pour restaurer les données, utilisées par 73 % des organisations dont les données ont été chiffrées. Dans le même temps, 46 % ont déclaré avoir payé la rançon pour restaurer leurs données. Ces chiffres reflètent le fait que de nombreuses organisations utilisent plusieurs méthodes de restauration pour maximiser la rapidité et l'efficacité de leur remise en service. Dans l'ensemble, près de la moitié (44 %) des personnes interrogées dont les données ont été chiffrées ont utilisé plusieurs méthodes pour les restaurer après l'attaque.

Si le paiement de la rançon permet presque toujours de récupérer des données, le pourcentage de données restaurées après le paiement a chuté. En moyenne, les organisations ayant payé la rançon n'ont récupéré que 61 % de leurs données, contre 65 % en 2020. De même, seuls 4 % de celles ayant payé la rançon ont récupéré LA TOTALITÉ de leurs données en 2021, contre 8 % en 2020.



Le montant des rançons payées a augmenté

965 répondants dont l'organisation a payé la rançon nous ont dévoilé le montant exact, révélant que le montant moyen des rançons payées a considérablement augmenté l'année dernière.

En 2021, la proportion de victimes ayant payé une rançon d'un million de dollars (environ 0,86 M€) ou plus a presque triplé : elle est passée de 4 % en 2020 à 11 % en 2021. Parallèlement, le pourcentage de personnes ayant payé moins de 10 000 dollars (env. 8 658 €) a diminué, passant d'une personne sur trois (34 %) en 2020 à une sur cinq (21 %) en 2021.

Dans l'ensemble, le montant moyen des rançons payées s'élève à 812 360 USD (env. 703 341 €), soit une augmentation de 4,8 fois par rapport à la moyenne de 170 000 USD (env. 147 186 €) en 2020 (sur la base de 282 répondants). Bien que cette somme globale soit influencée par 15 paiements à 8 chiffres, il ressort clairement des données collectées que le montant des rançons payées a augmenté dans tous les secteurs. On observe des variations considérables d'un secteur à l'autre, les adversaires soutirant les sommes les plus élevées à ceux qu'ils considèrent comme les plus aptes à payer :

- Les montants moyens LES PLUS ÉLEVÉS s'élevaient à 2,04 millions de dollars (env. 1,77 M€) dans le secteur manufacturier et de la production (n=38) et de 2,03 millions de dollars (env. 1,76 M€) dans le secteur de l'énergie, du pétrole/gaz et des services d'utilité publique (n=91).
- Les montants moyens LES PLUS FAIBLES étaient de 197 000 USD (env. 170 562 €) dans le secteur de la santé (n=83) et de 214 000 USD (env. 185 281 €) dans les administrations locales/étatiques (n=20).

En Italie, où les paiements d'extorsion sont illégaux, c'est-à-dire où la loi interdit aux organisations de payer la rançon, 43 % des personnes dont les données ont été chiffrées admettent que leur organisation a payé la rançon (n=76). Cette étude démontre que les barrières législatives seules ne sont pas efficaces pour arrêter le paiement des rançons.

3x
plus de personnes ont payé une rançon de 1 million de dollars ou plus

21 %
ont payé une rançon inférieure à 10 000 $

812 360 $
Montant moyen des rançons (sauf quelques valeurs aberrantes)

MANUFACTURIER, SERVICES PUBLICS
Rançon moyenne la plus élevée (2 millions de dollars)

SANTÉ
Rançon moyenne la plus basse (197 000 $)

Taux de conversion utilisés: 1 £ (GBP) = 1,35 $ (USD); 1 £ (GBP) = 0,74 € (EUR)

Les ransomwares ont un impact commercial et opérationnel majeur

Les montants des rançons ne sont qu'un aspect d'une attaque, et l'impact des ransomwares va bien au-delà du chiffrement des bases de données et des appareils. 90 % des organisations touchées par un ransomware en 2021 ont déclaré que l'attaque la plus importante avait eu un impact sur leur capacité à fonctionner. En outre, 86 % des organisations du secteur privé ont déclaré que l'attaque avait entraîné une perte d'activité ou de revenus.

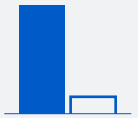
Dans l'ensemble, en 2021, le coût moyen supporté par une organisation pour remédier aux conséquences de l'attaque de ransomware la plus récente était de 1,4 million de dollars (env. 1,21 M€). Cette baisse bienvenue par rapport au 1,85 million de dollars (env. 1,60 M€) de 2020, reflète probablement le fait qu'avec la multiplication des cas de ransomwares, le préjudice de réputation lié à une attaque a perdu de son importance. Parallèlement, les assureurs sont mieux à même de guider les victimes rapidement et efficacement dans le processus de réponse à l'incident, réduisant les coûts de remédiation.

Il est intéressant de noter que dans de nombreux cas où la rançon est payée, c'est l'assureur, et non la victime, qui paie la facture. Nous aborderons ce point plus en détail plus loin.

En moyenne, les organisations ayant subi des attaques en 2021 ont mis un mois pour se remettre de l'attaque la plus importante, ce qui est une période très longue pour la plupart des organisations. C'est dans l'enseignement supérieur et l'administration centrale/fédérale que le rétablissement a été le plus lent : environ deux organisations sur cinq ont mis plus d'un mois pour s'en remettre. En revanche, les secteurs les plus résilients sont ceux de la manufacture et de la production (seuls 10 % ont mis plus d'un mois pour se rétablir) et des services financiers (12 % ont mis plus d'un mois), ce qui s'explique probablement par leurs niveaux élevés de planification et de préparation à la reprise après sinistre.

Par ailleurs, certaines organisations continuent de faire confiance à des défenses inefficaces. Parmi les personnes interrogées dont les organisations n'ont pas été touchées par un ransomware l'année dernière et ne s'attendent pas à l'être à l'avenir, 72 % se basent sur des approches qui n'empêchent pas les entreprises d'être attaquées : 57 % ont cité les sauvegardes et 37 % la cyberassurance comme raisons pour lesquelles elles n'anticipent pas une attaque, certains choisissant les deux options. Si ces éléments vous aident à vous remettre d'une attaque, ils ne l'empêchent pas de se produire en premier lieu.

90 %
des attaques de ransomware ont affecté la capacité à fonctionner de l'entreprise



86 %
des attaques de ransomware ont entraîné une perte d'activité/de revenus

1,4 M$
Coût moyen de remédiation d'une attaque de ransomware

UN MOIS
Temps moyen nécessaire pour se remettre d'une attaque

72 %
font confiance à des approches qui n'empêchent pas une attaque

Les organisations ne parviennent pas à utiliser efficacement leurs budgets et leurs ressources pour lutter contre les ransomwares

L'enquête a révélé qu'il ne suffit pas d'injecter du personnel et du budget pour résoudre le problème ; il faut plutôt investir dans la bonne technologie et disposer des compétences et du savoir-faire pour l'utiliser efficacement. Sans cela, votre retour sur investissement restera très faible.

