WAVESTONE

Quel bilan de maturité cybersécurité dans les rapports annuels du CAC 40 ?

Juin 2018

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
+33 (0)6 10 99 00 60
@gbillois

Alexandre LUKAT
Senior Consultant
alexandre.lukat@wavestone.com
+33 (0)6 72 58 26 52

Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders dans leur secteur

2 800 collaborateurs sur 4 continents

Parmi les leaders du conseil indépendant en Europe, n°1 en France

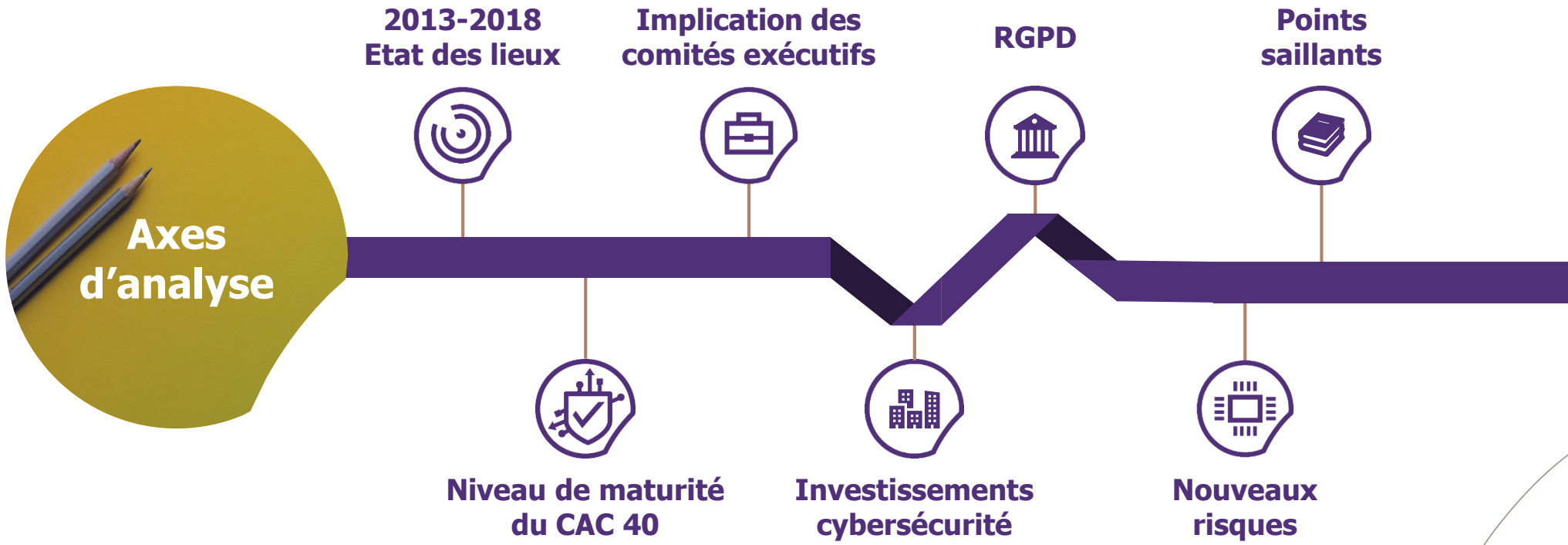
Paris | Londres | New York | Hong Kong | Singapour* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milan* | Bruxelles | Genève | Casablanca | Istanbul*
Lyon | Marseille | Nantes

