WAVESTONE

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

Juin 2019

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

3 000 collaborateurs dans 8 pays

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* | Edimbourg
Lyon | Marseille | Nantes

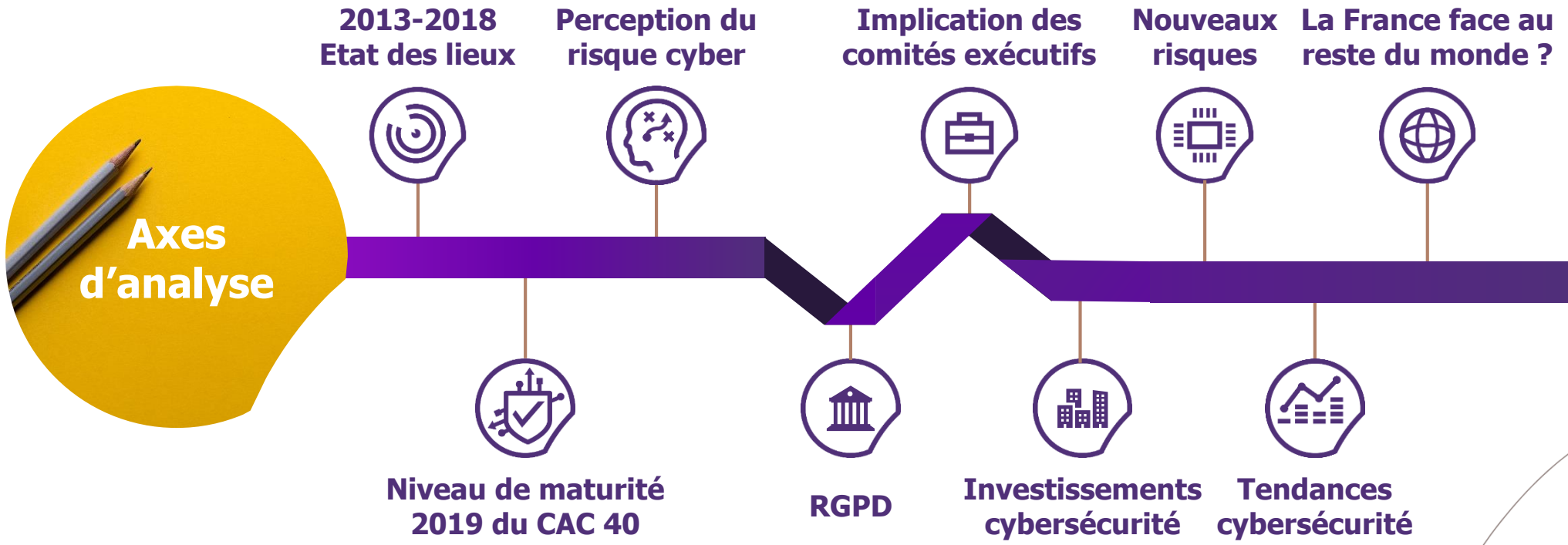
* Partenariats

© WAVESTONE

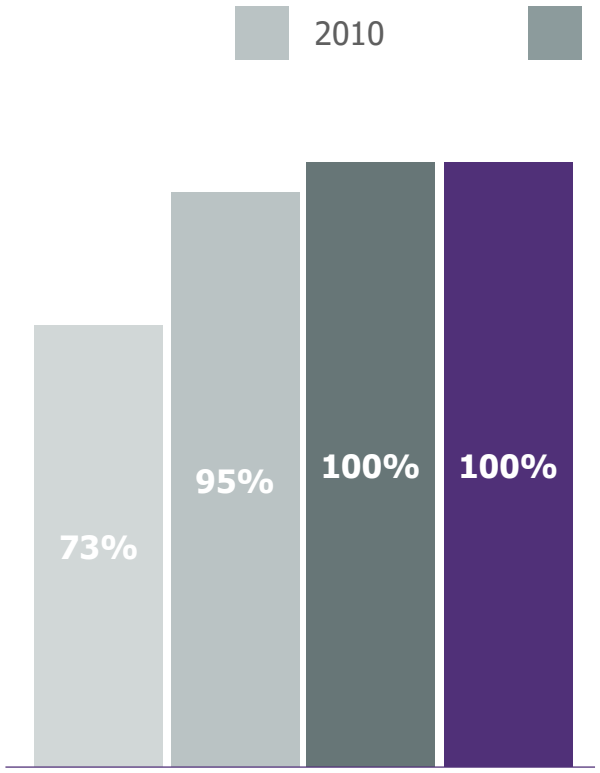
Quelle maturité en cybersécurité pour le CAC 40 en 2019 ?

Méthodologie : cette étude repose sur une analyse factuelle des derniers rapports annuels et documents de référence, publiés au 01/06/2019 par les entreprises du CAC 40.

