LES CYBERATTAQUES RÉUSSIES EN FRANCE : UN COÛT DE 2 MDS€ EN 2022

Étude économique

Juin 2023

ASTERÈS
études, recherche & conseil économique

RÉSUMÉ EXÉCUTIF

Asterès évalue le coût des cyberattaques réussies sur les systèmes d'information des organisations françaises à 2 Mds€ en 2022[1]. Les cyberattaques réussies sont définies comme une intrusion (par exemple *phishing*, exploitation de faille), une attaque par rançongiciel ou une attaque par déni-de-service, avérées dans le système d'information d'une organisation et ayant un impact opérationnel et/ou financier. Le coût de l'ensemble de ces cyberattaques réussies se répartit entre un coût direct de 887 M€, le paiement des rançons qui s'élève à 888 M€ et des pertes de production qui équivalent à 252 M€. Les montants en question font des cyberattaques un enjeu économique non-négligeable pour la France, en particulier au vu de l'alimentation d'organisations cybercriminelles et du probable effet sur la balance des paiements. Ce coût global revêt une grande dispersion entre les types d'attaques et les organisations concernées. Il ne prend pas en compte les dépenses préventives pour éviter le succès des cyberattaques ni le coût si ces cyberattaques aujourd'hui mises en échec étaient réussies.

MÉTHODE : ESTIMER LE COÛT DES CYBERATTAQUES RÉUSSIES EN FRANCE EN 2022

Asterès s'est appuyé sur la littérature et une enquête menée auprès des adhérents du CRiP pour estimer le volume des cyberattaques réussies en France en 2022 puis pour calculer le coût moyen de la résolution de la crise, le coût moyen d'une rançon et les pertes moyennes de productivité. Les coûts ainsi estimés constituent les principaux impacts économiques des trois types d'attaques couvertes par l'étude : intrusion avérée dans le système d'information d'une organisation, attaque par rançongiciel, ou attaque par déni-de-service, ayant eu un impact opérationnel et/ou financier. Asterès a conduit une revue de littérature internationale sur les cyberattaques et leur impact économique dans le but de sélectionner les meilleures données et de proposer un chiffrage à partir de sources multiples. Ce sont *in fine* cinq études qui ont été retenues (Forrester Consulting - Hiscox, OpinionWay - CESIN, Kaspersky Lab, CoveWare et Accenture - Ponemon Institute[2]). En complément, Asterès a mené sa propre enquête auprès des adhérents du CRiP pour récolter les données manquantes. Ces différentes sources ont permis un chiffrage qui intègre les organisations de la sphère publique (administration centrale, collectivités territoriales/locales, établissements publics) et de la sphère privée. Le travail repose sur des moyennes, le plus souvent possible pondérées en fonction des tailles d'organisation, des types d'organisation et des types d'attaque.

FRÉQUENCE ET VOLUME : 1,8 CYBERATTAQUE RÉUSSIE EN MOYENNE PAR ORGANISATION ET PAR AN, SOIT 385 000 EN 2022

Asterès estime que les systèmes d'information des organisations françaises ont été victimes d'au moins 385 000 attaques réussies en 2022. Une organisation française subit en moyenne 1,8 cyberattaque réussie par an (43% des organisations toutes tailles confondues ont subi une moyenne de 4,3 cyberattaques au cours des douze derniers mois). Les vecteurs d'attaque les plus fréquents sont le *phishing* ou *spearfishing* et l'exploitation d'une faille existante. Le volume total de cyberattaques a été estimé en extrapolant le nombre moyen de cyberattaques par organisation à la démographie des organisations publiques et privées en France. D'après cette estimation, les 831 attaques portées à la connaissance de l'ANSSI en 2022 ne représenteraient donc que 0,2% du volume total. Cette estimation exclut les microentreprises (moins de 10 salariés) et les communes de moins de 500 habitants.

---

[1] L'ensemble des données présentées dans la Synthèse sont sourcées dans la suite de l'étude.
[2] Les références complètes sont présentées dans la suite de l'étude.

COÛT MOYEN : 59 000€ PAR CYBERATTAQUE RÉUSSIE

Par cyberattaque réussie, le coût public – privé est estimé en France en 2022 à 59 000 €, une moyenne qui recouvre des réalités disparates selon le type d'attaque et d'organisation. Ce coût moyen se décompose entre un coût direct (44%), qui comptabilise les ressources allouées à la résolution de la crise (mobilisation des équipes internes, services professionnels externes, sollicitation des avocats), un coût des rançons (44%) et des pertes de productivité (12%). Le coût direct et le coût des rançons constituent autant de ressources qui auraient pu être investies dans la transformation numérique et donc générer des gains de productivité, au lieu de cela, les coûts de production augmentent, ce qui implique des pertes de qualité, des hausses de prix ou des hausses de dépenses publiques. Le temps de travail perdu est pour une part compensé plus tard dans l'année (à hauteur de 44% d'après Asterès), et constitue pour le reste une perte de productivité. Par-delà les moyennes, les cyberattaques les plus significatives en 2022 ont probablement atteint un coût d'au moins 10 M€, et pour les grandes entreprises le coût moyen d'une cyberattaque réussie peut être estimé à 225 000€ hors rançon.

PRÉAMBULE

Le cabinet ASTERES a été mandaté par le Club des Responsables d'Infrastructure, de technologies et de Production Informatique (CRiP) pour travailler sur le coût des cyberattaques réussies en France.

Les économistes d'ASTERES ont bénéficié d'une totale indépendance dans la conduite de cette étude. Les sources de l'ensemble des données utilisées sont disponibles dans l'étude.

Les propos tenus ici n'engagent que leurs auteurs. Le document a été rédigé par Guillaume Moukala Same et Charles-Antoine Schwerer, économistes chez ASTERES.

