WAVESTONE

COMMUNIQUE DE PRESSE *Paris, le 18 avril 2023*

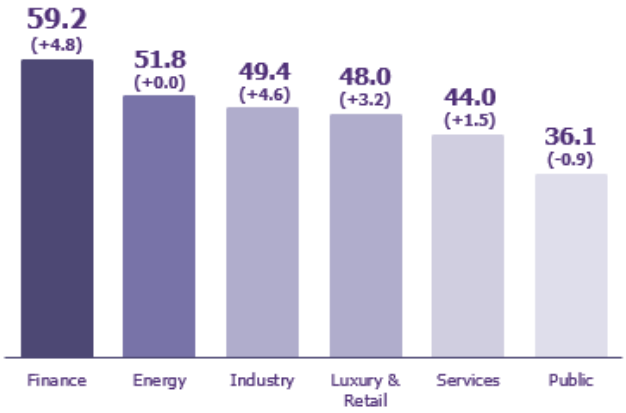
Maturité cyber en France : une progression notable dans les grandes organisations qui se ressent sur la réussite des attaques cyber

- Un niveau de maturité des grandes organisations encore faible (**49%**) mais qui connait une amélioration (**+3 points**)
- **23%** des grandes organisations évaluées restent très fragiles aux risques d'attaque par *ransomware*, contre **30%** l'an dernier.
- Les budgets cyber représentent **5,6% du budget IT** tous secteurs confondus, dans le bas de la fourchette recommandée (entre 5 et 10%).
- **1 expert** est dédié à la cybersécurité **pour 1300 employés** en moyenne, ce qui représente une amélioration de **11%** par rapport à l'an dernier malgré les difficultés de recrutement.
- La capacité de **reconstruction à la suite d'une attaque reste le sujet le plus complexe à traiter** (**43%** de maturité).
- Certains domaines clés de la cybersécurité restent en souffrance, en particulier la **sécurité des tiers** (partenaires, fournisseurs… de plus en plus interconnectés) **à 46.9%** de maturité, la **sécurité du *Cloud* à 44.0%** et celle des **systèmes industriels 37.6%.**

Alors que les cyberattaques se multiplient (criminalité, hacktivisme, état) - encore plus dans un climat géopolitique bouleversé - les entreprises françaises doivent toujours accélérer leur transformation numérique. Dans ce contexte, quel est le niveau de sécurité des différents secteurs en France ? Quelles sont les forces et faiblesses des grandes organisations en matière de cybersécurité ?

Pour répondre à ces questions, le cabinet de conseil Wavestone a réalisé un benchmark détaillé et basé sur une évaluation terrain de près de 200 mesures de sécurité. Depuis 3 ans, les données de plus de 100 organisations, représentant près de 5 millions d'utilisateurs, ont été consolidées et analysées. Les résultats illustrent le long chemin restant à parcourir pour les grandes organisations, mais aussi une progression sensible, puisque celles-ci obtiennent un score global de maturité de 49% contre 46% l'an dernier, le score étant relatif aux exigences des normes internationales NIST CSF Framework & ISO 27001/2.

Avec une progression de 3% : les investissements en cybersécurité commencent à se faire sentir



Le niveau de maturité général est en hausse atteignant **49%**, l'étude révèle néanmoins une hétérogénéité en fonction des secteurs. Celui de **la Finance** tire son épingle du jeu avec un score de **59,2 % en progression de 4.8 points depuis 2022**. Ce résultat s'explique par les investissements conséquents et historiques réalisés dans ce secteur, encouragés par les réglementations. Le secteur de **l'Industrie suit la progression (4.6 points)** montrant les efforts effectués pour rattraper leur retard en menant leur transformation numérique. Celui des **Services (44%)** avec le **Public (36,1%) ferme la marche**. Ces derniers, bien que conscients des risques, peinent à identifier les financements nécessaires. Avec un score de **51,8%,** le secteur de **l'Energie** reste légèrement au-dessus de la moyenne.