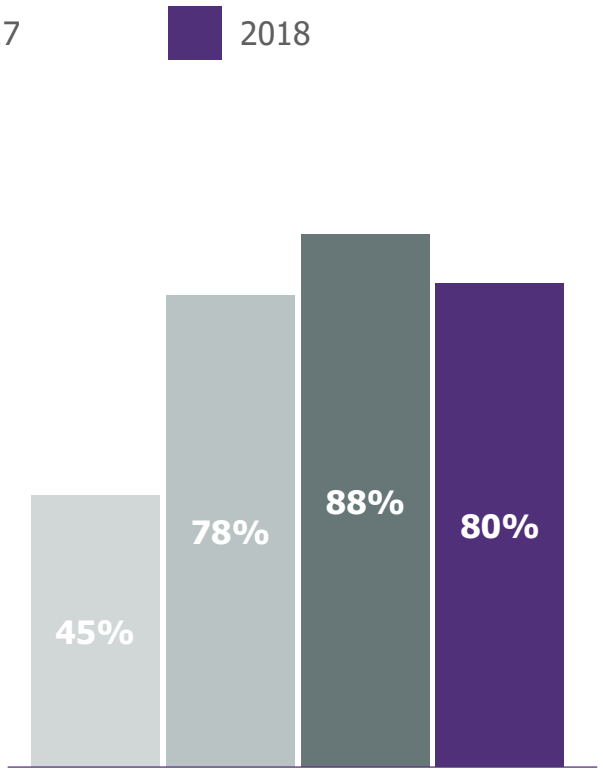
L'analyse se fonde uniquement sur les éléments présentés dans ces documents. Il est à noter que ceux-ci ne reflètent pas toujours l'exhaustivité des actions menées sur le terrain.



La cybersécurité stable, avec un léger fléchissement des investissements



Mentions des enjeux de cybersécurité



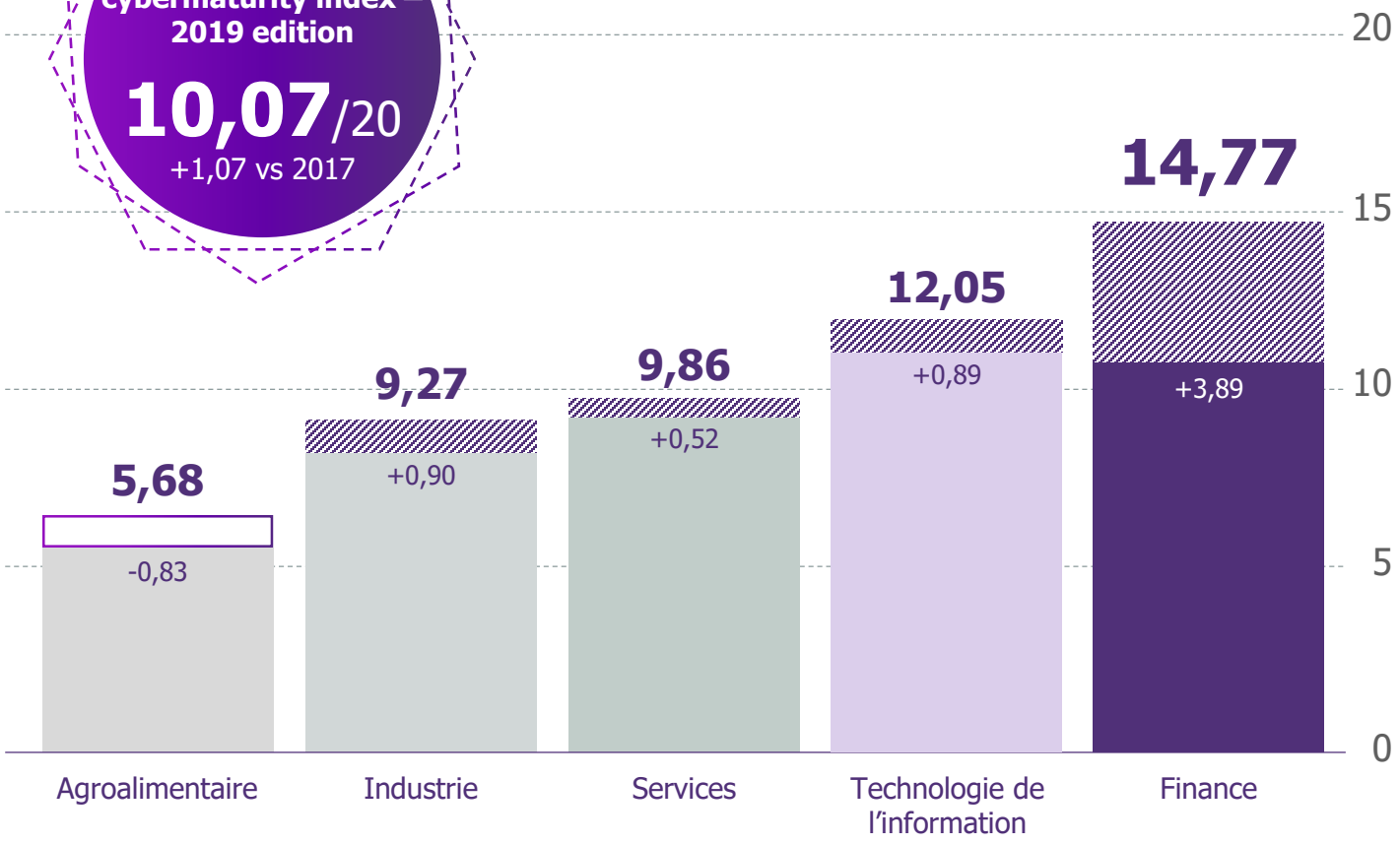
Mentions de la mise en place d'actions de couverture du risque cyber