SOMMAIRE

1. MÉTHODE : ESTIMER LE COÛT DES CYBERATTAQUES RÉUSSIES EN FRANCE EN 2022

1.1. DÉFINITION ET PÉRIMÈTRE : LES CYBERATTAQUES RÉUSSIES DANS LE PUBLIC ET LE PRIVÉ

Dans cette étude, une cyberattaque réussie est définie comme une intrusion ou une attaque avérée dans le système d'information d'une organisation et ayant un impact opérationnel et/ou financier. Ce terme recouvre plusieurs types d'intrusions (par exemple *phishing*, exploitation d'une faille) et d'attaques (par rançongiciel, par déni-de-service) mais exclut les arnaques (au président, acquisition de noms de domaine). Les données présentées correspondent à une cyberattaque moyenne, ce qui permet de calculer un coût total pour l'économie mais ne met pas en lumière la grande dispersion de coût selon les attaques et les entreprises concernées. Ainsi, lorsque les données sont disponibles, des précisions sont apportées sur la variété des conséquences. Enfin, cette étude ne s'intéresse pas aux tentatives d'intrusion et ou d'attaque ayant échouées.

Asterès considère les cyberattaques qui touchent le secteur privé et le secteur public (collectivités territoriales, ministères, établissements de santé publics, établissements d'enseignement supérieur et autres établissements publics). Pour le secteur privé, les microentreprises (moins de 10 salariés) ne sont pas prises en compte en raison de leur nombre important (près de 4 millions), comparé à la taille des échantillons sur lesquels sont basées les enquêtes utilisées dans cette étude. Les PME (10 à 249 salariés) sont comptabilisées dans l'estimation du volume de cyberattaques réussies en 2022, mais pas dans l'estimation du coût des cyberattaques réussies, pour les mêmes raisons. Pour les communes, sont prises en compte dans l'estimation du volume seules les communes de plus de 500 habitants et dans l'estimation du coût seules les communes de plus de 10 000 habitants[3]. Les autres organisations publiques sont considérées d'une taille équivalente à une ETI ou grande entreprise.

1.2 SOURCES : UNE REVUE DE LITTÉRATURE COMPLÉTÉE D'UNE ENQUÊTE

La présente étude cherche à identifier dans la littérature les meilleures données pour proposer un chiffrage à partir de sources multiples. Asterès a conduit une revue de littérature internationale sur l'impact économique des cyberattaques réussies. Les publications académiques et les publications des cabinets d'études et de conseil ont été scrutées en prenant en compte les limites méthodologiques de chacune pour ne conserver que les données les plus robustes. *In fine*, cinq études ont été retenues, servant chacune à chiffrer une à deux données[4]. Les coûts ont été actualisés en prenant en compte l'inflation quand nécessaire et les données étant récentes, le chiffrage a pu être réalisé pour l'année 2022. En complément, Asterès a mené une enquête auprès des adhérents du CRiP (entreprises, collectivités, administration centrale, établissements publics) qui a recueilli 86 réponses. Seulement, 56% des répondants n'étaient pas habilités dans le cadre de leurs fonctions à communiquer sur les cyberattaques subies par leur organisation, réduisant l'échantillon à 25 organisations, dont 11 ont été

[3] D'après les « Enquêtes sur les Personnels des Collectivités territoriales et des Établissements publics locaux » de l'Insee, dans une commune, le ratio est d'environ 24,6 employés pour 1 000 habitants. Asterès considère ainsi que les communes de 500 à 9 999 habitants sont équivalentes en taille aux PME et les communes de plus de 10 000 habitants équivalentes aux ETI – GE.

[4] Ces études sont présentées plus loin dans le présent document.

victime de cyberattaque(s) en 2022. Finalement, ce questionnaire n'a été utilisé que pour l'estimation du nombre des jours-hommes nécessaire à la résolution d'une crise cyber, donnée manquante dans la littérature. A la connaissance d'Asterès, l'estimation la plus récente du coût agrégé des cyberattaques en France remonte à 2013, mais ne prenait en compte que deux secteurs (information et communication, finance) et un seul type de coût (pertes de production). Les auteurs avaient estimé un coût entre 11 M€ 43 M€[5].

1.3 TYPES DE COÛT : DÉPENSES CASH, RÉALLOCATION DE RESSOURCES ET PERTE DE PRODUCTIVITÉ

Plusieurs types de coût sont pris en compte. Ces coûts varient selon les types de cyberattaque et les données présentées intègrent ainsi ces dispersions pour proposer un coût moyen lorsque les conséquences ont lieu. Asterès distingue le coût direct, du coût de la rançon et des pertes dues à l'interruption de l'activité. Dans le cas de cyberattaques réussies, l'ensembles des attaques ont un coût direct et des pertes dues à l'interruption de l'activité, quand seulement certaines attaques impliquent un coût de la rançon.

- **Le coût direct correspond aux dépenses consenties par l'organisation pour réagir à l'attaque et à ses conséquences**. Il s'agit essentiellement du coût de la main d'œuvre ayant travaillé à la résolution de la crise, qu'elle soit interne (équipes IT, juristes) ou externe (consultants en cybersécurité, en gestion du risque, sollicitation des avocats de l'entreprise ou autres). Ce coût comprend une part de dépenses (les services externes) et une part de réallocations de ressources (sollicitations des équipes en interne).

- **Le coût de la rançon correspond au montant moyen payé par les victimes** (et non le montant moyen demandé par les malfaiteurs). Ce coût constitue donc une dépense cash pour l'organisation.

- **Les pertes résultent de la paralysie des systèmes d'information occasionnée par la cyberattaque,** qui limite pendant un certain temps la productivité des employés, voire les empêche totalement d'effectuer leurs tâches. Les pertes dues à l'interruption de l'activité correspondent à ce qui est appelé « *downtime cost* » dans la littérature. Il ne s'agit ni d'une dépense cash pour l'organisation ni d'une réallocation de ses ressources, mais plutôt d'une perte de productivité qui peut être exprimée en heures de travail ou en équivalent monétaire.

[5] Rokhaya Dieye et al., « Estimates of the Macroeconomic Costs of Cyber-attacks », *Risk Management and Insurance Review* 23, nº 2 (juin 2020): 183-208, https://doi.org/10.1111/rmir.12151.