Les entreprises soumises aux réglementations sur la sécurité des infrastructures critiques (NIS/LPM) se démarquent et sont plus matures (56,1% VS 46,4%).

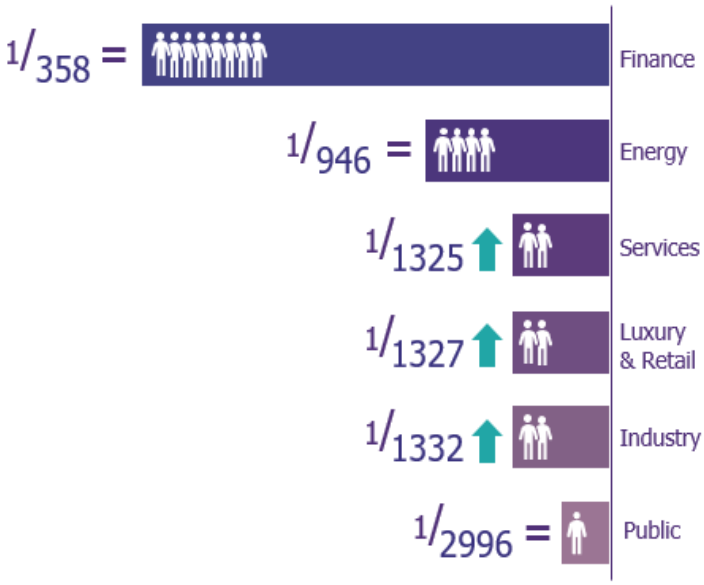
Face aux risques d'une attaque par ransomware, 23% des organisations sont dans une situation à risque, c'est 7 points de moins que l'an dernier.

Wavestone gère de nombreuses cyberattaques pour le compte de ses clients grâce à son équipe de réponse à incident le **CERT-Wavestone**. Les principales failles utilisées par les cybercriminels ont été identifiées et une analyse particulière de la maturité a été réalisée. De cette analyse ressort que :

- **23%** des organisations restent **très fragiles** aux risques **d'attaque par ransomware**. Ce phénomène touche surtout les secteurs des services et le secteur public même si certains acteurs financiers ou industriels ne sont pas à l'abri.
- Les **très grandes organisations** (type CAC40, FTSE100 ou celles qui ont plus de 100k employés), du fait de leur niveau de maturité proche des **60%**, sont des cibles moins faciles.

Cette progression se ressent sur le terrain où l'on observe une diminution des attaques sur les grandes structures, en réalité les tentatives d'attaques ont toujours lieu mais elles ont pu être détectées et interrompues avant de générer trop de dégâts.

Les effectifs restent le nerf de la guerre…

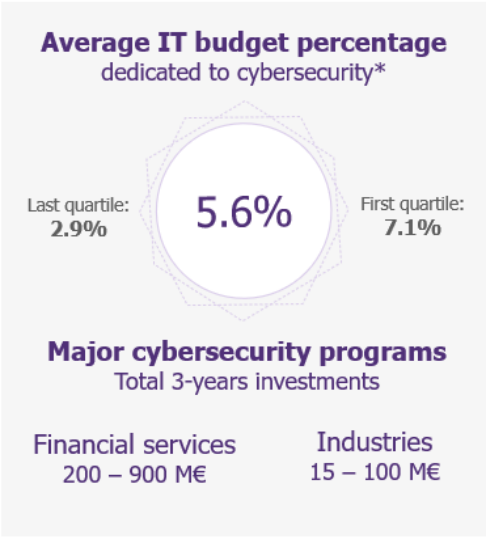


En France, comme à l'échelle mondiale, la cybersécurité fait face à une pénurie de talents constante : plus de **15 000 postes** sont disponibles mais non couverts. Les grandes entreprises tentent d'inverser la courbe et renforcent de plus en plus leurs équipes mais les écarts sont importants en fonction de la maturité digitale des secteurs.

En ce qui concerne les **effectifs dans les organisations évaluées, il y a environ 1 personne dédiée à la cybersécurité pour 1300 employés**, un chiffre trop faible pour faire face aux enjeux actuels. Les disparités sectorielles sont sur ce thème encore plus marquées.