Le CAC 40 progresse globalement, la finance valorise ses investissements

Financial communication cybermaturity index – 2019 edition

10,07/20

+1,07 vs 2017



Financial communication cybermaturity index – 2019 edition

Le *Wavestone Financial communication cybermaturity index – 2019 edition* 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.

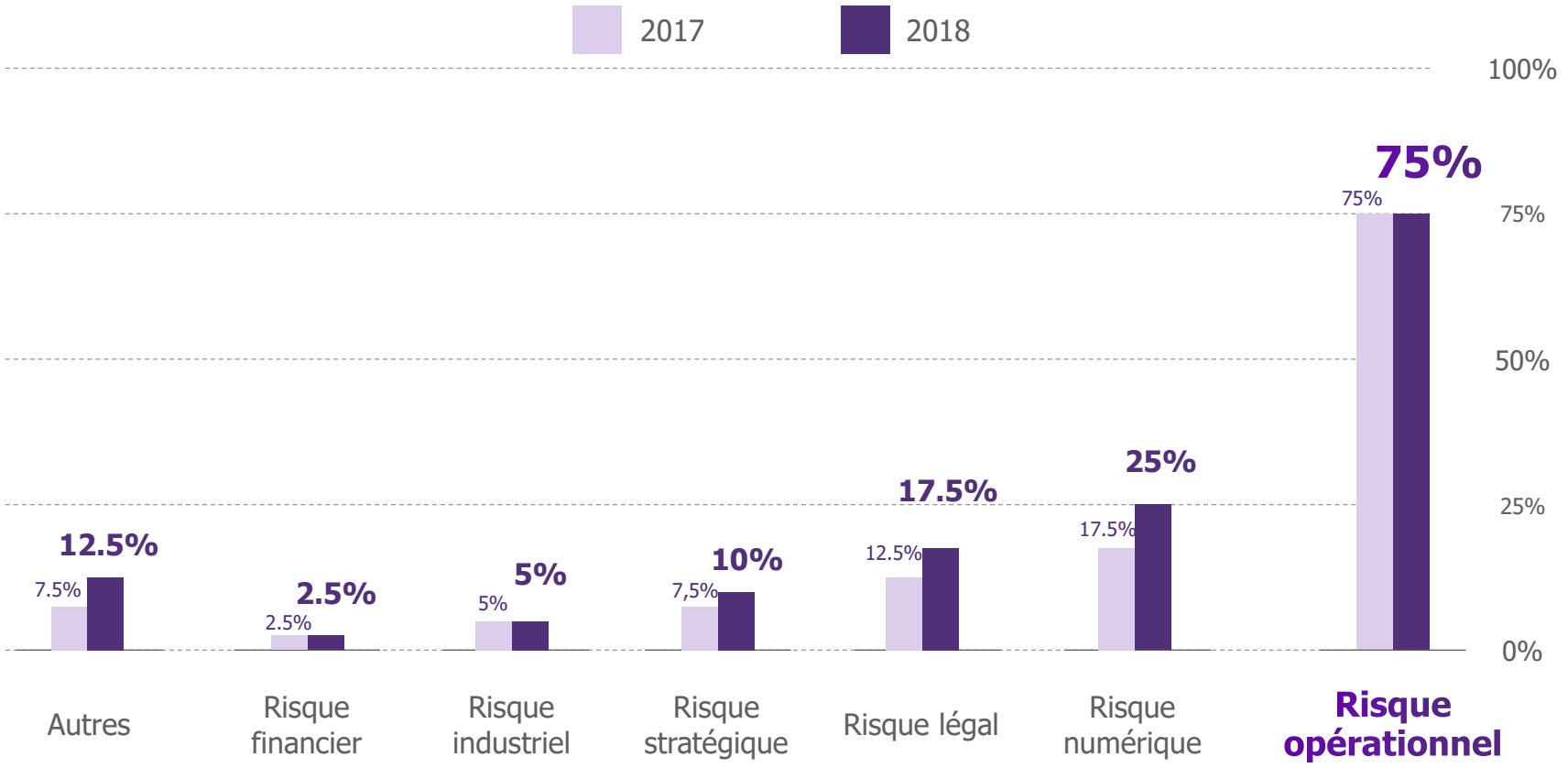
Protection et contrôle
Mise en place de plan d'actions, de programme de cybersécurité, sécurisation des systèmes métier, audit et contrôle.

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

Évolution de la composition du CAC 40 en 2018 : entrée des valeurs Dassault Systèmes et Hermès, sortie des valeurs Solvay et LafargeHolcim.