* Partenariats

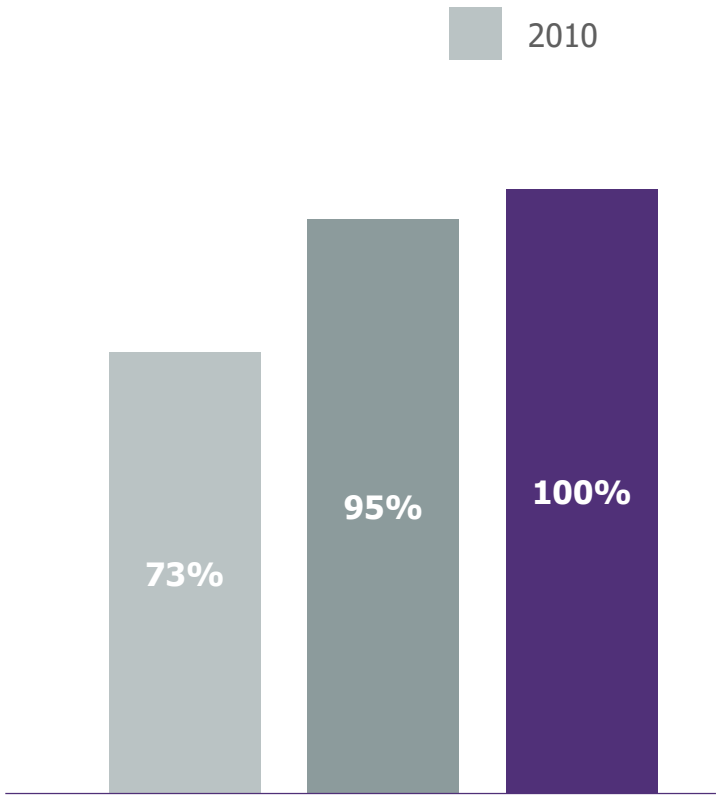
Quelle maturité en cybersécurité pour le CAC 40 ?

Méthodologie : cette étude repose sur une analyse factuelle des derniers rapports annuels et documents de référence, publiés au 01/06/2018 par les entreprises du CAC 40.

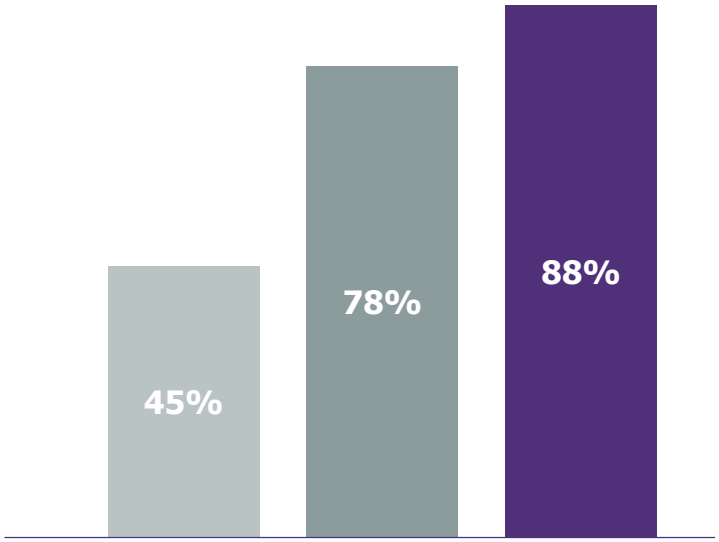
L'analyse se fonde uniquement sur les éléments présentés dans ces documents. Il est à noter que ceux-ci ne reflètent pas toujours l'exhaustivité des actions menées sur le terrain.