64 % des organisations touchées par un ransomware en 2021 déclarent disposer d'un budget cybersécurité supérieur à leurs besoins, tandis que 24 % affirment disposer d'un budget adéquat. De même, 65 % des victimes de ransomware déclarent avoir plus d'ingénieurs en cybersécurité que nécessaire et 23 % estiment avoir le bon niveau de personnel. Ces résultats suggèrent que de nombreuses organisations ont du mal à déployer efficacement leurs ressources face à l'accélération du volume et de la complexité des attaques.

De plus, Les résultats indiquent que les organisations ne se rendent pas toujours compte qu'elles ne disposent pas des compétences nécessaires pour faire face aux dernières techniques d'attaque : 58 % de celles qui ont été touchées par un ransomware décrivent leur organisation comme étant plutôt/complètement au point pour l'examen des journaux pour identifier les signaux ou activités suspects, et 56 % disent être plutôt/complètement au point sur les derniers outils/méthodologies d'attaque.

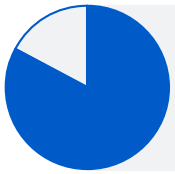
À l'inverse, parmi les organisations qui n'ont pas été touchées par un ransomware en 2021 et qui ne prévoient pas d'attaque future, la première raison de cette confiance est le fait de disposer d'un personnel de sécurité informatique formé ou d'un centre opérationnel de sécurité (SOC) interne capable de bloquer les attaques.

Les ransomwares favorisent le recours à la cyberassurance

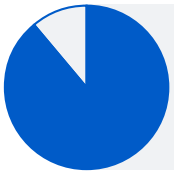
Plus de quatre organisations de taille moyenne sur cinq sont dotées d'une cyberassurance les protégeant contre les ransomwares. Cependant, si 83 % des personnes interrogées déclarent que leur organisation dispose d'une cyberassurance qui les couvre en cas de ransomware, 34 % déclarent que leur police comporte des exclusions/exceptions. Les secteurs de l'énergie, du pétrole/gaz et des services d'utilité publique sont les plus susceptibles d'être couverts (89 %), suivis de près par le commerce de détail (88 %). Le recours à la cyberassurance augmente avec la taille de l'entreprise : 88 % des entreprises de 3 001 à 5 000 employés étant couvertes, contre 73 % de celles de 100 à 250 employés.

Les organisations touchées par un ransomware en 2021 sont beaucoup plus susceptibles d'être assurées que celles n'ayant pas été victimes d'une attaque. Parmi celles qui ont été touchées, 89 % ont une cyberassurance, contre 70 % de celles qui n'ont pas été touchées. Le lien de cause à effet ici n'est pas clair. Il se peut que l'expérience directe d'un incident de ransomware ait poussé de nombreuses organisations à souscrire une assurance pour atténuer l'impact de futures attaques. Il se peut aussi que les adversaires ciblent leurs attaques sur des organisations dont ils savent qu'elles sont assurées, afin d'augmenter leurs chances d'obtenir le paiement d'une rançon. Une autre possibilité est que certaines organisations aient pris une couverture pour compenser des faiblesses connues dans leurs défenses. La réalité est probablement une combinaison de ces trois possibilités.

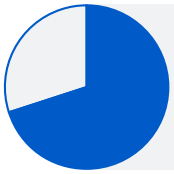
Le taux de couverture tombe à 61 % parmi ceux qui n'ont pas été touchés et ne s'attendent pas à subir une attaque. Étant donné que de nombreux membres de ce groupe font confiance à des approches qui ne bloquent pas les ransomwares, l'absence de couverture les expose pleinement aux coûts d'un incident.



83 %
ont une cyberassurance contre les ransomwares



89 %
touchés par un ransomware ont une cyberassurance



70 %
non touchés par un ransomware ont une cyberassurance

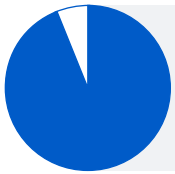
La cyberassurance permet d'améliorer les cyberdéfenses

94 % des personnes ayant souscrit une cyberassurance ont déclaré que le processus d'obtention de la couverture avait changé au cours de l'année dernière.

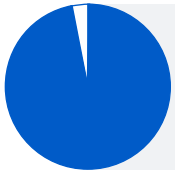
- 54 % déclarent que le niveau de cybersécurité requis pour être éligible est désormais plus élevé.
- 47 % déclarent que les polices sont désormais plus complexes.
- 40 % déclarent que moins de compagnies d'assurance proposent une cyberassurance.
- 37 % déclarent que le processus est plus long.
- 34 % déclarent qu'elle est plus chère.

Étant donné que les principales hausses de prix des cyberassurances ont commencé au cours des deuxième et troisième trimestres de 2021, il est probable que de nombreuses personnes interrogées n'avaient pas ressenti l'effet de ce changement au moment de l'enquête.

Alors que le marché de la cyberassurance se durcit et qu'il devient plus difficile d'obtenir une couverture, 97 % des organisations qui ont une cyberassurance ont apporté des changements à leurs cyberdéfenses pour améliorer leur position en matière de cyberassurance. 64 % ont mis en place de nouvelles technologies/services, 56 % ont augmenté les activités de formation/éducation du personnel et 52 % ont modifié leurs processus/comportements.



94 %
ont eu plus de mal à souscrire une cyberassurance l'année dernière



97 %
de ceux dotés d'une cyberassurance ont modifié leurs défenses pour améliorer leur position en matière de cyberassurance

La cyberassurance prend en charge presque toutes les demandes d'indemnisation liées à un ransomware

Fait rassurant pour ceux qui ont une cyberassurance, 98 % de ceux ayant été touchés par un ransomware et qui avaient souscrit une cyberassurance couvrant les ransomwares ont déclaré que la police d'assurance a fonctionné lors de l'attaque la plus importante — contre 95 % en 2019. Dans un certain nombre de pays, ce taux atteint même les 100 % : Suisse (n=52), Mexique (n=131), Suède (n=68), Belgique (n=66), Pologne (n=75), Turquie (n=51), EAU (n=49), Inde (n=218) et Singapour (n=91).

En examinant ce que la cyberassurance a payé, l'enquête révèle une augmentation du paiement des coûts de nettoyage et une diminution du paiement de la rançon par les assureurs. 77 % des personnes interrogées ont déclaré que leur assureur a payé les coûts de nettoyage, c'est-à-dire les coûts engagés pour remettre l'organisation en état de marche — contre 67 % en 2019. À l'inverse, 40 % ont déclaré que l'assureur avait payé la rançon, contre 44 % en 2019.