… autant que les investissements financiers dédiés

Sur le budget informatique global des entreprises, **5,6% est dédié à la sécurité**. Un nombre qui peut paraître faible à première vue, mais qui augmente significativement en cas d'attaque cyber pour avoisiner les 15%.



Gérôme BILLOIS, Associé en charge de l'activité cybersécurité de Wavestone, ajoute d'ailleurs que « *la matérialisation d'une crise permet une mobilisation à haut niveau du coté exécutif ; elle engendre également les mécaniques permettant des niveaux d'investissements très forts* ».

D'un point de vue sectoriel, ceux qui investissent le plus sont les Services Publics (6,6%), l'Industrie (6%) et le Luxe & Retail (6%). Le retard à rattraper est plus important dans ces secteurs et la prise de conscience, plus tardive, montre aujourd'hui ses effets. À l'inverse de l'Énergie (5,5%), de la Finance (5,4%) et des Services (4.5%). Il est à noter que la finance a largement investi les années précédentes et qu'elle dispose de budgets informatiques sans commune mesure avec les autres secteurs d'activité.

De nombreux challenges à relever pour les entreprises françaises

- Sur les axes stratégiques de la cybersécurité, on observe une **homogénéité des piliers NIST (identifier les risques, protéger, détecter, réagir)** avoisinant les **50%** sur l'ensemble des thèmes. **Toutefois, la résilience à la suite d'une attaque reste le parent pauvre, à 43% de maturité.**
- Sur le sujet de la **résilience**, nous observons **un marché à deux vitesses**, séparant le secteur financier du reste des organisations, pourtant les risques sont bien présents et tous sont concernés.

- Alors que **70%** des **entreprises du secteur financier** revoient régulièrement leurs **risques résiduels** au niveau de leur **Plan de Traitement des Risques (PTR),** seulement **28%** des **entreprises des autres secteurs** font de même.
- Sur la **gestion des incidents** de sécurité, **60%** améliorent **continuellement** leur processus et possèdent différents plans de cyber-réponse en fonction des scénarios, contre seulement **40%** des **entreprises en dehors de la finance**.
- Au niveau des **tiers**, **25%** des **entreprises en finance** ont mis en place un processus pour **auditer régulièrement** leurs fournisseurs, en fonction de leur criticité, contre seulement **11%** pour les **entreprises des autres secteurs.**
- Mais le plus marquant reste le fait que **55%** des **entreprises financières** testent **tous les scénarios** du **PCA** au moins tous **les deux ans** (la réglementation **DORA** demandant de le faire **tous les ans**). Au niveau des **entreprises non financières**, seulement **9%** effectuent ces tests.

- Le **Zero Trust** est l'un des enjeux majeurs de ces prochaines années en cybersécurité. Bien qu'en plein déploiement, il nous a semblé clé de faire zoom dessus :
  - **24%** des organisations ont mis en place une **micro segmentation** automatique (e.g.: Illumino) en fonction de l'exposition, de la sensibilité, de l'environnement, etc. déployé à hauteur de **32%** en moyenne.
  - **14%** des organisations ont mis en place du **Zero Trust Network Access** basé sur l'identité pour leurs environnements *Cloud*, déployé à hauteur de **46%** en moyenne.
  - **28%** des organisations prennent en compte la **sensibilité des ressources** et le **contexte de connexion** et ont déployé une **authentification multifacteurs** (MFA) avec **accès conditionnel**, déployé à hauteur de **73%** en moyenne.
  - **13%** des organisations ont commencé à déployer un **SOAR** permettant **d'isoler les ressources** lors de la détection d'une **alerte**, déployé à hauteur de **48%** en moyenne.