Le risque cyber avant tout perçu comme un risque sur les opérations

Le risque cybersécurité est majoritairement perçu comme un risque qui peut arrêter temporairement les opérations de l'entreprise, mais n'est pas vu comme un risque pouvant porter atteinte à la vie de l'entreprise à long terme.



Il est à noter que certaines entreprises peuvent classer le risque sous plusieurs catégories.

Forte progression de la mobilisation des comités exécutifs

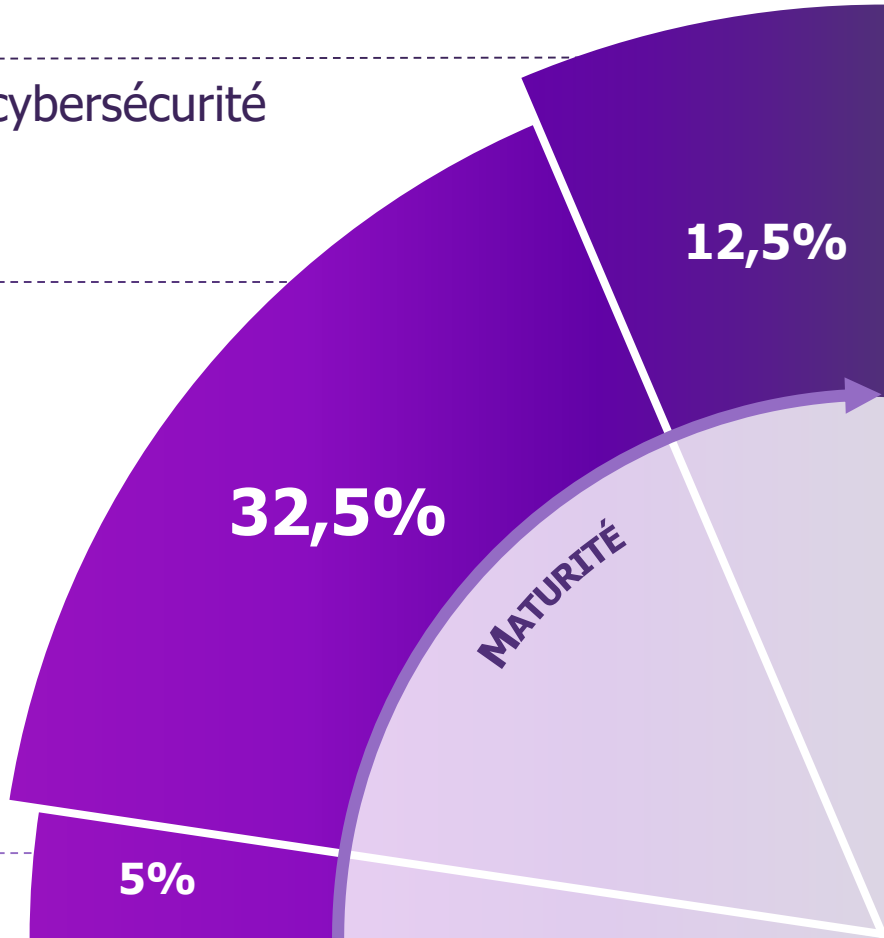
50% des groupes du CAC 40 adressent la problématique de la cybersécurité au niveau du comité exécutif.

+25 points vs 2017

Un membre du comité exécutif est mobilisé sur la cybersécurité

Une instance régulière avec le comité exécutif adresse la cybersécurité

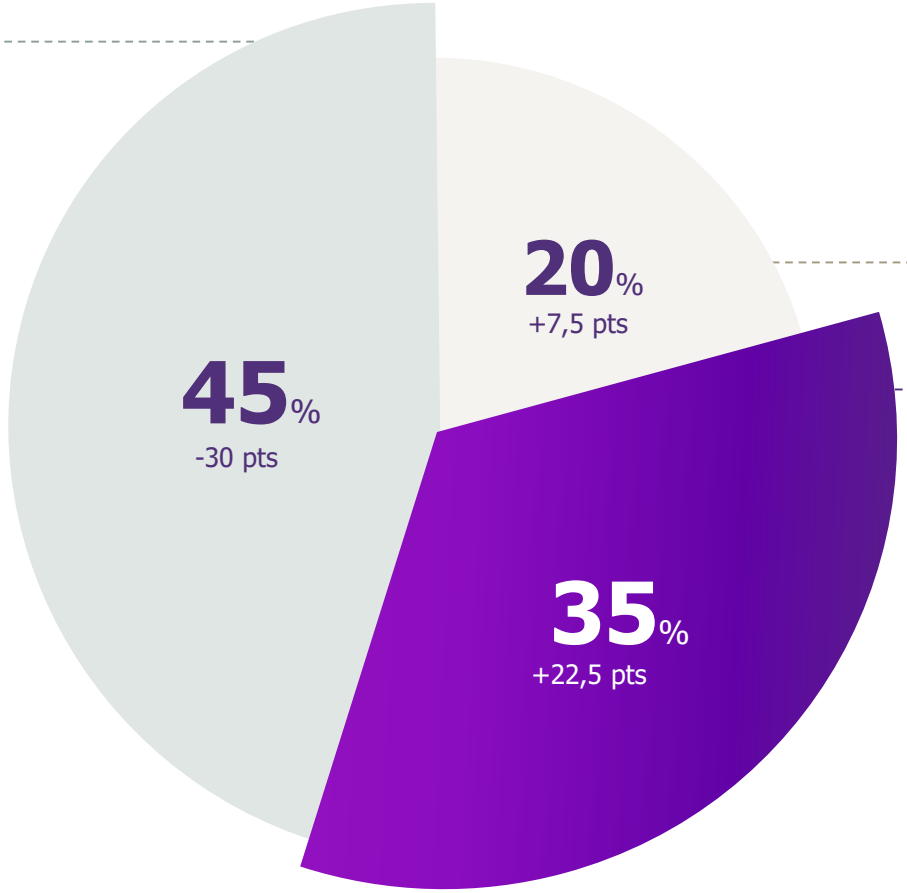
La cybersécurité est intégrée à la stratégie d'entreprise