Enfin 100% des entreprises du CAC 40 se mobilisent sur le sujet cyber

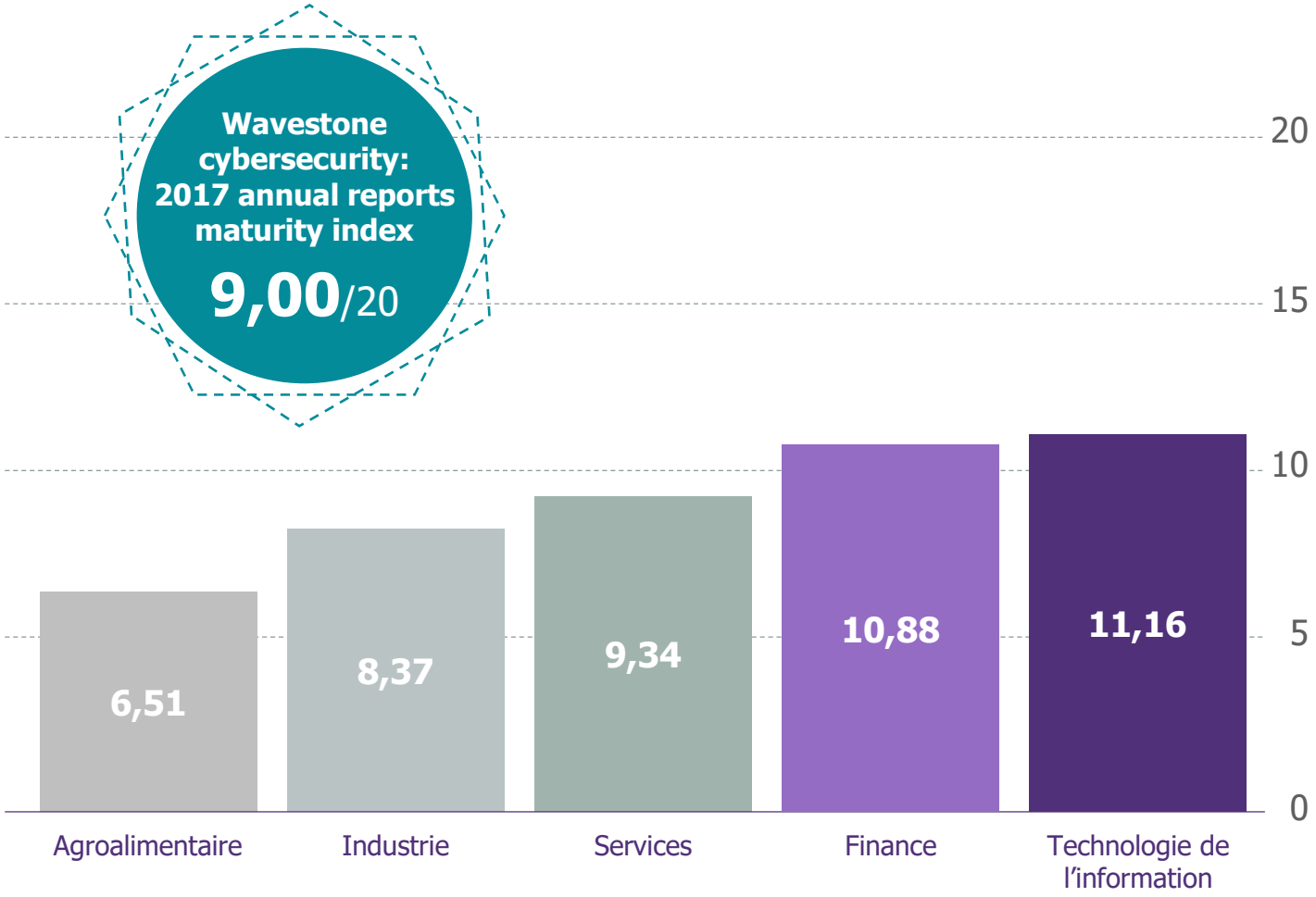


Mentions des enjeux de sécurité du SI



Mentions de la mise en place d'actions de couverture du risque

Les secteurs des technologies de l'information et de la finance se démarquent



Wavestone cybersecurity: 2017 annual reports maturity index

Le *Wavestone cybersecurity: annual reports maturity index* permet d'apprécier le niveau de maturité des entreprises, à partir des éléments contenus dans leur document de référence. Cet indice, exprimé sur 20 points, se base sur 14 critères pondérés et notés entre 0 et 2. Ces critères* concernent les thématiques suivantes :

Enjeux et risques
Enjeux cyber, risques et impacts cyber, souscription d'une cyberassurance, sécurisation de la transformation numérique et des nouvelles technologies.

Gouvernance et règlementation
Implication du comité exécutif, gouvernance SSI, protection des données à caractère personnel, sensibilisation et formation, transparence vis-à-vis des incidents de sécurité, réglementations et respect des normes.