2. FRÉQUENCE ET VOLUME : 1,8 CYBERATTAQUE RÉUSSIE EN MOYENNE PAR ORGANISATION, SOIT 385 000 EN 2022

2.1 FRÉQUENCE : 1,8 CYBERATTAQUE RÉUSSIE PAR ORGANISATION EN MOYENNE

Par an, une organisation française subit en moyenne de 1,8 cyberattaque avec des conséquences opérationnelles ou financières, le plus souvent des attaques par *phishing* ou *spearfishing* et des exploitations de failles existantes. A la connaissance d'Asterès, deux enquêtes ont estimé la part des organisations françaises ayant été victime d'une ou plusieurs cyberattaque(s) réussies en 2022 : l'enquête de Forrester Consulting menée pour Hiscox auprès de 921 représentants d'organisations françaises (entreprises, administrations et associations) entre fin 2021 et début 2022[6] et l'enquête d'OpinionWay menée pour le CESIN auprès de 328 représentants d'organisations françaises (entreprises, administrations, collectivités et autres services publics) en 2022[7]. Ces deux sources permettent de chiffrer la part des organisations françaises ayant subi une cyberattaque réussie au cours des douze derniers mois et leur nombre :

- **Asterès retient de l'étude CESIN le nombre moyen de cyberattaques réussies subies, de 4,3 par an (parmi les organisations victimes de cyberattaques)**. Cette enquête porte sur la cyber-malveillance, définie comme « un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information »[8]. D'après cette enquête, parmi les entreprises ayant subi un acte de cyber-malveillance au cours de l'année 2022, 32% en ont subi entre 2 et 3, 7% entre 4 et 9, 2% entre 10 et 14 et 4% en ont subi 15 ou plus. Selon cette enquête, les vecteurs les plus fréquents sont le *phishing* ou *spearfishing* et l'exploitation d'une faille existante (voir *graphique 2*). Le CESIN intègre les arnaques au président et les acquisitions de nom de domaine quand Asterès les exclut de son périmètre en les considérant comme des actes de cyber-malveillance mais pas comme des cyberattaques.

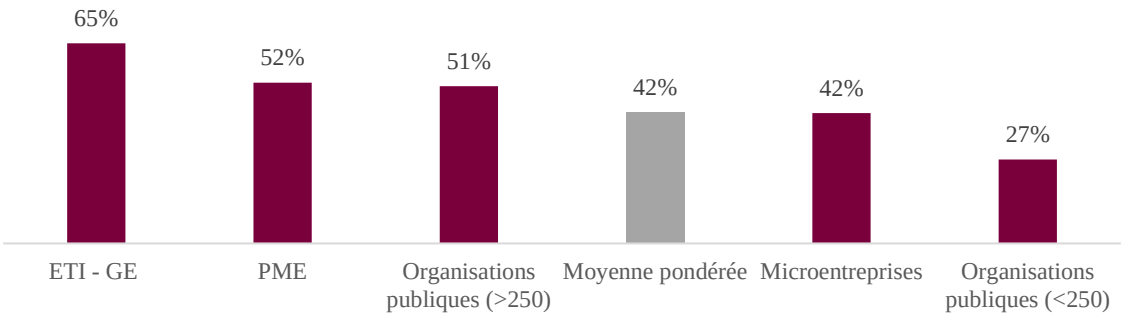
- **Asterès a estimé à 43% en moyenne la part des organisations ayant été victimes d'au moins une cyberattaque réussie au cours des douze derniers mois, à partir des données d'Hiscox.** D'après cette enquête, en France, 51% des organisations publiques de 250 employés ou plus ont subi au moins une cyberattaque au cours des douze derniers mois, 27% des organisations publiques de moins de 250 employés[9], 65% des ETI et grandes entreprises, 52%

---

[6] « Hiscox Cyber Readiness Report 2022 | Hiscox Group ».
[7] Laurent Delattre, « Cybersécurité, le CESIN souligne une légère baisse des attaques réussies en 2022 », *IT for Business* (blog), 1 février 2023, https://www.itforbusiness.fr/cybersecurite-le-cesin-souligne-une-legere-baisse-des-attaques-reussies-en-2022-59399.
[8] Il est également précisé que les cyberattaques telles qu'entendues entrainent « des pertes financières significatives et/ou une atteinte à l'image de l'entreprise et/ou des efforts significatifs de défense pour contenir et traiter l'attaque ». Les tentatives d'attaques qui ont été arrêtées par les systèmes de prévention ne sont pas comptés.
[9] Ici, Asterès utilise le secteur « gouvernement et ONG » comme proxy pour le secteur public.

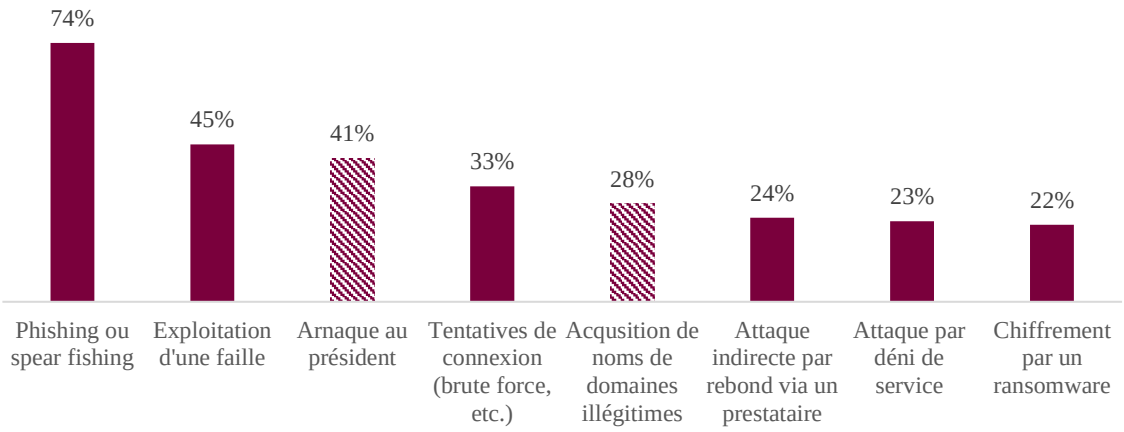
des PME et 42% des microentreprises[10] (voir *graphique 1*). La proportion moyenne pondérée toutes organisations confondues a été calculée par Asterès. Cette enquête a été préférée à celle du CESIN en raison de la taille de l'échantillon et de la précision des données. La définition d'une cyberattaque n'est pas précisée, mais les résultats étant cohérents avec l'enquête du CESIN, qui estime à 45% la part des organisations françaises ayant été victime de cyberattaque en 2022[11], Asterès considère qu'il s'agit bien des cyberattaques réussies. Le résultat est également cohérent avec les données remontées à l'ANSSI, d'après lesquelles les organisations publiques représentent près de la moitié des cyberattaques[12].