Un marché qui se divise entre investissement lourd et attentisme

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

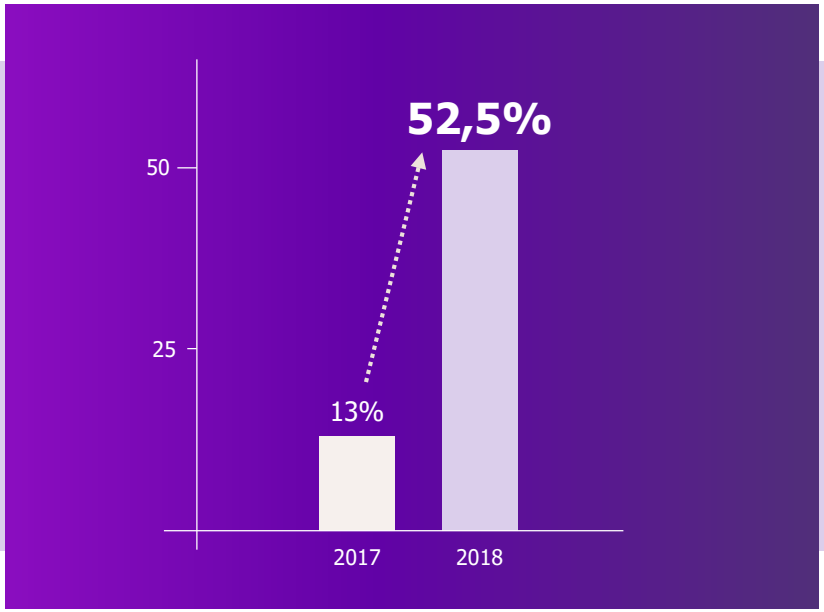
Des programmes de sécurité impliquant des investissements conséquents sont mentionnés

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€.

Enfin 100%

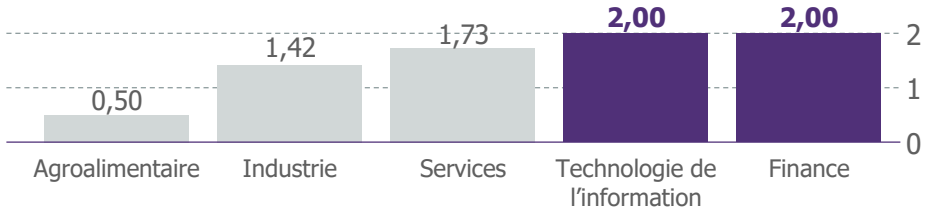
des entreprises du CAC 40 se mobilisent sur le sujet de la protection des données personnelles et du RGPD*

+42 points vs 2017



Une nette progression dans la prise de fonction de DPO *(Data Protection Officer)*

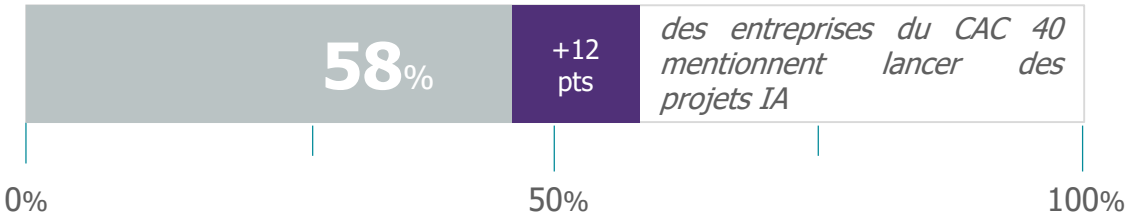
Le niveau de maturité du CAC 40 à nouveau tiré par les secteurs de la **finance** et des **technologies de l'information**