Protection et contrôle
Mise en place de plan d'actions, de programme de cybersécurité, sécurisation des systèmes métier, audit et contrôle.

**La grille d'évaluation complète est précisée en annexes.*

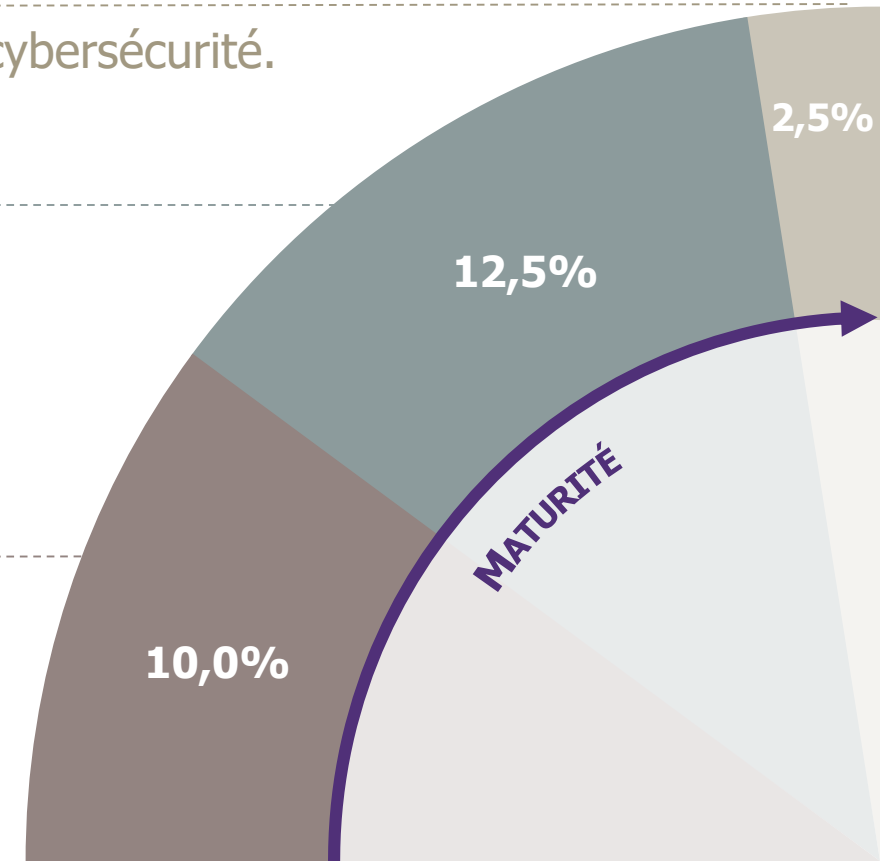
Les comités exécutifs de plus en plus impliqués

25% des groupes du CAC 40 adressent la problématique de la cybersécurité au niveau du comité exécutif.

Un membre du comité exécutif est mobilisé sur la cybersécurité.

Une instance régulière avec le comité exécutif adresse la cybersécurité.