Graphique 1. Part des organisations ayant été victime d'au moins une cyberattaque réussie au cours des douze derniers mois, par type d'organisation



Source : *Hiscox Cyber Readiness Report 2022*, moyenne pondérée calculée par Asterès

Graphique 2. Principaux actes de cybermavleillance ayant eu un impact selon le CESIN



Source : CESIN

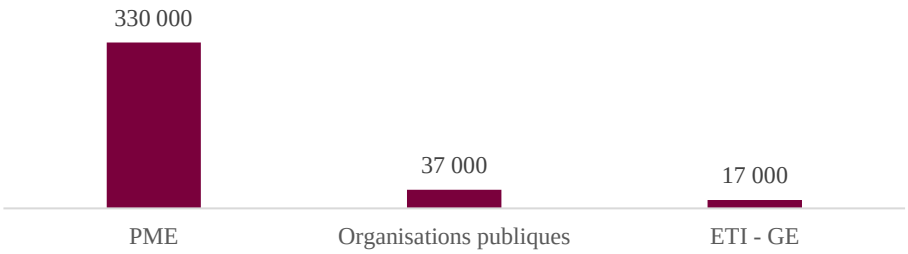
Lecture : Parmi les organisations ayant subi au moins un acte de cybermalveillance, part des entreprises ayant subi un acte de ce type. Note : le CESIN compte le chiffrement par ransomware dans les conséquences, nous considérons ici qu'il s'agit d'un vecteur d'attaque

[10] Notons toutefois que ce dernier chiffre doit être interprété avec précaution en raison de la faible taille de l'échantillon (233) relativement au nombre de microentreprises en France (près de 4 millions).
[11] Delattre, « Cybersécurité, le CESIN souligne une légère baisse des attaques réussies en 2022 ».
[12] « Panorama de la cybermenace 2022 ».

2.2 VOLUME : AU MOINS 385 000 CYBERATTAQUES EN 2022

Asterès estime à 385 000 le nombre de cyberattaques réussies sur des organisations françaises en 2022. Ce chiffre a été obtenu en extrapolant le nombre moyen de cyberattaques réussies par organisation à la démographie des entreprises, collectivités, administrations et établissements publics français (voir détails en annexe). D'après cette estimation, les 831 attaques portées à la connaissance de l'ANSSI en 2022 ne représentent que 0,2% du volume total estimé de cyberattaques réussies. Du fait de leur nombre, les premières victimes de cyberattaques sont des entreprises, et en particulier des PME : parmi les 347 000 cyberattaques réussies touchant des entreprises, 330 000 concernent des PME (voir *graphique 3*). Asterès estime que près de 40 000 cyberattaques réussies ont visé des organisations publiques en 2022, soit 10% du total.

Graphique 3. Ventilation de cyberattaques réussies en 2022 entre les entreprises et les organisations publiques



3. COÛT MOYEN EN FRANCE : 58 600€ PAR CYBERATTAQUE RÉUSSIE

3.1. COÛT DIRECT : 25 600€ PAR CYBERATTAQUE RÉUSSIE

Le coût direct moyen d'une cyberattaque réussie en France est estimé à 25 600€ (hors rançon). Pour le calcul, Asterès s'appuie sur les données recueillies par l'enquête réalisée dans le cadre de cette étude auprès des adhérents du CRiP et sur les données du cabinet Kapersky Lab. Le coût retenu correspond au chiffre médian entre ces deux sources, pondéré avec la répartition entre les entreprises et les acteurs publics, pour corriger des différences entre ces deux types d'acteurs (voir annexe pour les détails). En moyenne, le coût direct pour une grande entreprise peut être estimé à 64 000€.

- **Le coût direct moyen estimé par Asterès s'élève à 39 000€ par cyberattaque réussie.** Les répondants à l'enquête Asterès ont déclaré avoir dédié 463 jours-hommes en moyenne (internes ou externes) à la résolution des cyberattaques subies en 2022. Asterès en a déduit le coût moyen par cyberattaque réussie sur la base d'un coût journalier de la main d'œuvre de 364€[13]. Ce coût est calculé sur un échantillon équilibré entre acteurs privés et publics.

- **Le coût direct moyen estimé par Kaspersky Lab s'élève à 20 000€.** En 2015, Kaspersky Lab a conduit une enquête sur les risques cyber auprès de 5 500 entreprises dans 26 pays. Cette enquête a permis d'estimer le coût des « services professionnels » auxquels les entreprises font appel pour résoudre une crise cyber. Le coût en dollars a été traduit en euros par Asterès et actualisé en prenant en compte l'inflation. Comme Kaspersky distingue le coût pour les entreprises de moins de 1 500 salariés du coût pour les entreprises de plus de 1 500 salariés (il existe un rapport de 1 à 8 entre les deux coûts), Asterès a déduit le coût moyen pour les organisations toutes tailles confondues en calculant une moyenne pondérée[14]. Le chiffre final est également pondéré de la part des entreprises ayant recours à des services externes selon l'enquête (88%). Le fait que l'estimation de Kaspersky prenne uniquement en compte l'expertise externe peut expliquer en partie l'écart avec l'estimation d'Asterès.