Cependant, le taux de paiement de la rançon variait considérablement selon le secteur. Les taux les plus élevés ont été signalés dans l'enseignement primaire et secondaire (53 %), les administrations étatiques/locales (49 %) et la santé (47 %), et les plus faibles dans le secteur manufacturier et la production (30 %) et les services financiers (32 %). Il est intéressant de noter que les secteurs où le taux de paiement de la rançon est le plus faible sont également ceux qui sont capables de se remettre le plus rapidement d'un incident, ce qui souligne l'importance de la planification et de la préparation à la reprise après sinistre.

Il est bon de rappeler que si la cyberassurance vous aide à retrouver votre état antérieur, elle ne couvre pas l'« amélioration », c'est-à-dire le moment où vous devez investir dans de meilleures technologies et de meilleurs services pour remédier aux faiblesses qui ont conduit à l'attaque.

98 %
taux de remboursement des demandes d'indemnisation pour ransomware

△ Paiement du coût de nettoyage △

67 %	77 %
2019	2021

▽ Paiement de la rançon ▽

44 %	40 %
2019	2021

Conclusion

Le défi posé par les ransomwares aux organisations ne cesse de croître. La proportion d'organisations directement impactées par les ransomwares a presque doublé en 12 mois : d'un peu plus d'un tiers en 2020 à deux tiers en 2021.

Face à cette quasi-normalisation, les organisations se sont améliorées pour faire face aux conséquences d'une attaque : pratiquement tout le monde récupère désormais certaines données chiffrées et près des trois quarts sont capables d'utiliser des sauvegardes pour restaurer des données.

Dans le même temps, la proportion de données chiffrées restaurées après le paiement de la rançon a chuté, passant à 61 % en moyenne. Malgré cela, le pourcentage de victimes ayant payé une rançon d'un million de dollars ou plus a été multiplié par près de trois.

L'enquête a révélé qu'il ne suffit pas d'injecter du personnel et du budget pour résoudre le problème ; il faut plutôt investir dans la bonne technologie et disposer des compétences et du savoir-faire pour l'utiliser efficacement. Les organisations doivent chercher à s'associer à des experts qui peuvent les aider à améliorer le rendement de leurs investissements en matière de cybersécurité et à renforcer leurs défenses.

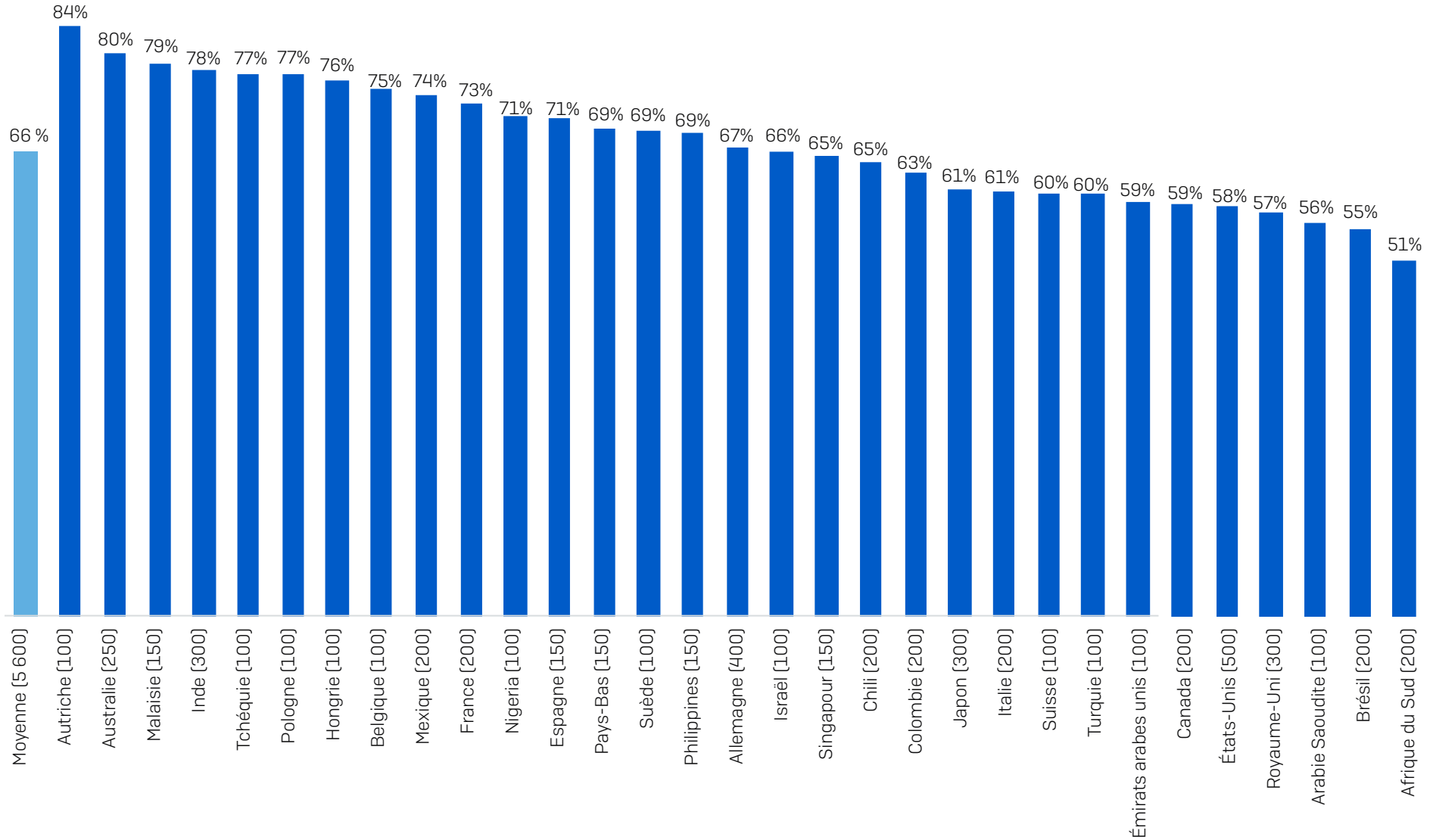
La plupart des organisations choisissent de réduire le risque financier associé à une attaque en souscrivant une cyberassurance. Pour elles, il est rassurant de savoir que les assureurs prennent en charge certains coûts dans presque tous les cas. Cependant, il devient de plus en plus difficile pour les organisations d'être couvertes, ce qui les a poussées à modifier leurs cyberdéfenses afin d'améliorer leur position en matière de cyberassurance.