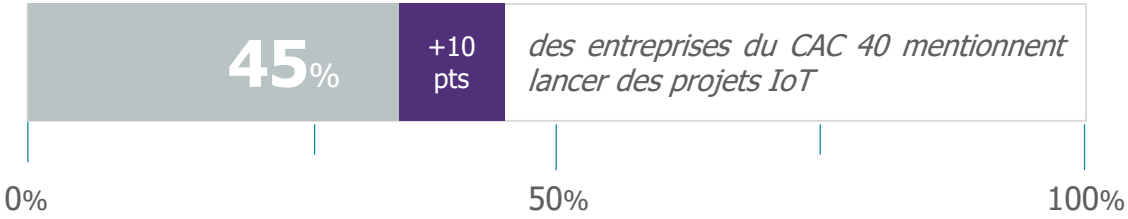
*RGPD : règlement général sur la protection des données à caractère personnel

Moins de blockchain, plus d'IoT et d'IA, mais toujours peu de lien avec la cybersécurité

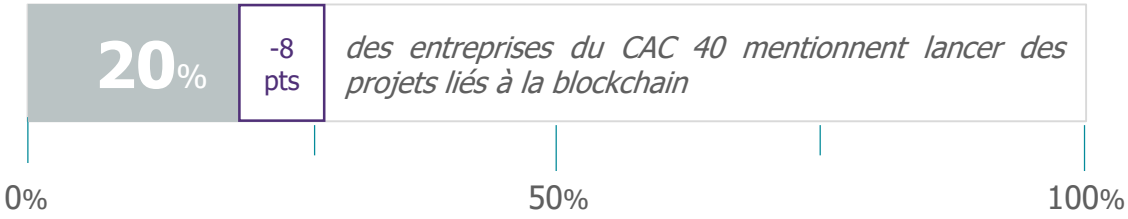
Nouveau dans l'étude



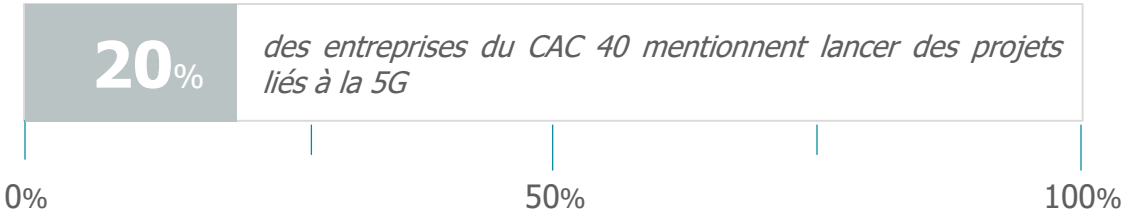
2 seulement font le lien avec la cybersécurité



2 seulement font le lien avec la cybersécurité

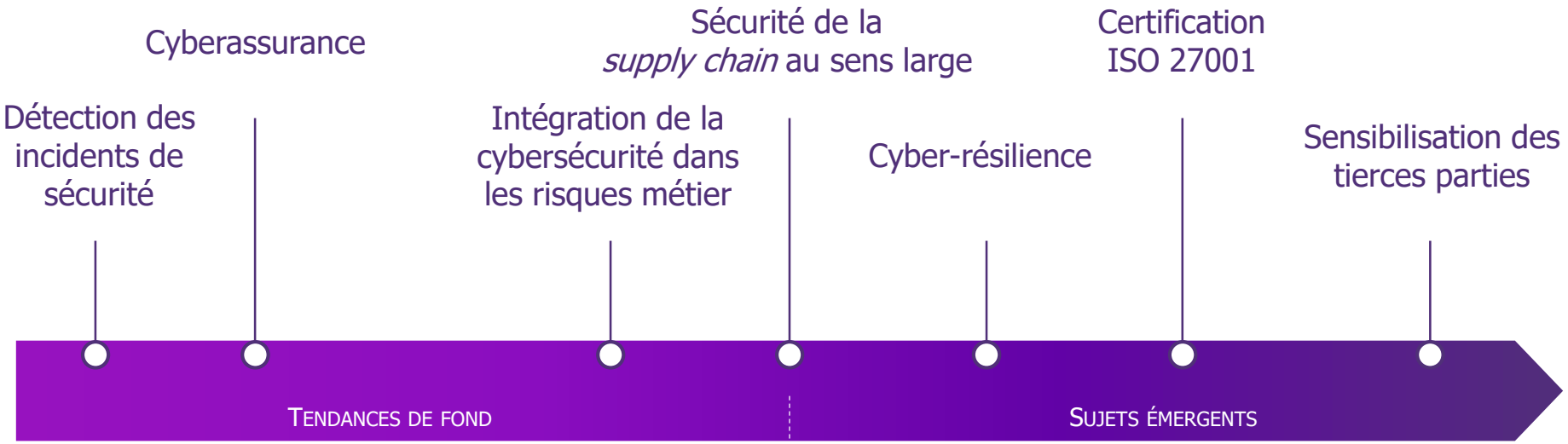


0 fait le lien avec la cybersécurité



1 seulement fait le lien avec la cybersécurité

Les tendances en cybersécurité



22 entreprises du CAC 40 mettent en place des actions de détection d'incidents de sécurité

19 entreprises du CAC 40 ont souscrit à une politique d'assurance « cyber »