3.2 COÛT DE LA RANÇON : 25 700€ PAR CYBERATTAQUE RÉUSSIE

Le coût moyen de la rançon est estimé à 25 700€ par cyberattaque réussie. Ce coût a été calculé à partir du montant moyen d'une rançon d'après les données du cabinet CoveWare auprès d'entreprises et la probabilité qu'une entreprise française paie une rançon d'après l'enquête Hiscox, en pondérant avec la répartition entre le public et le privé (voir annexe). Ce coût moyen recouvre une dispersion considérable entre les acteurs.

- **Le montant moyen d'une rançon pour une entreprise privée s'élève à 250 000€ selon le cabinet CoveWare**. Ce cabinet américain spécialisé dans la réponse aux attaques par

[13] Le coût horaire du travail est de 52€ dans le secteur « Information et communication » (source Insee). Asterès fait l'hypothèse que ce secteur représente l'essentiel de la main d'œuvre sollicitée pour résoudre une crise cyber. Aurélie Delaporte, « Le coût de la main-d'œuvre en France en 2020 : 38,7 euros par heure travaillée - Insee Focus - 283 », consulté le 8 mars 2023, https://www.insee.fr/fr/statistiques/6685426#graphique-figure2.

[14] Notons pour la suite que même si nous ne connaissons pas la taille moyenne des entreprises qui constituent la catégorie « moins de 1 500 », nous considérons qu'il s'agit principalement d'organisations de plus de 250 employés.

ransomware estime chaque trimestre le montant moyen des rançons à partir des données recueillies auprès de ses clients[15]. Le chiffre retenu correspond à la moyenne des quatre trimestres de l'année 2022, converti en euros par Asterès. Notons que le coût moyen d'une rançon a été multiplié par 43 depuis 2018 d'après l'historique de CoveWare[16]. D'autres cabinets ont récemment estimé le coût moyen d'une rançon mais Asterès ne les a pas retenu afin d'avoir une approche conservatrice. Ces estimations sont le fait de Unit 42[17], dont les résultats pour l'année 2020 sont deux fois plus élevés que ceux de CoveWare sans que cela puisse s'expliquer, et de Sophos[18], dont l'estimation est jugée moins robuste car réalisée à partir d'une enquête et non de cas réellement étudiés. L'enquête réalisée par Sophos nous renseigne néanmoins sur la dispersion des montants payés, qui varient, en appliquant les ratios issus de l'enquête de Sophos à la donnée de CoveWare, de 300€ à plus de 1,5 M€.

- **12% des cyberattaques conduisent au paiement d'une rançon d'après Hiscox**. Parmi les organisations ayant subi au moins une cyberattaque au cours des douze derniers mois, 19% ont été victimes d'une attaque par rançongiciel, dont 62% se sont résolues à payer.

3.3 COÛT DE L'INTERRUPTION D'ACTIVITÉ : 7 300€ PAR CYBERATTAQUE RÉUSSIE

Asterès estime que 216 heures de travail sont définitivement perdues en moyenne par cyberattaque réussie, ce qui équivaut à 7 300€. Cette perte a été déterminée à partir d'une estimation d'Accenture et du Ponemon Institute, en faisant l'hypothèse qu'une partie seulement n'était pas compensée par une augmentation temporaire de la charge de travail une fois la situation rétablie et en pondérant avec la répartition entre le public et le privé (voir annexe). Notons qu'il s'agit d'une moyenne qui couvre différentes tailles d'organisations. Dans l'hypothèse où les pertes sont proportionnelles au chiffre d'affaires, l'interruption d'activité équivaut en moyenne à 161 000€ pour les grandes entreprises.

- **Accenture et le Ponemon Institute évaluaient en 2018 à 17 500€ les pertes dues à l'interruption temporaire de l'activité.** Dans leur étude sur le coût de la cybercriminalité, Accenture et le Ponemon Institute définissent le coût induit par l'interruption d'activité (« *business disruption* ») comme « l'impact économique des *downtime* ou des pannes non planifiées qui empêchent l'organisation de répondre à ses exigences en matière de traitement des données »[19]. L'impact pour les entreprises françaises initialement calculé par Accenture et le Ponemon Institute a été converti en euros et actualisé par Asterès puis interprété comme un équivalent monétaire des heures de travail perdues en raison de la paralysie du système

[15] Exemple pour le Q1 2022 : « Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting », Coveware: Ransomware Recovery First Responders, 3 mai 2022, https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting.

[16] « Coveware's 2018 Q4 Ransomware Marketplace Report », Coveware: Ransomware Recovery First Responders, 22 janvier 2019, https://www.coveware.com/blog/2019/1/21/covewares-2018-q4-ransomware-marketplace-report.

[17] Unit 42, « 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner », *Unit 42* (blog), 24 mars 2022, https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/.

[18] « The State of Ransomware 2023 » (Sophos, mai 2023), https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.

[19] « The Cost of Cybercrime - Ninth annual cost of cybercrime study » (Accenture, Ponemon Institute, s. d.), https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf.

d'information. Asterès a ainsi estimé à 491 heures le volume de travail perdu, en faisant l'hypothèse d'un coût horaire du travail de 38,7€[20].

- **Asterès fait l'hypothèse que seulement 44% des pertes dues à l'interruption de l'activité sont définitivement perdues, le reste étant compensé par une augmentation temporaire de la charge de travail.** Cette hypothèse se fonde sur une enquête réalisée auprès de 18 000 managers et salariés canadiens qui conclut qu'en cas d'arrêt maladie dans une entreprise, 56% de la production du salarié en arrêt est compensée par ses collègues pendant son absence[21]. Asterès fait l'hypothèse qu'en cas d'interruption de l'activité à la suite d'une cyberattaque, la production rattrapée par les salariés une fois la situation rétablie devrait être au moins égale à la production assurée par les collègues d'un salarié en arrêt maladie.

Encadré 1. Comparaison du coût moyen avec la littérature

Le coût moyen pondéré obtenu par Asterès est proche du coût de 56 809€ par cyberattaque estimé par Accenture en 2018[22], mais bien inférieur au coût moyen d'une fuite de donnée (« *data breach* ») d'environ 4 millions d'euros estimé par IBM et le Ponemon Institute en 2022.