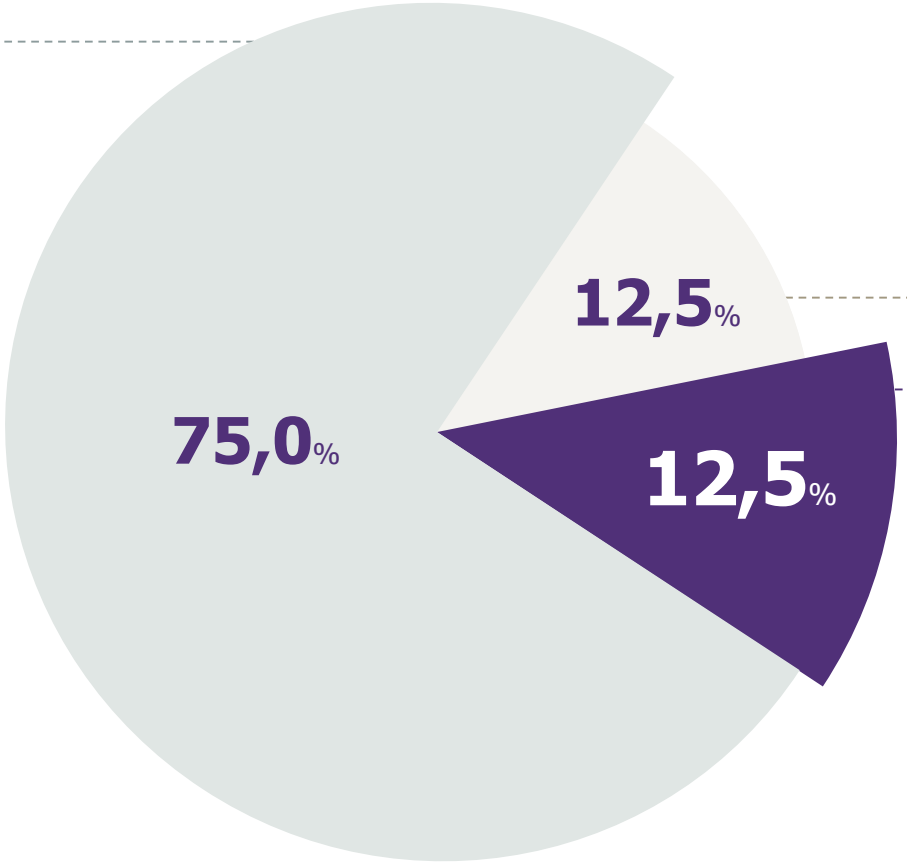
La cybersécurité est intégrée à la stratégie d'entreprise.



Des investissements morcelés et à des niveaux hétérogènes

Plans d'actions unitaires

Il est fait mention de plans d'actions mis en œuvre afin de déployer des mesures de sécurité.



Aucune mention

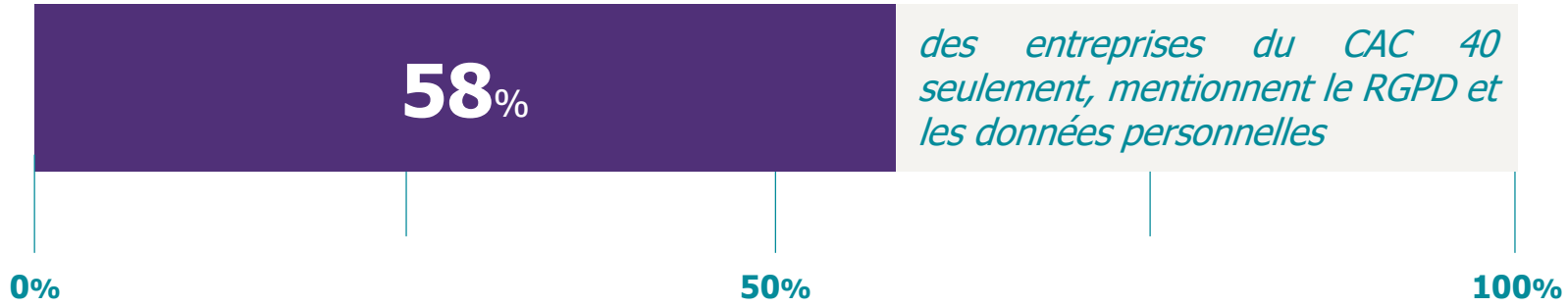
Les rapports ne mentionnent aucun investissement spécifique sur le risque cyber.