Que vous cherchiez à obtenir une assurance ou non, l'optimisation de la cybersécurité est un impératif pour toutes les organisations. Nos cinq principaux conseils sont les suivants :

- Assurez des défenses de haute qualité en tout point de votre environnement. Passez en revue vos contrôles de sécurité et assurez-vous qu'ils continuent de répondre à vos besoins.
- Réalisez une chasse aux menaces proactive afin de bloquer les adversaires avant qu'ils ne puissent exécuter leur attaque. Si vous n'avez pas le temps ou les compétences en interne, sous-traitez à un spécialiste de la détection des menaces.
- Durcissez votre environnement en recherchant et en comblant les failles de sécurité : dispositifs non corrigés, machines non protégées, ports RDP ouverts, etc. Une solution XDR (Extended Detection and Response) est idéale à cet effet.
- Préparez-vous au pire. Sachez ce qu'il faut faire en cas de cyber incident et qui vous devez contacter.
- Faites des sauvegardes et entraînez-vous à les restaurer. Votre objectif est de vous remettre en marche rapidement, avec un minimum de perturbations.

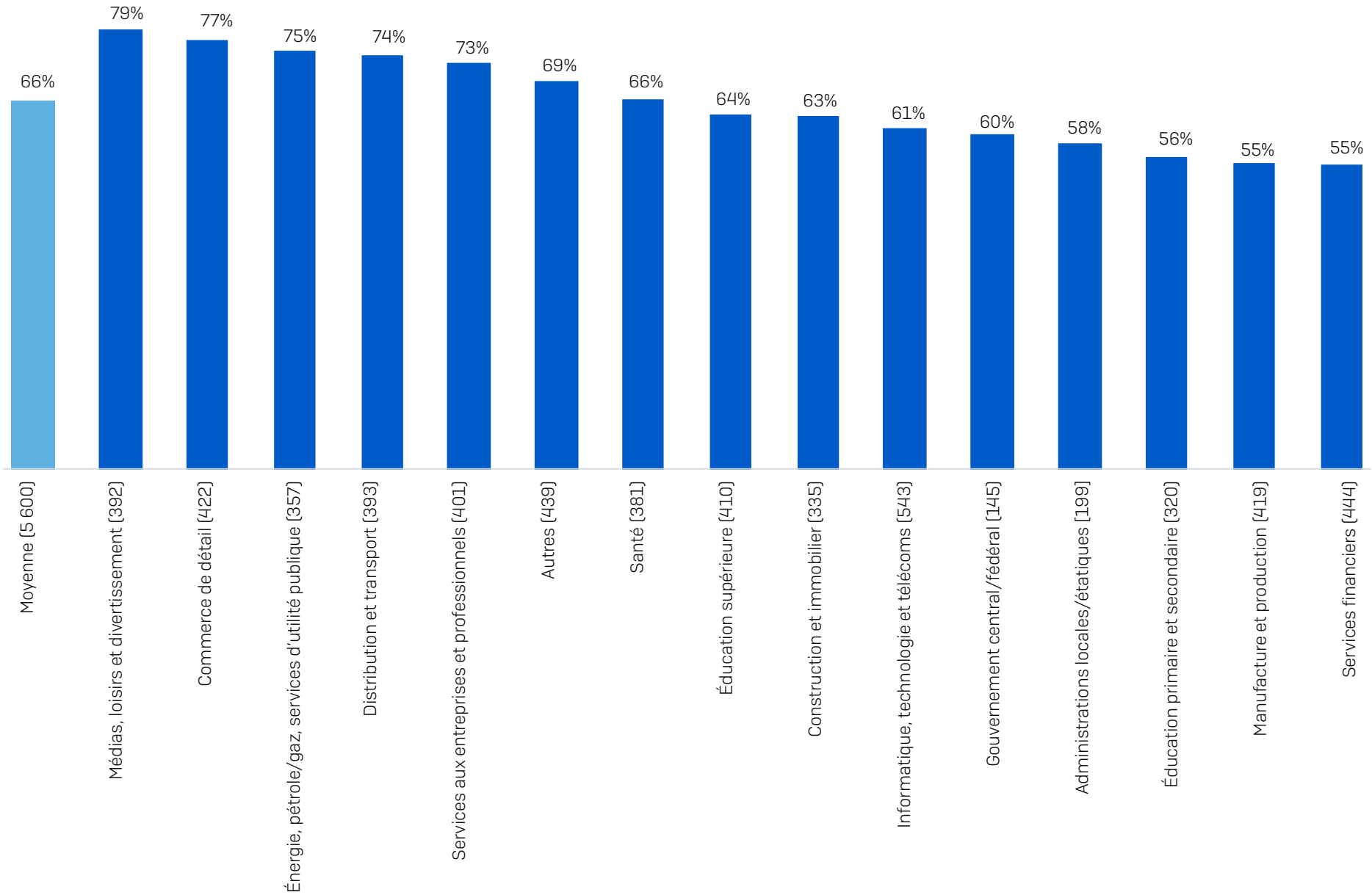
Pour obtenir des informations détaillées sur les différents groupes de ransomware, consultez le Centre de renseignements sur les menaces de ransomware de Sophos.

Pourcentage d'organisations touchées par un ransomware au cours de l'année passée