Outre le fait que l'étude d'IBM porte sur un sujet plus large que les cyberattaques (les fuites de données causées par des cyber-intrusions ou d'autres événements[23]), l'écart avec l'estimation d'Asterès peut s'expliquer par la taille des organisations interrogées. Même si peu de détails sont disponibles sur les caractéristiques des organisations composant l'échantillon de l'étude d'IBM (« *various sizes* »), celui-ci est probablement constitué en majorité d'entreprises de grandes tailles, un coût de 4 M€ représentant près de 10% du chiffre d'affaires d'une grosse PME / petite ETI. En outre, le coût de la perte d'activité calculé par IBM et le Ponemon Institute (« *lost business* ») prend en compte la perte de clients et la perte de réputation qu'Asterès a choisi de ne pas chiffrer. En effet, la perte des uns constituant le gain des autres, l'impact à l'échelle macroéconomique est nul.

[20] Il s'agit du coût horaire moyen de la main d'œuvre en France, tous secteurs et catégories d'entreprises confondues. Delaporte, « Le coût de la main-d'œuvre en France en 2020 : 38,7 euros par heure travaillée - Insee Focus - 283 ».

[21] Wei Zhang, Nick Bansback, et Aslam H. Anis, « Measuring and Valuing Productivity Loss Due to Poor Health: A Critical Review », *Social Science & Medicine* 72, nº 2 (janvier 2011): 185-92, https://doi.org/10.1016/j.socscimed.2010.10.026.

[22] Le coût par entreprise calculé par Accenture est très élevé mais les entreprises ont également rapporté subir en moyenne de 145 cyberattaques par an.

[23] L'étude d'IBM ne s'intéresse pas uniquement aux cybreattaques ayant pour conséquence une fuite de données mais également aux erreurs humaines et défaillances du système informatique.

4. CONCLUSION : UN COÛT DE 2 MDS€ POUR LES ORGANISATIONS

Le coût des cyberattaques réussies pour les organisations privées et publiques françaises est estimé par Asterès à 2,0 Mds€ en 2022. Pour rappel, cette estimation ne prend en compte que les ETI, grandes entreprises et les organisations publiques de taille équivalente. Il s'agit d'un coût global comprenant des réalités différentes selon le type d'intrusion, la taille de l'organisation ou encore le secteur d'activité. Le coût de la cyberattaque la plus significative en 2022 pourrait ainsi se situer autour de 10 M€, si l'on applique le ratio coût maximal / coût médian obtenu dans l'enquête Hiscox pour l'Allemagne[24]. Dans l'ensemble, le secteur privé représente trois quarts du coût des cyberattaques en France et le secteur public un quart. Le coût direct et le coût des rançons représentent chacun 44% du coût total, tandis que les pertes de production y contribuent pour 12% (voir *graphique 4*) :

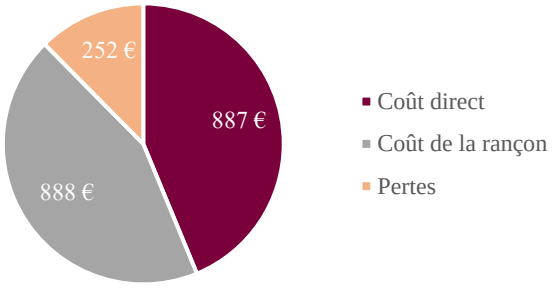
- **Le coût direct des cyberattaques réussies est estimé à 887 M€ en 2022**, ce qui se matérialise par des pertes de productivité et une hausse des coûts de production. Ces ressources auraient pu être investies dans la transformation numérique et ainsi générer des gains de productivité à court, moyen et long terme. Au lieu de cela, les organisations voient leur coût de production augmenter, ce qui, dans le cas du secteur marchand, peut être répercuté sur les prix (dans le cas des fuites de données, 60% des entreprises déclarent augmenter leurs prix conséquemment à une cyberattaque[25]) et dans le cas du secteur public implique des baisses de qualité ou des hausses de dépenses publiques.

- **Le coût des rançons est estimé à 888 M€ en 2022**. Comme pour le coût direct, les rançons limitent la productivité à terme et augmentent les coûts de production. Seulement, les rançons ont en plus un effet sur la balance des paiements, puisqu'une partie conséquente est probablement réglée à l'étranger, et sur l'économie du crime, puisque ces rançons sont réglées à des organisations cybercriminelles. Leur impact est donc particulièrement néfaste pour l'économie française.

- **Les pertes de production sont estimées à 7 millions d'heures de travail, soit un équivalent monétaire de 252 M€.** Asterès estime qu'il s'agit d'une perte de productivité de l'ordre de 0,02%[26]. Dans le secteur privé, le consommateur subit peu d'effets si le secteur est concurrentiel. Ainsi, il ne s'agit pas nécessairement d'une perte à l'échelle macroéconomique : un client perdu pour une entreprise peut constituer un nouveau client pour une entreprise concurrente. Dans le secteur public, la conséquence peut être une baisse de satisfaction pour les citoyens, en raison du dysfonctionnement d'un service ou du délai allongé pour le traitement d'une demande, ou d'une hausse des dépenses à terme.

[24] « Hiscox Cyber Readiness Report 2022 | Hiscox Group », 8 juin 2023, https://www.hiscoxgroup.com/cyber-readiness.
[25] « Cost of Data Breach - Report 2022 » (IBM Security, s. d.), https://www.ibm.com/downloads/cas/3R8N1DZJ.
[26] 0,36 heures perdues par salarié en moyenne (1,8 cyberattaque par organisation et une taille moyenne de 1 000 employés), sur un total 1 561 heures travaillées (253 jours ouvrés, 30 jours de vacances, 7 heures par jour).