- Le ***Cloud*** est un sujet clé concentrant des investissements importants atteignant maintenant **44.5%** de maturité, contre seulement **36.1%** l'an dernier. La progression la plus importante se fait au niveau de **l'administration *Cloud*** : entre 2022 et 2023, **14%** des organisations ont mis en place une authentification multi-facteurs (code en plus du mot de passe) ou un **bastion** (rebond intermédiaire) pour l'accès aux actions d'**administrations *Cloud***. Au sujet de la surveillance, en 2022, **42%** des entreprises comptaient **uniquement** sur les alertes de leur fournisseur *Cloud*, ils ne sont plus que **38%** en 2023. Enfin, nous avons maintenant **70%** des organisations qui disent **vérifier** automatiquement la **conformité du *Cloud* à l'aide d'outils ;** uniquement **11% corrigent** cependant automatiquement les **problèmes** de conformité du *Cloud*.

- **Dans le secteur de l'industrie, la plus grande problématique reste la sécurité des systèmes d'information industriels (37.9% de maturité).** Des systèmes historiques ont été conçus sans sécurité par défaut et s'ouvrent désormais du fait de la transformation numérique. Les efforts pour mettre en place une gouvernance se poursuivent (71% contre 50% en 2022) et les travaux d'isolation continuent (86% contre 78% en 2022) mais sont souvent difficiles à mener jusqu'au bout. De plus ces périmètres sont toujours aujourd'hui très peu surveillés (37%) même si on observe une amélioration (+8 points).

« De manière instinctive, on pense que le Cloud est sécurisé. C'est vrai pour ce qui est de la responsabilité des fournisseurs, mais beaucoup d'actions restent de la responsabilité des organisations utilisatrices… et sont malheureusement souvent oubliées ! C'est un point majeur pour la sécurité des nouvelles applications », déclare Gérôme BILLOIS.

Méthodologie de l'étude

Les niveaux de maturité ont été mesuré par rapport aux référentiels internationaux (NIST CSF / ISO 27001/2) lors de missions d'évaluation réalisés par des consultants de Wavestone, majoritairement sous forme d'entretiens déclaratifs avec les responsables sécurité des organisations concernées. L'échantillon, datant du 1 avril 2023, regroupe plus de 100 organisations (dont une majorité avec plus de 10 000 employés et 30 groupes du Tier1 : organisations du CAC40, du FTSE100, ou avec plus de 100k employés) ce qui représentent près de 5 millions de collaborateurs en France. Les données issues de ces évaluations individuelles ont ensuite été consolidées et analysées par les équipes de spécialistes de Wavestone.

Notre expert, Gérôme Billois se tient à votre disposition pour vous commenter les résultats de l'étude et apporter son analyse sur le sujet.

Gérôme BILLOIS, Partner au sein du cabinet Wavestone, a près de 20 ans d'expérience dans le conseil en cybersécurité et gestion des risques numériques. Il est diplômé de l'Institut national des Sciences appliquées de Lyon. Depuis 2001, il a piloté de nombreux projets pour des grands comptes internationaux incluant la définition de stratégie cyber sécurité pour permettre une transformation numérique en toute confiance et le pilotage de programmes de lutte contre la cybercriminalité. Il a animé et participé à des cellules de gestion de crise suite à des cyberattaques. Il anime également des conférences et donne des cours dans les grandes écoles (INSA, Télécom Sud Paris...).

A propos de Wavestone

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. Une ambition ancrée dans l'ADN du cabinet et résumée par la signature « The Positive Way ».

Wavestone rassemble 4 000 collaborateurs en Europe, aux Etats-Unis et en Asie et se distingue parmi les leaders indépendants du conseil.

Wavestone est coté sur Euronext à Paris, labellisé Great Place To Work® et figure parmi les meilleurs cabinets de conseil au monde dans le classement Forbes 2022.

Plus d'informations sur www.wavestone.com // @wavestoneFR

Wavestone

Mélodie LAUQUE

press@wavestone.com

Wellcom PR Agency

Chloé Bencivengo

chloe.bencivengo@wellcom.fr

Marie-Charlotte Fauquette

mariecharlotte.fauquette@wellcom.fr

Bastien Depond

bastien.depond@wellcom.fr

Tel. : + 33 1 46 34 60 60