10 entreprises du CAC 40 prennent en compte la sécurité de leurs fournisseurs, prestataires ou partenaires

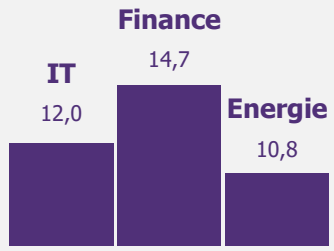
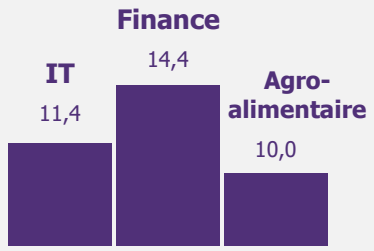
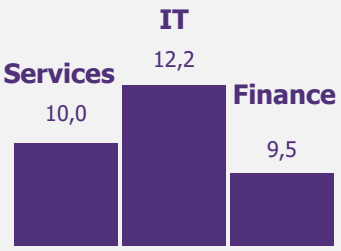
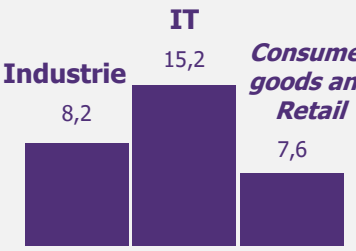
2 entreprises du CAC 40 mènent des initiatives de sensibilisation pour leurs sous-traitants ou clients

11 entreprises du CAC 40 prennent en compte la cybersécurité dans les risques métier (industrie 4.0, voiture connectée, vie privée et IoT, fraude dans les services financiers, piratage de contenu audiovisuel, etc.)

8 entreprises du CAC 40 œuvrent à la résilience de leur infrastructure face aux cyber-attaques

6 entreprises du CAC 40 sont certifiés ISO 27001 sur certains périmètres

La France, dans le peloton de tête, met la *Privacy* à l'honneur

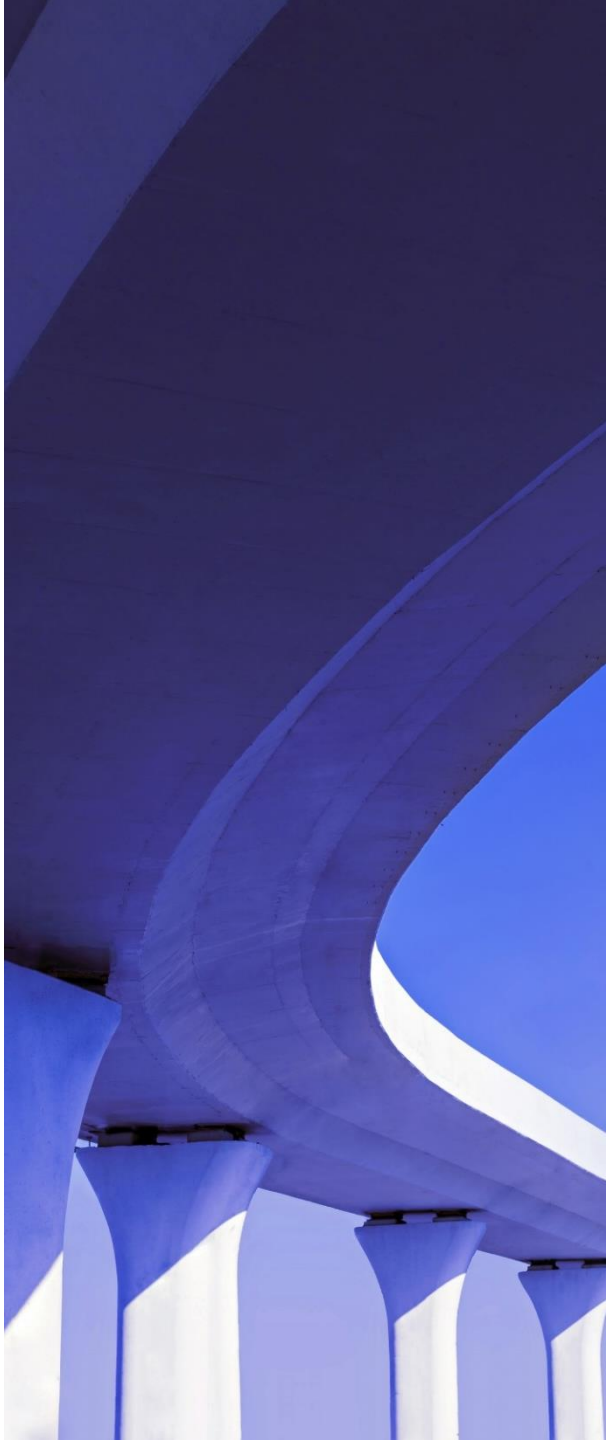
Score global	**10,07/20**	**10,15/20**	**9,09/20**	**8,57/20**
Secteurs en tête				
Implication du COMEX	**50%**	**83%**	**61%**	**50%**
Investissements	**35%**	**30%**	**46%**	**15%**
Privacy	**100%**	**87%**	**71%**	**75%**

Et pour conclure

Une prise en compte de la cybersécurité dans les documents de référence qui se stabilise…

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

Et l'année prochaine, dépasserons-nous la barre des 50% des comités exécutifs mobilisés sur la cybersécurité ?