Graphique 4. Ventilation du coût des cyberattaques en France, par type de coût, en M€

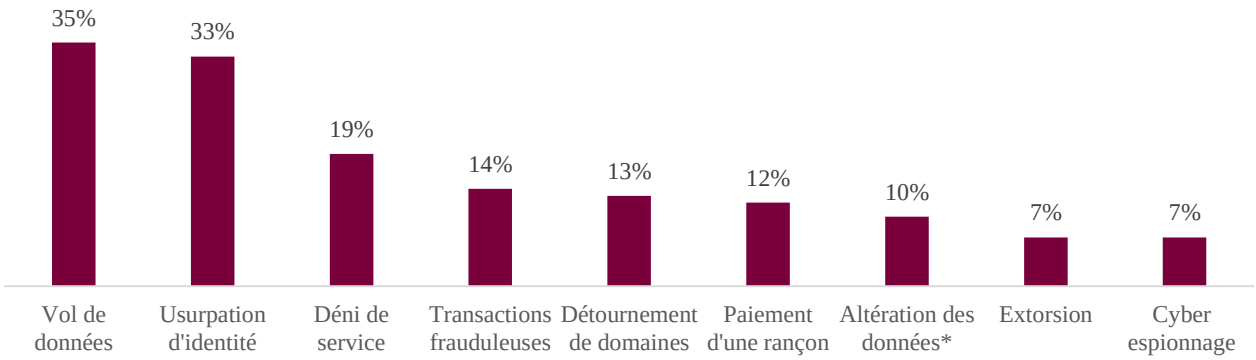


Sources : voir parties 2 et 3.

ANNEXE

CONSÉQUENCES LES PLUS FRÉQUENTES

Graphique 5. Principales conséquences des cyberattaques selon le CESIN et Hiscox.



Sources : CESIN et Hiscox

CALCUL DU VOLUME DE CYBERATTAQUES

Le volume de cyberattaques en France en 2022 a été obtenu en extrapolant les données sur la fréquence des cyberattaques par type d'organisation à la démographie des organisations publiques et privées françaises (voir tableau 1). Les données démographiques proviennent de l'Insee pour les entreprises[27], de la Drees pour les établissements de santé publics et privés[28], de l'AMF pour les communes[29], de la Direction générale des collectivités locales (DGCL) pour les régions et départements[30], de Campus France pour les établissements d'enseignement supérieur[31], et des sites des ministères de tutelle pour les établissements publics administratifs (EPA) et à caractère industriel et commercial (EPIC). Pour ces derniers, Asterès ne prétend pas à l'exhaustivité. Certaines données ne sont pas complètement à jour

[27] « Caractéristiques des entreprises par catégorie | Insee », consulté le 2 juin 2023, https://www.insee.fr/fr/statistiques/2016091.
[28] « Les établissements de santé - édition 2022 | Direction de la recherche, des études, de l'évaluation et des statistiques », consulté le 2 juin 2023, https://drees.solidarites-sante.gouv.fr/publications-documents-de-reference-communique-de-presse/panoramas-de-la-drees/les-etablissements#footnote1_x94xz3h.
[29] AMF Association des maires de France et des présidents d'Intercommunalités, « Statistiques », Association des Maire de France et des présidents d'intercommunalité de France - AMF, consulté le 2 juin 2023, https://www.amf.asso.fr/page-statistiques/36010.
[30] « Chapitre 1 - Les chiffres clés des collectivités-2022.xlsx », consulté le 2 juin 2023, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.collectivites-locales.gouv.fr%2Ffiles%2FAccueil%2FDESL%2F2022%2FColloc%2520en%2520chiffres%2FChiffres%2520clef%2FChapitre%25201%2520-%2520Les%2520chiffres%2520cl%25C3%25A9s%2520des%2520collectivit%25C3%25A9s-2022.xlsx&wdOrigin=BROWSELINK.
[31] « Établissements d'enseignement supérieur en France », Campus France, consulté le 2 juin 2023, https://www.campusfrance.org/fr/etablissements-enseignement-superieur-France.

pour l'année 2022 (notamment pour les entreprises) et Asterès a fait le choix conservateur de ne pas prédire leur évolution à court terme.

Tableau 1. Calcul du volume de cyberattaques en France, par type d'organisation

	Nombre total d'organisations	Dont victimes de cyberattaque (s)	Nombre total de cyberattaques en 2022
Entreprises (hors microentreprises)	154 189	80 800	347 441
Dont PME	148078	76 852	330 466
Dont ETI	5841	3 773	16 225
Dont GE	270	174	750
Collectivités territoriales/locales	18 052	5 096	21 911
Dont régions	18	8	35
Dont départements	101	45	195
Dont communes > 10 000 hab.	1 018	458	1 970
Dont communes de 500 à 9 999 hab.	16 915	4 584	19 711
Établissements de santé	2989	1 744	7 498
Dont public	1347	683	2 937
Dont privé	1642	1 061	4 561
Établissements d'enseignement supérieur	3500	1 775	7 630
Autres établissements publics	122	62	266
Dont EPIC	51	23	99
Dont EPA	71	32	137
Ministères	15	8	33
Total	178 867	89 483	384 779

Note : Les résultats de la modélisation d'Asterès sont présentés ici par souci de transparence mais ne doivent pas être interprétés comme valables à l'unité près. Il s'agit avant tout d'estimer un ordre de grandeur.

CALCUL DES RATIOS PAR SECTEUR

Les différences de coût entre le public et le privé ont pu être prises en compte grâce aux données sectorielles d'Accenture et du Ponemon Institute[32]. Ces données datent de 2018 mais Asterès fait l'hypothèse que les ratios demeurent les mêmes en 2022 (voir *tableau 2*). Asterès considère ainsi que le coût pour le secteur privé s'élève à 103% du coût moyen, le coût pour le secteur public (hors administration centrale) à 60% du coût moyen et le coût pour l'administration centrale (c'est-à-dire les ministères) à 104% du coût moyen. Notons que les services publics (« *utilities* » en anglais), qui rentrent dans la catégorie des EPIC en France, n'ont pas été pris en compte en raison de leur très faible nombre.

[32] « The Cost of Cybercrime - Ninth annual cost of cybercrime study ».