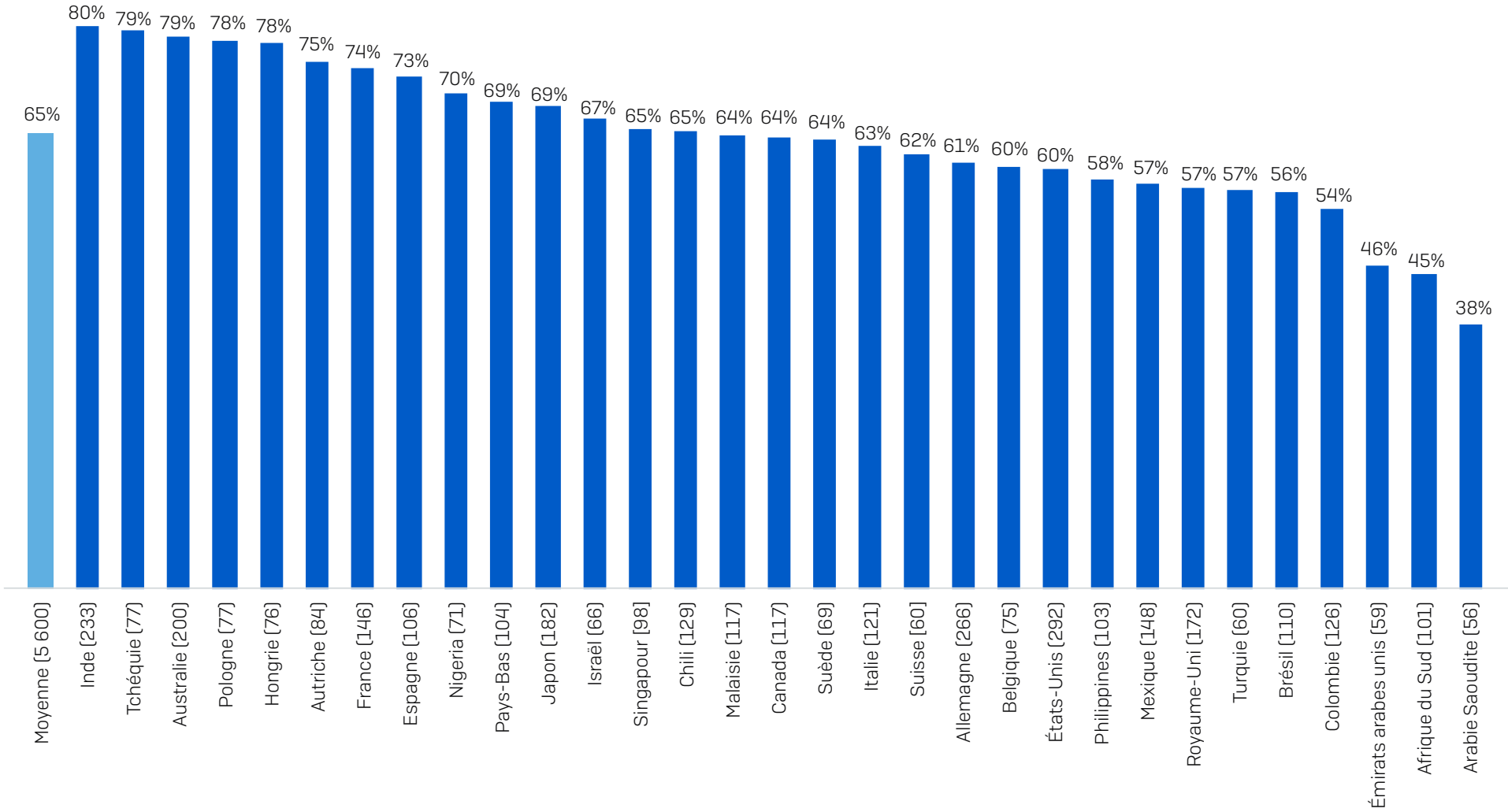
Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? (N=5 600) : Oui

Pourcentage des entreprises touchées par un ransomware au cours de l'année passée



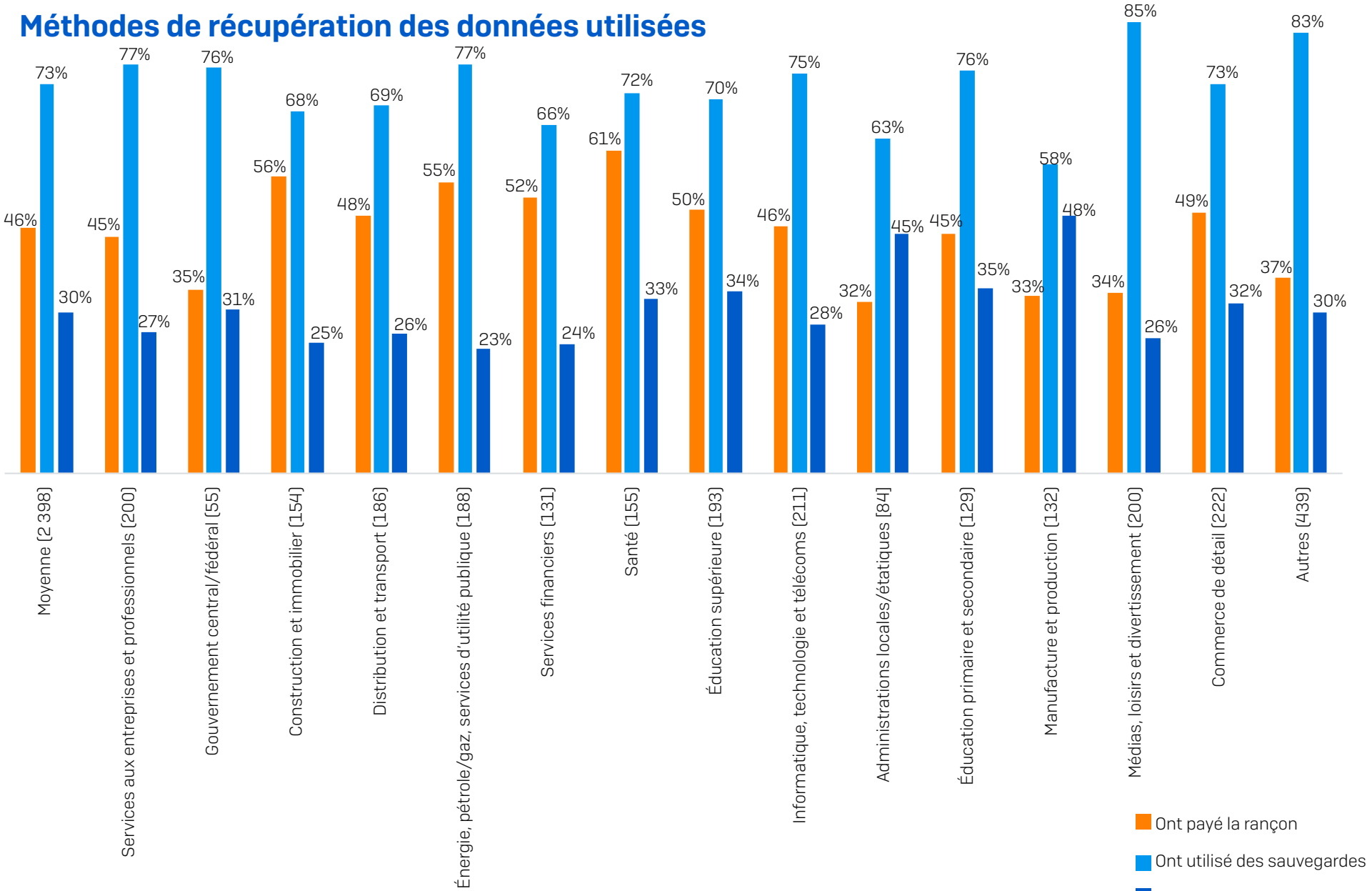
Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? (N=5 600) : Oui