Programmes de cybersécurité

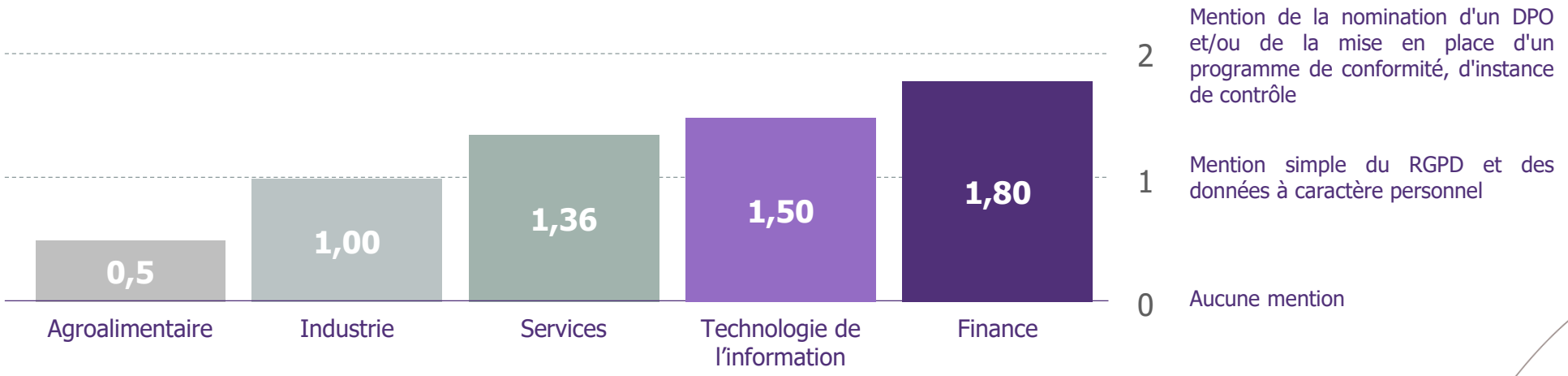
Des programmes de sécurité impliquant des investissements conséquents sont mentionnés.

Aucun groupe du CAC 40 ne mentionne le niveau d'investissement mais Wavestone a observé sur le marché des programmes de cybersécurité allant de 50 M€ à 900 M€. Les plans d'actions unitaires sont chacun de l'ordre de quelques M€.

RGPD* et données à caractère personnel : la surprise de l'analyse ?



Le niveau de maturité du CAC 40 à nouveau tiré par les secteurs de la **finance** et des **technologies de l'information**.



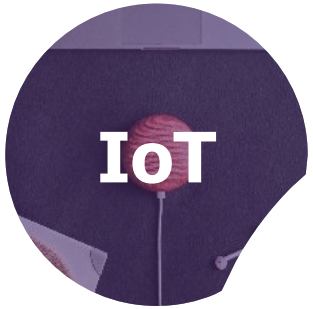
*RGPD : règlement général sur la protection des données à caractère personnel

Des innovations technologiques qui oublient la cybersécurité

46% *des entreprises du CAC 40 mentionnent lancer des projets IA*

0% 50% 100%

0 font le lien avec la cybersécurité



35% *des entreprises du CAC 40 mentionnent lancer des projets IoT*

0% 50% 100%

5 seulement font le lien avec la cybersécurité

28% *des entreprises du CAC 40 mentionnent lancer des projets liés à la blockchain*

0% 50% 100%

0 font le lien avec la cybersécurité

Des points saillants observés dans les rapports

LA SENSIBILISATION SORT DES MURS DE L'ENTREPRISE

En complément de clauses contractuelles cybersécurité habituelles, quelques pionniers lancent des initiatives de sensibilisation et de formation envers leurs fournisseurs, partenaires ou sous-traitants.

Des pratiques à encourager car elles amplifient la sensibilisation de l'ensemble du tissu économique, en particulier les PME et ETI, qui sont fournisseurs des grands groupes.

DES RISQUES MÉTIER INTÉGRANT LA CYBERSÉCURITÉ

La numérisation de l'économie transparait dans les risques cyber avec des risques métier spécifiques de plus en plus mentionnés :

- industrie 4.0 ;
- voiture autonome ;
- vie privée et IoT ;
- fraude dans les services financiers ;
- piratage de contenu audiovisuel.