Tableau 2. Le coût moyen de la cybercriminalité par secteur, selon Accenture

	Ent. dans l'échantillon	Pourcentage	Coût moyen
Banque	40	11%	$ 18,4
Détail	35	10%	$ 11,4
High Tech	30	8%	$ 14,7
Santé	23	6%	$ 11,8
Voyage	23	6%	$ 8,2
Assurance	20	6%	$ 15,8
Énergie	18	5%	$ 13,8
Logiciel	18	5%	$ 16,0
IT	16	5%	$ 9,2
Biens de consommation	15	4%	$ 11,9
Sciences du vivant	14	4%	$ 10,9
Services publics	13	4%	$ 17,8
Marché des capitaux	12	3%	$ 13,9
Automobile	11	3%	$ 15,8
Secteur public	27	8%	$ 7,9
Gouvernement fédéral	20	6%	$ 13,7
Moyenne pondérée			$ 13,2
Moyenne privé			$ 13,7

Source : Accenture, *The cost of cybercrime*

BIBLIOGRAPHIE

Campus France. « Établissements d'enseignement supérieur en France ». Consulté le 2 juin 2023. https://www.campusfrance.org/fr/etablissements-enseignement-superieur-France.

« Caractéristiques des entreprises par catégorie | Insee ». Consulté le 2 juin 2023. https://www.insee.fr/fr/statistiques/2016091.

« Chapitre 1 - Les chiffres clés des collectivités-2022.xlsx ». Consulté le 2 juin 2023. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.collectivites-locales.gouv.fr%2Ffiles%2FAccueil%2FDESL%2F2022%2FColloc%2520en%2520chiffres%2FChiffres%2520clef%2FChapitre%25201%2520-%2520Les%2520chiffres%2520cl%25C3%25A9s%2520des%2520collectivit%25C3%25A9s-2022.xlsx&wdOrigin=BROWSELINK.

« Cost of Data Breach - Report 2022 ». IBM Security, s. d. https://www.ibm.com/downloads/cas/3R8N1DZJ.

Coveware: Ransomware Recovery First Responders. « Coveware's 2018 Q4 Ransomware Marketplace Report », 22 janvier 2019. https://www.coveware.com/blog/2019/1/21/covewares-2018-q4-ransomware-marketplace-report.

Coveware: Ransomware Recovery First Responders. « Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting », 3 mai 2022. https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting.

Delaporte, Aurélie. « Le coût de la main-d'œuvre en France en 2020 : 38,7 euros par heure travaillée - Insee Focus - 283 ». Consulté le 8 mars 2023. https://www.insee.fr/fr/statistiques/6685426#graphique-figure2.

Delattre, Laurent. « Cybersécurité, le CESIN souligne une légère baisse des attaques réussies en 2022 ». *IT for Business* (blog), 1 février 2023. https://www.itforbusiness.fr/cybersecurite-le-cesin-souligne-une-legere-baisse-des-attaques-reussies-en-2022-59399.

Dieye, Rokhaya, Ahmed Bounfour, Altay Ozaygen, et Niaz Kammoun. « Estimates of the Macroeconomic Costs of Cyber-attacks ». *Risk Management and Insurance Review* 23, nº 2 (juin 2020): 183-208. https://doi.org/10.1111/rmir.12151.

« Hiscox Cyber Readiness Report 2022 | Hiscox Group », 8 juin 2023. https://www.hiscoxgroup.com/cyber-readiness.

Intercommunalités, AMF Association des maires de France et des présidents d'. « Statistiques ». Association des Maire de France et des présidents d'intercommunalité de France - AMF. Consulté le 2 juin 2023. https://www.amf.asso.fr/page-statistiques/36010.

« Les établissements de santé - édition 2022 | Direction de la recherche, des études, de l'évaluation et des statistiques ». Consulté le 2 juin 2023. https://drees.solidarites-sante.gouv.fr/publications-documents-de-reference-communique-de-presse/panoramas-de-la-drees/les-etablissements#footnote1_x94xz3h.

« Panorama de la cybermenace 2022 ». Agence nationale de la sécurité des systèmes d'information, 24 janvier 2023. https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/.

« The Cost of Cybercrime - Ninth annual cost of cybercrime study ». Accenture, Ponemon Institute, s. d. https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf.

« The State of Ransomware 2023 ». Sophos, mai 2023. https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.

Unit 42. « 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner ». *Unit 42* (blog), 24 mars 2022. https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/.

Zhang, Wei, Nick Bansback, et Aslam H. Anis. « Measuring and Valuing Productivity Loss Due to Poor Health: A Critical Review ». *Social Science & Medicine* 72, nº 2 (janvier 2011): 185-92. https://doi.org/10.1016/j.socscimed.2010.10.026.

CHARTE ETHIQUE

Asterès est régulièrement sollicité par des entreprises et des fédérations professionnelles pour intervenir en amont de leurs activités de lobbying, particulièrement lors des débats d'orientation budgétaire. Asterès peut donc être amené à réaliser des travaux financés par des donneurs d'ordres et démontrant l'impact d'une mesure qui pourrait leur être appliquée.

Dans ce cas, notre démarche répond à une charte éthique stricte. Notre client s'engage à accepter que les travaux menés par Asterès répondent aux principes intangibles suivants :

- Asterès ne peut s'engager sur les résultats d'une étude avant de l'avoir réalisée. Nous ne délivrons nos conclusions qu'au terme de nos analyses.
- Nos travaux suivent une méthodologie standard qui s'appuie sur l'utilisation de données statistiques publiques, ou conçues par nous-mêmes.
- Si un client souhaite modifier des conclusions de travaux réalisés par Asterès sans une totale approbation de nos consultants, il devient le seul signataire de l'étude, et n'a plus le droit d'utiliser la marque Asterès.
- Les consultants d'Asterès ne défendent dans le débat public que des travaux qu'ils ont réalisés eux-mêmes. En aucun cas ils n'acceptent de se faire le relais de travaux réalisés par d'autres.

ASTERÈS
études, recherche & conseil économique

ASTERES ETUDES & CONSEIL

81 rue Réaumur,

75002 PARIS 01 44 76 89 16

contact@asteres.fr