Taux de chiffrement dans les attaques de ransomware



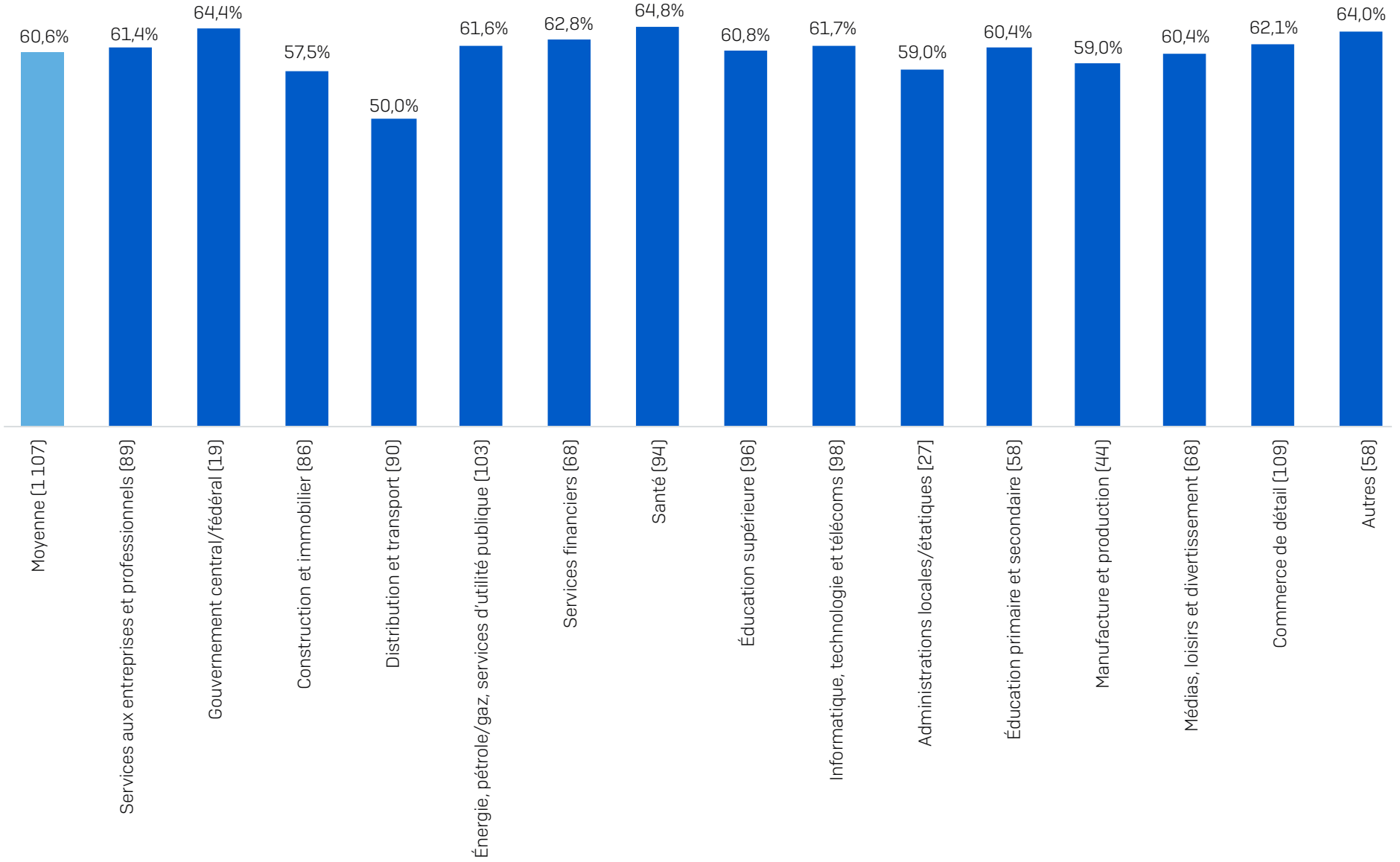
Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? (n=3 702 organisations touchées par un ransomware en 2021) : Oui

Méthodes de récupération des données utilisées



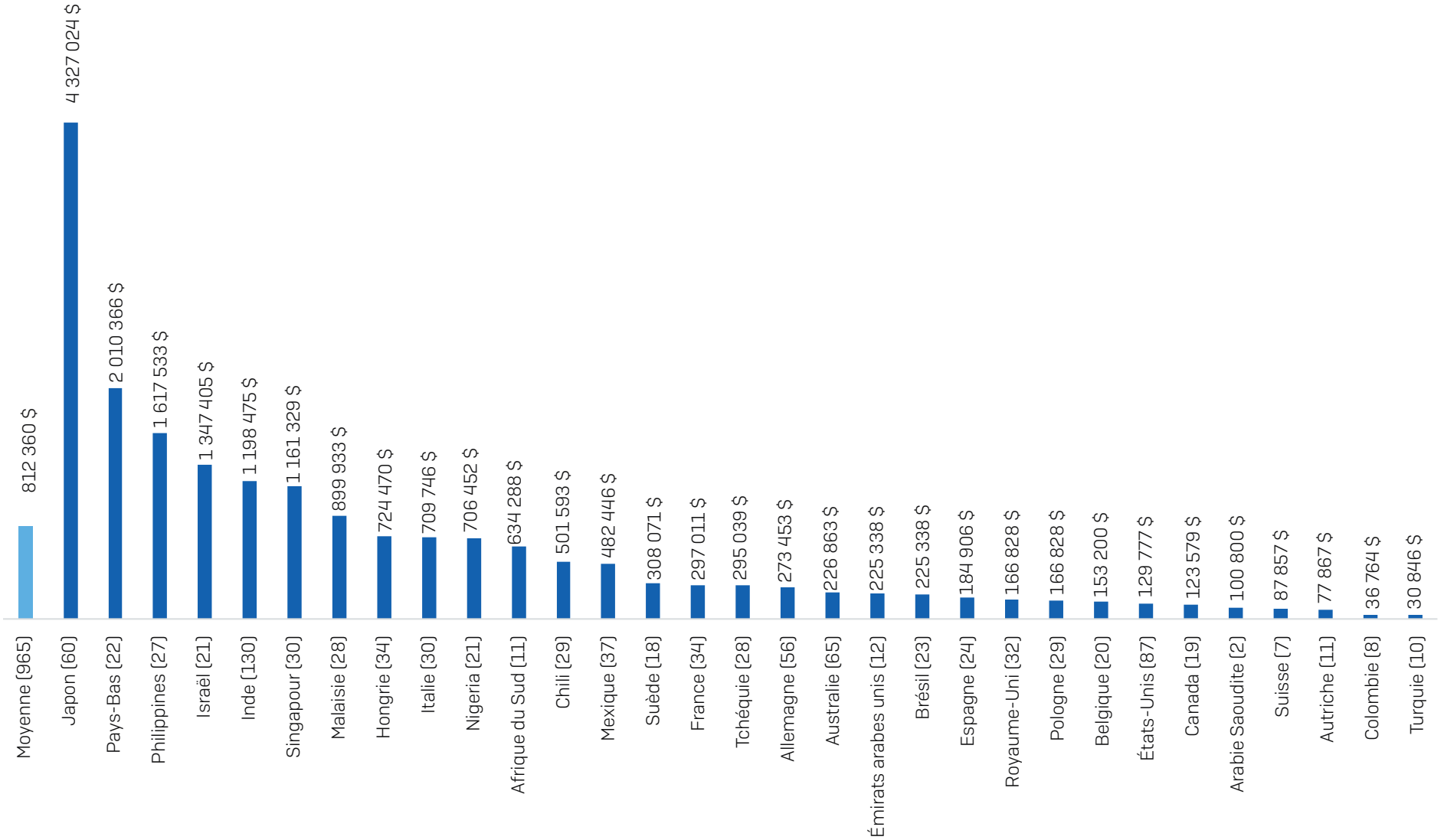
Lors de l'attaque de ransomware la plus importante, votre organisation a-t-elle récupéré des données ? (n=2 398 organisations dont les données ont été chiffrées) : Oui, nous avons payé la rançon et récupéré des données, Oui, nous avons utilisé des sauvegardes pour restaurer des données, Oui, nous avons utilisé d'autres moyens pour récupérer nos données.