L'ISO 27001, SEULE CERTIFICATION D'ENTREPRISE EN CYBERSÉCURITÉ

Quatre membres du CAC 40 sont certifiés sur certains périmètres et cinq s'inspirent de ces normes internationales sur la cybersécurité.

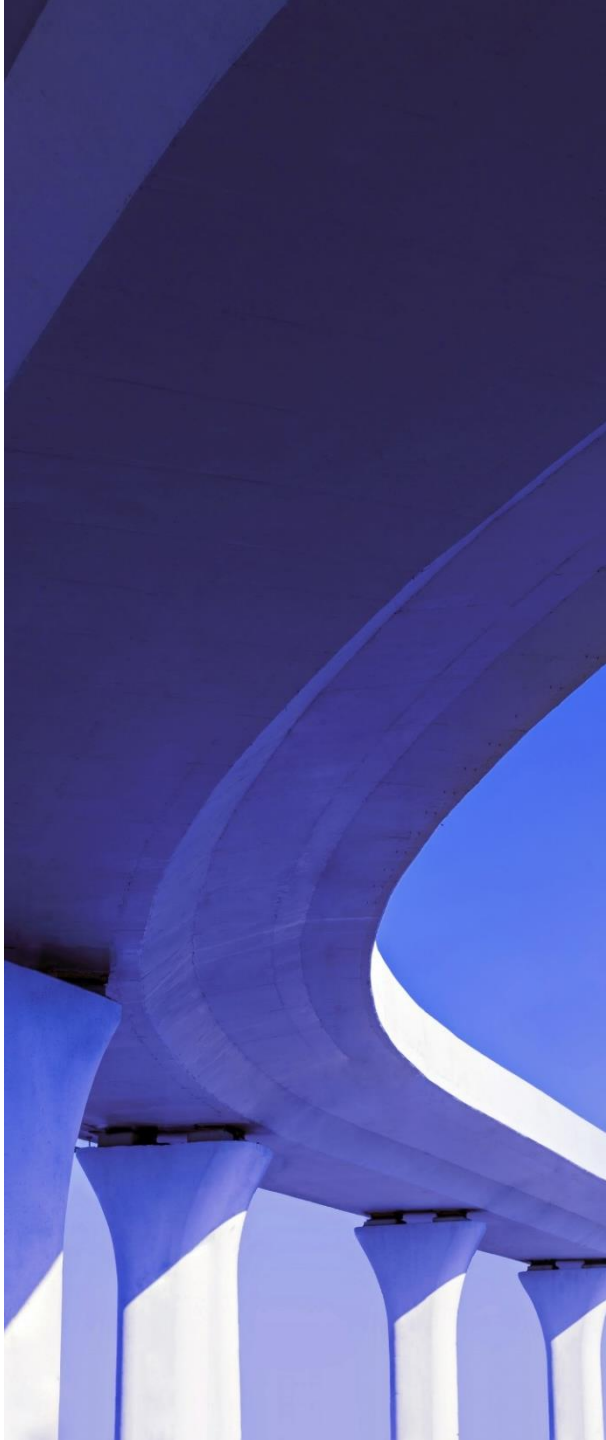
À noter : l'apparition de la mention des référentiels de l'ANSSI et du NIST (organisme de normalisation américain), qui apportent des éléments concrets de sécurisation.

Et pour conclure

Une prise en compte accrue de la cybersécurité dans les documents de référence depuis 2013…

… mais qui pourrait être meilleure, si les entreprises valorisaient intégralement leurs actions.

Pour l'année prochaine, une obligation de transparence accrue sur les incidents est à prévoir du fait de l'entrée en application du RGPD.