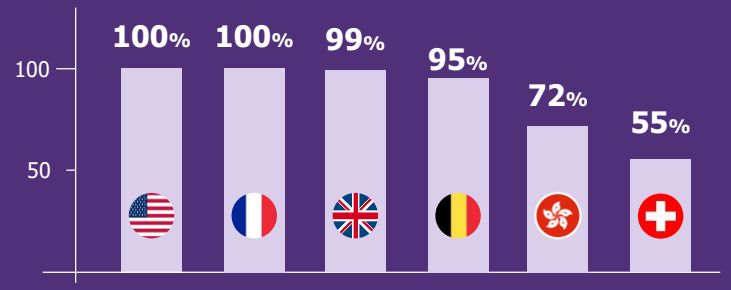


Quelle situation à l’international ?

Une large mobilisation à l'échelle internationale

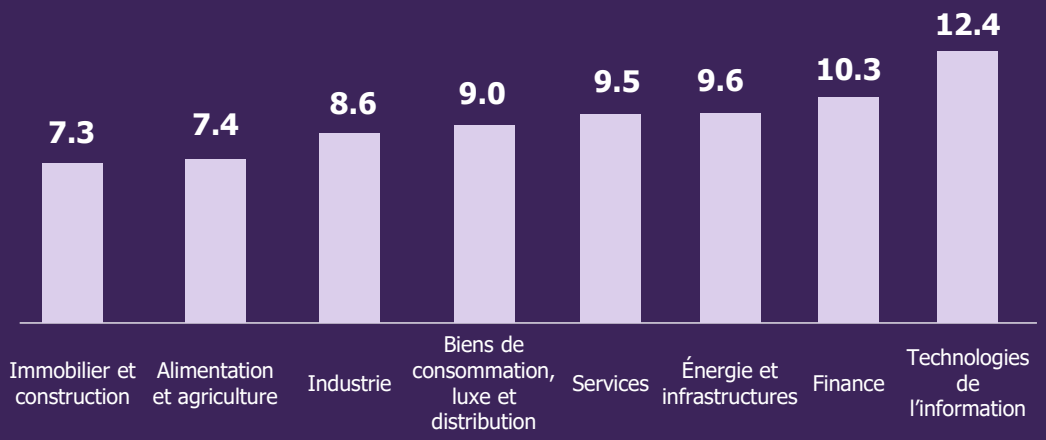
Les chiffres suivants sont basés sur les communications financières les plus récentes, publiées au 1er juin 2019, par les entreprises cotées dans le principal indice boursier des pays où Wavestone est présent : Dow Jones (), CAC 40 (), FTSE 100 (), BEL 20 (), SMI (), HSI (), i.e. représentant un panel de 260 entreprises.

90% **des entreprises agissent en matière de cybersécurité**



Focus sur les pays en tête

Les chiffres qui suivent se concentrent sur les 190 entreprises cotées dans les 4 indices boursiers leaders



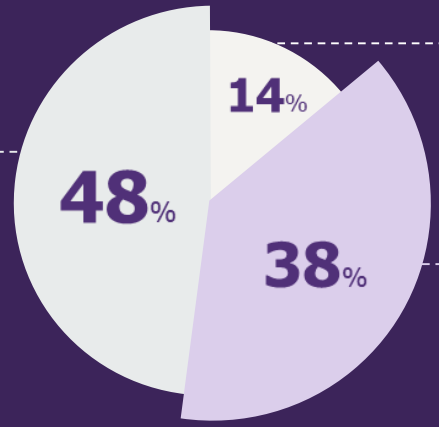
2019 Global Cybermaturity Index /20

Le secteur des Technologies de l'information en tête, devant le secteur de la finance

Focus sur les pays en tête

61% des entreprises traitent le sujet de la cybersécurité au niveau du Comité Exécutif

Des investissements dans la cybersécurité assez fragmentés



- Pas de mention
- Plans d'actions unitaires
- Programmes impliquant des investissements conséquents

PRIVACY, le grand gagnant de cette année

80%

du panel mentionnant le RGPD, la vie privée ou la protection des données personnelles

Focus sur les pays en tête

Comment construire un futur plus sécurisé ? Les entreprises investissent dans les technologies innovantes, pourtant la cybersécurité fait rarement partie des discussions, alors qu'elle le devrait

66 le mentionnent,

4 font le lien avec la cybersécurité

38 le mentionnent,

3 font le lien avec la cybersécurité

22 le mentionnent,

2 font le lien avec la cybersécurité

17 le mentionnent,

2 font le lien avec la cybersécurité

Que font les entreprises leader du marché ?

- **Cyberassurance**
- **Sécurité de la chaîne d'approvisionnement**
- **Cyberrésilience**
- **Sécurité des fusions-acquisition**

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 Learning*, IoT, *Blockchain*)	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	+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