Pourcentage des données restaurées après le paiement de la rançon



Quelle proportion des données de votre organisation avez-vous récupérée lors de la plus importante attaque de ransomware ?
(n=1 107 organisations ayant payé la rançon et ayant récupéré des données)

Montant moyen de la rançon payée par pays



Quel était le montant de la rançon payée par votre organisation lors de l'attaque de ransomware la plus importante ? US$. Chiffres de base dans le graphique. À l'exclusion des réponses « Ne sait pas » et des valeurs aberrantes.

N.B. Pour les pays dont les effectifs de base sont faibles, les résultats doivent être considérés comme indicatifs.

Coût moyen pour l'organisation pour remédier à l'attaque (millions de dollars US)

Pays	2021	2020	Variation sur un an
Moyenne (3 702)	1,40 $	1,85 $	-24 %
Australie (200)	1,01 $	1,84 $	-45 %
Autriche (84)	0,81 $	7,75 $	-90 %
Belgique (75)	3,71 $	4,75 $	-22 %
Brésil (110)	0,69 $	0,82 $	-16 %
Canada (117)	0,65 $	1,92 $	-66 %
Chili (129)	1,58 $	0,73 $	116 %
Colombie (126)	0,50 $	1,26 $	-60 %
Tchéquie (77)	2,58 $	0,37 $	589 %
France (146)	2,03 $	1,11 $	83 %
Allemagne (266)	1,73 $	1,17 $	48 %
Hongrie (76)	1,51 $	-	-
Inde (233)	2,81 $	3,38 $	-17 %
Israël (66)	1,41 $	0,57 $	148 %
Italie (121)	1,65 $	0,68 $	141 %
Japon (182)	0,96 $	1,61 $	-40 %
Malaisie (118)	1,22 $	0,77 $	58 %

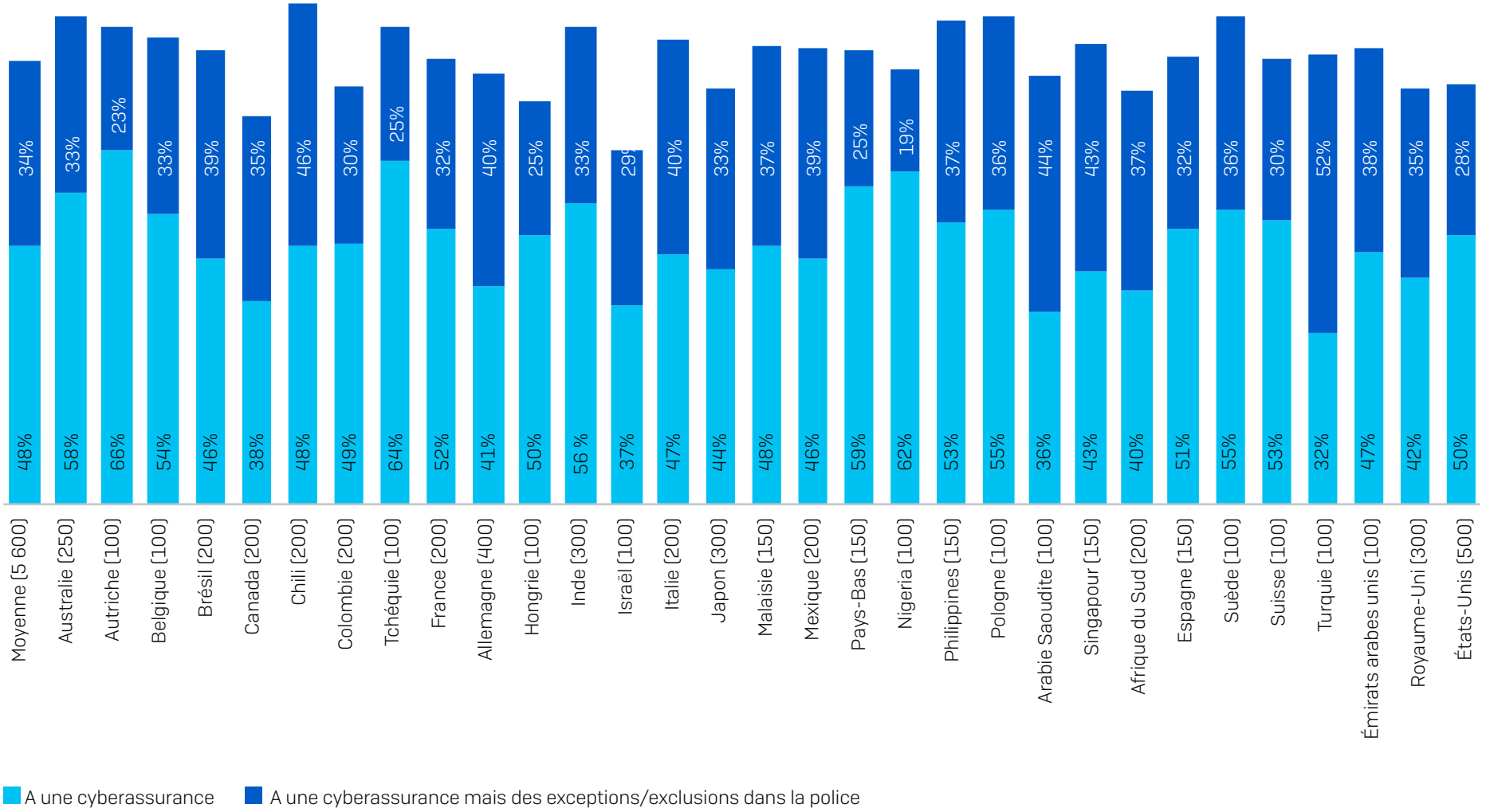
Pays	2021	2020	Variation sur un an
Mexique (148)	0,88 $	2,03 $	-57 %
Pays-Bas (104)	0,98 $	2,71 $	-64 %
Nigeria (71)	3,43 $	0,46 $	644 %
Philippines (103)	1,34 $	0,82 $	63 %
Pologne (77)	1,78 $	-	-
Arabie Saoudite (56)	0,65 $	0,21 $	212 %
Singapour (98)	1,91 $	3,46 $	-45 %
Afrique du Sud (101)	0,71 $	-	-
Espagne (106)	0,75 $	0,60 $	25 %
Suède (69)	0,75 $	1,40 $	-46 %
Suisse (60)	1,64 $	1,43 $	15 %
Turquie (60)	0,37 $	0,58 $	-36 %
Émirats arabes unis (59)	1,26 $	0,52 $	144 %
Royaume-Uni (172)	1,08 $	1,96 $	-45 %
États-Unis (292)	1,08 $	2,09 $	-49 %

N.B. Les chiffres de base sont pour les données de 2021 seulement.

N.B. Les valeurs sont en millions de dollars US.

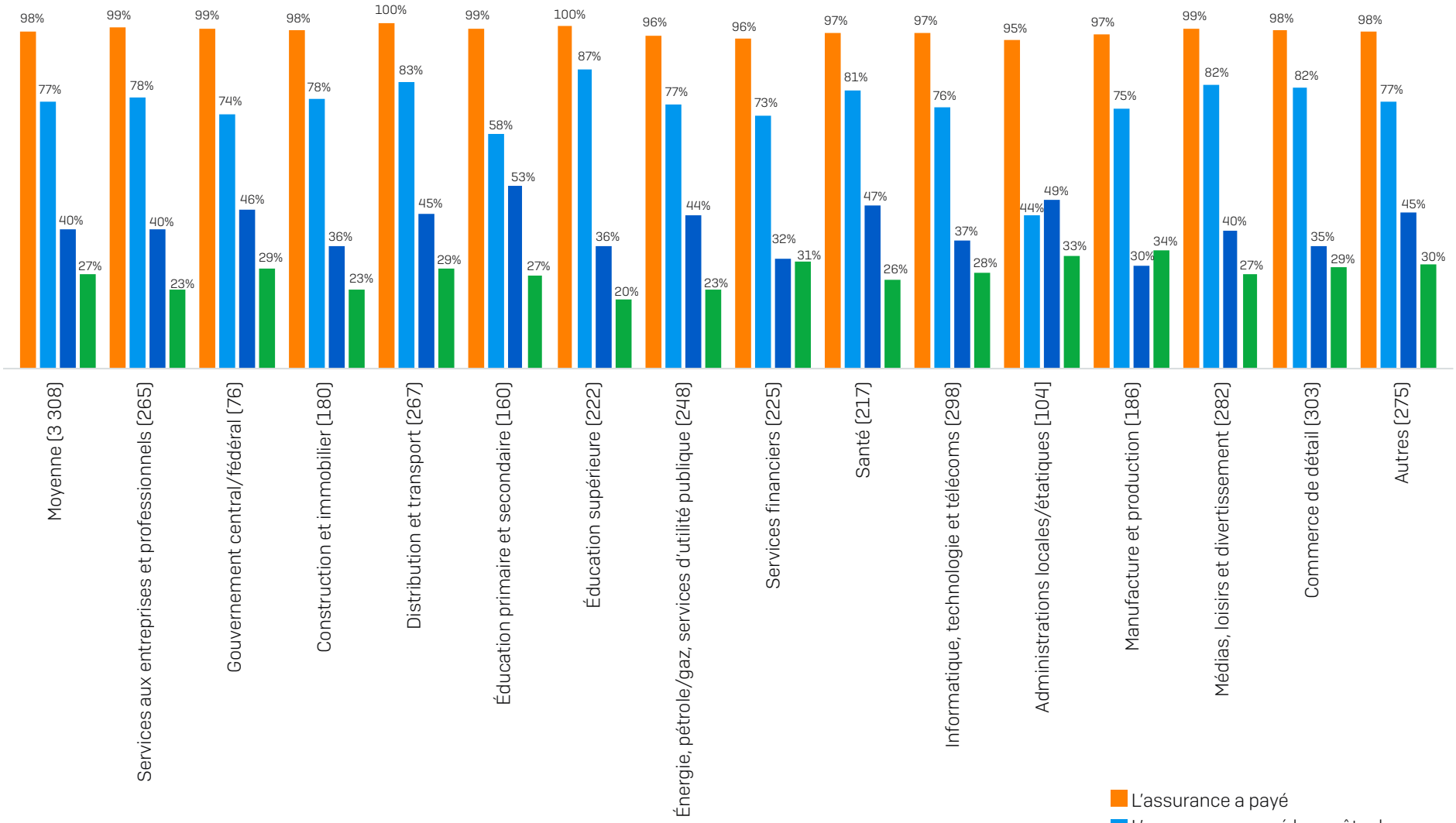
Quel était le montant approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus récente (en prenant en compte les pannes, temps de travail sacrifié, coûts du matériel et du réseau, manque à gagner, rançons payées, etc.) ? (n=3 702 organisations touchées par un ransomware en 2021)

Pourcentage d'organisations ayant une cyberassurance



Votre organisation dispose-t-elle d'une cyberassurance qui la couvre si elle est touchée par un ransomware ? (n=5 600). Oui ; Oui, mais il y a des exceptions/exclusions dans notre police

Taux d'indemnisation des cyberassurances



L'assurance cyber risques a-t-elle permis de couvrir les coûts associés à la plus importante attaque de ransomware subie par votre organisation ? (n=3 308 organisations touchées par un ransomware en 2021 et dotées d'une cyberassurance couvrant les ransomwares). Oui, elle a payé les coûts de nettoyage (par exemple, le coût de la remise en service de l'organisation) ; Oui, elle a payé la rançon ; Oui, elle a payé d'autres coûts (par exemple, le coût des temps d'arrêt, la perte d'opportunités, etc.)

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre entreprise.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2022-04-04 (WP-NP)

SOPHOS