ANNEXES

Grille d'évaluation (1/2)

	Poids	Niveau 0	Niveau 1	Niveau 2
Enjeux de la cybersécurité et compréhension de la menace contextualisée à l'entreprise	3	0 point Absence de mention	+1 point Mention simple des enjeux	+2 points Mention détaillée des enjeux, incluant les mentions d'évolution de la menace et/ou des risques cyber spécifiques sur le métier
Prise en compte du risque cyber et de ses impacts spécifiques sur l'activité de l'entreprise	3	0 point Absence de mention	+1 point Mention du risque cyber	+2 points Mention détaillée du risque et de ses impacts
Sensibilisation et formation à la cybersécurité	2	0 point Absence de mention	+1 point Mention de sensibilisation des collaborateurs et/ou du comité exécutif	+2 points Mention d'initiatives de sensibilisation de grande ampleur et/ou de formation à destination des sous-traitants et/ou en dehors de l'entreprise
Niveau d'implication du comité exécutif dans le sujet cybersécurité	2	0 point Absence de mention	+1 point Mention de l'implication du comité exécutif	+2 points Mention de l'existence d'un membre directement impliqué et chargé de suivre le sujet cyber sous l'angle maitrise des risques (*top owner* du risque cyber)
Remédiation et couverture du risque cyber : programme de sécurité et plan d'actions	2	0 point Absence de mention	+1 point Mention de plans d'actions	+2 points Mention d'investissements conséquents à travers un programme (*i.e.* plusieurs dizaines de M€ ou montant approximatif évalué par Wavestone si non précisé)
Intégration de la cybersécurité dans la transformation numérique (IA, *Machine Larning*, IoT, *Blokchain*)	1	0 point Absence de mention	+1 point Mention simple	+2 points Mention détaillée sur les risques précis sur ces nouvelles technologies et/ou des actions de sécurisation spécifiques
Gouvernance SSI (*Sécurité des Systèmes d'Information*)	2	0 point Absence de mention	+1 point Mention simple des enjeux	+2 points Mention du rattachement du RSSI, de la manière dont l'organisation est déclinée à l'échelle du Groupe

Grille d'évaluation (2/2)

	Poids	Niveau 0	Niveau 1	Niveau 2
Sécurité des systèmes spécifiques métier (système de contrôle industriel, lutte contre la fraude, systèmes de paiement, etc.)	1	0 point Absence de mention	+1 point Mention des risques spécifiques au métier	+2 points Mention d'un programme conséquent et d'investissements
Privacy : RGPD / Vie privée / Protection des données personnelles	2	0 point Absence de mention	+1 point Mention simple	+2 points Mention de la nomination d'un DPO et/ou de la mise en place d'un programme de conformité, d'instance de contrôle
Transparence et réaction vis-à-vis d'attaques ou d'incidents majeurs rendus public	0	-2 points Absence de mention d'un incident largement relayée	-1 point Mention d'un incident sans les actions de remédiation associées	0 point Mention des incidents accompagnée des plans d'actions et/ou des modifications réalisées dans le cadre de la remédiation
Souscription à une cyberassurance	0	0 point Absence de mention	+1 point Mention de la souscription à une cyberassurance	+2 points Mention d'un niveau de couverture supérieur à 100 M€
Conformité aux règlementations de cybersécurité (LPM, NIS, PCI-DSS, HADS, NYDFS, etc.)	1	0 point Absence de mention	+1 point Mention de règlementations	+2 points Mention de plans de mise en conformité aux règlementations citées
Respect de normes et certifications de cybersécurité (ISO27001, NIST, FFIEC, CIS20, SANS, etc.)	1	0 point Absence de mention	+1 point Mention de normes de cybersécurité	+2 points Mention de la conformité, certification ou de l'alignement aux normes citées
Audit et contrôle du risque cyber	2	0 point Absence de mention	+1 point Mention d'audit et de mesures de couverture du risque cyber	+2 points Mention d'un plan de contrôle large ou significatif spécifique porté par l'équipe cybersécurité / l'audit interne / l'inspection générale

WAVESTONE

Gérôme BILLOIS
Partner

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com

Alexandre LUKAT
Senior Consultant

M +33 (0)6 72 58 26 52
alexandre.lukat@wavestone.com

Dominique YANG
Consultant

M +33 (0)7 62 36 62 28
dominique.yang@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE