WAVESTONE

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

Juillet 2020

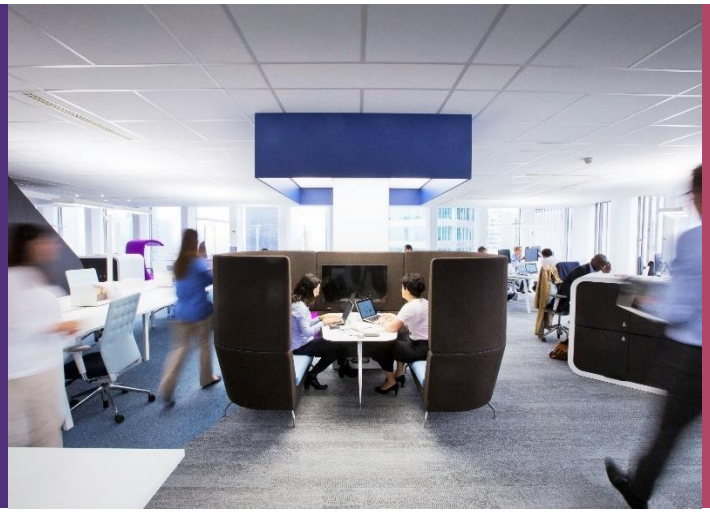
Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
+33 (0)6 10 99 00 60
@gbillois

Dominique YANG
Senior Consultant
dominique.yang@wavestone.com
+33 (0)6 72 58 26 52
@dominique_yang

Stimulés par les défis, engagés jusqu'aux réussites

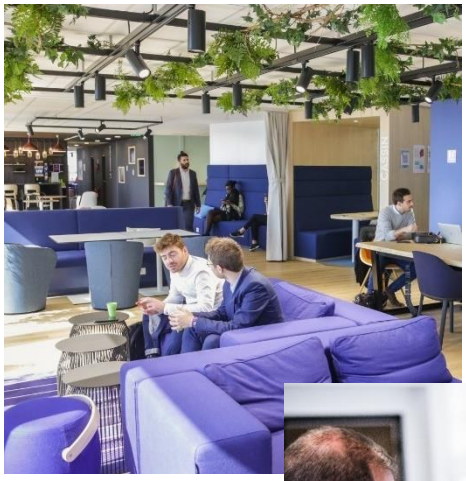
Business
&
Technologies

Transformation



Positive Way

Wavestone, indépendance et croissance



Pure player
indépendant

392 M€
+10%

+3 000
collaborateurs

12 bureaux
dans 8 pays

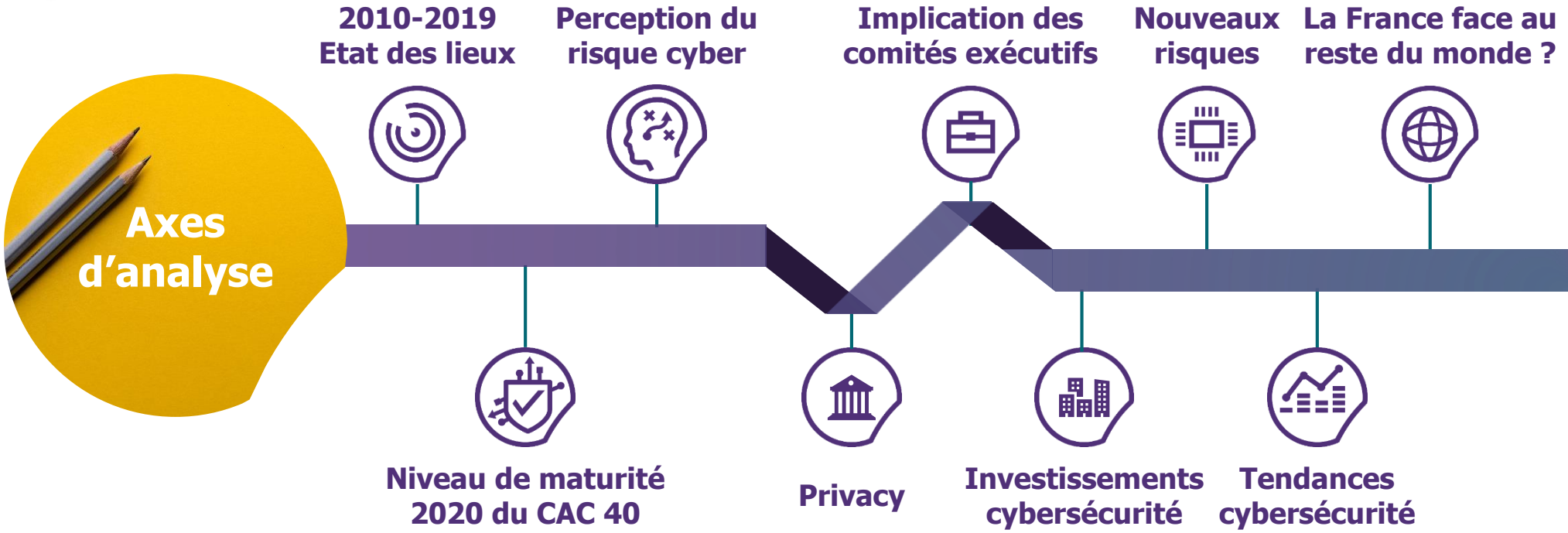
Quelle maturité en cybersécurité pour le CAC 40 en 2020 ?

Méthodologie : cette étude repose sur une analyse factuelle des derniers rapports annuels et documents d'enregistrement universel, publiés au 01/06/2020 par les entreprises du CAC 40.

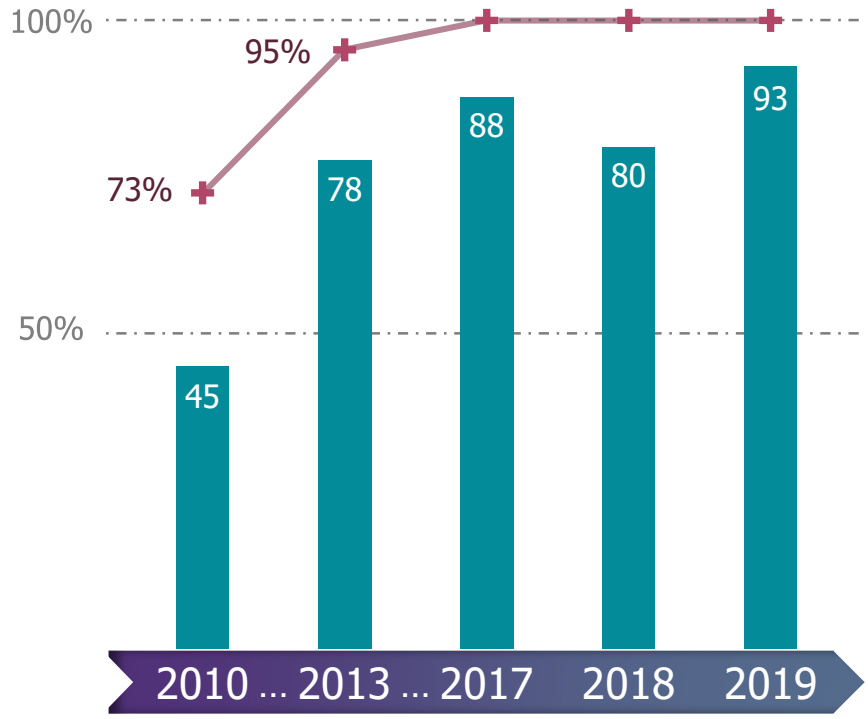
L'analyse se fonde uniquement sur les éléments présentés dans ces documents. Il est à noter que ceux-ci ne reflètent pas toujours l'exhaustivité des actions menées sur le terrain.

Covid-19

Cette année dans le cadre de l'étude, une analyse spécifique a été apportée à l'impact de la crise sanitaire vis-à-vis des enjeux cyber sur la base des communications financières du premier trimestre 2020.



L’âge de maturité de la cybersécurité avant le déclin ?



COVID-19

Certaines entreprises annoncent déjà des réductions significatives des coûts opérationnels et plus spécifiquement sur la partie cyber sécurité.

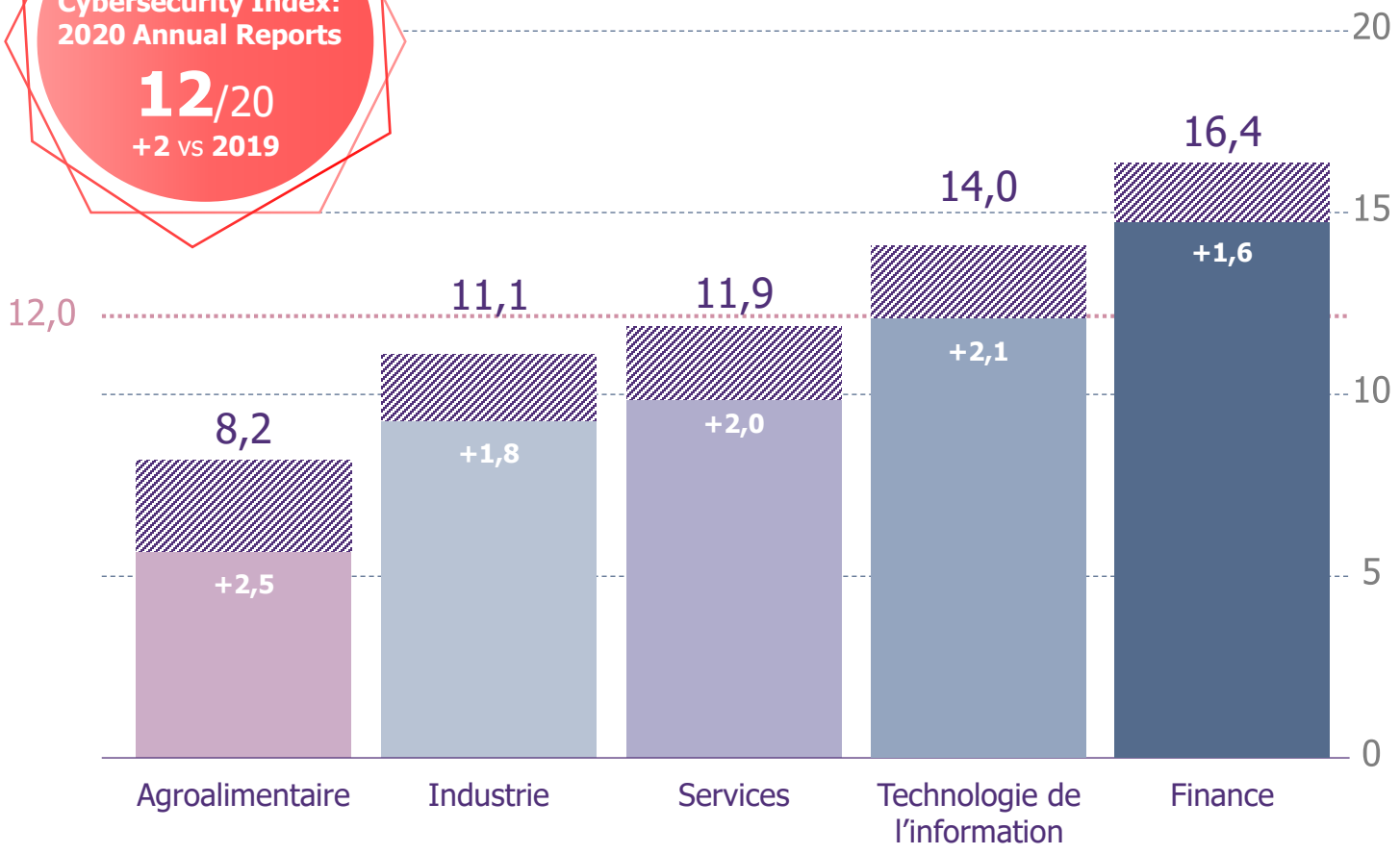
Depuis **3 ans** maintenant, l’ensemble des entreprises abordent le sujet de la cybersécurité. Cette appropriation du sujet est suivie petit à petit par la **mise en place d’action**.

Le CAC 40 continue de progresser quel que soit le secteur

Wavestone's CAC 40 Cybersecurity Index: 2020 Annual Reports

12/20

+2 vs **2019**



Évolution de la composition du CAC 40 en 2019 : entrée de la valeur Thales, sortie de la valeur Valeo.

Wavestone's Top Companies Cybersecurity Index: 2020 Annual Reports

Le *Wavestone's Top Companies Cybersecurity Index* permet d'apprécier le niveau de maturité des entreprises, à partir des éléments contenus dans leur document d'enregistrement universel. 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 cyber assurance, 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.

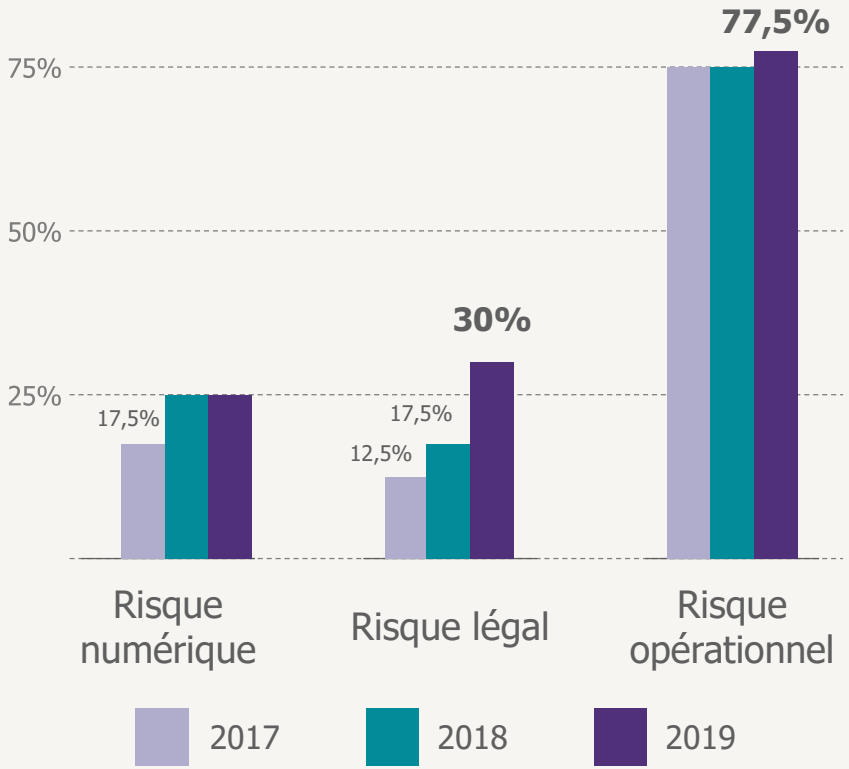
Protection et contrôle

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

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

Le risque cyber souvent présenté comme affectant les opérations des entreprises

Les entreprises sont de plus en plus nombreuses à classifier le risque cyber comme un **risque de non mise en conformité légale** pour l'organisation (e. g. non-conformité au RGPD).



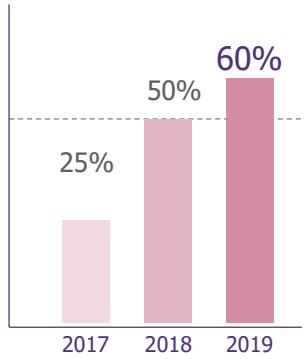
NB : certaines entreprises peuvent classer le risque sous plusieurs catégories.

1 entreprise le présente dans une nouvelle catégorie indépendante de type risque **cyber**

5 entreprises le considèrent comme un risque **stratégique**

Des comités exécutifs toujours plus mobilisés sur le sujet

60% des groupes du CAC 40 adressent la problématique de la cybersécurité au plus haut de niveau de l'organisation.

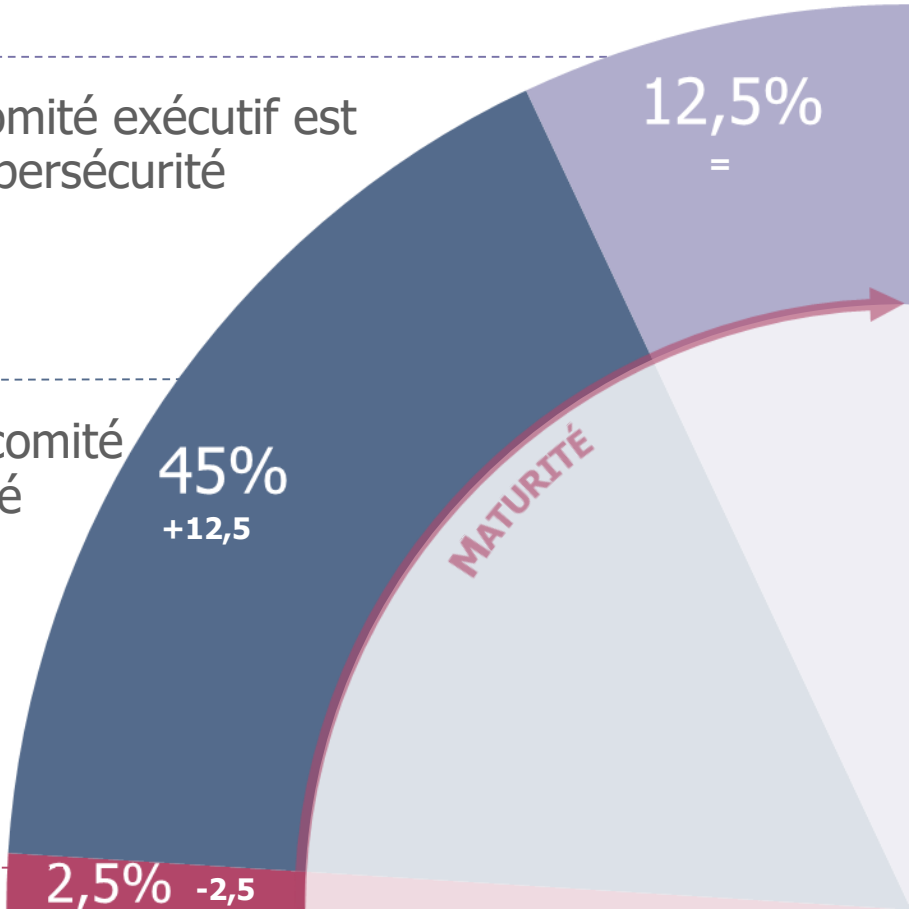


Suivi du critère « Niveau d'implication du comité exécutif»

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 toujours centrés vers la protection au détriment des autres thématiques de sécurité

93% des entreprises mentionnent couvrir les risques cyber via la mise en place de plans d'action ou des programmes de sécurité de grande envergure

+13 points vs 2019

Protection 93 %

Renforcement du contrôle d'accès, mise en place d'architecture sécurisée, correctif sécurité

65 % Détection

Des moyens de détection mis en place notamment via des centres opérationnels de sécurité

Réaction 55 %

Déploiement de moyens de réponse à incident au travers d'équipes dédiées ou un suivi spécifique des incidents de sécurité

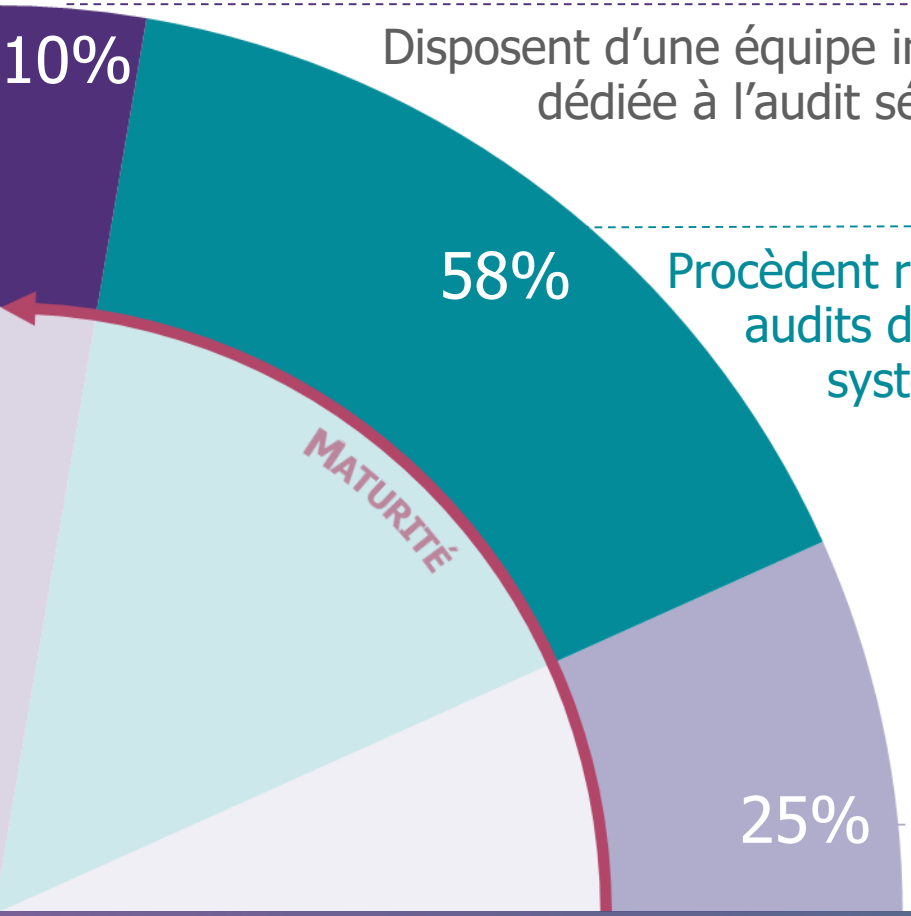
65 % Récupération

Mise en œuvre de plan de continuité d'activité ou de plan de reprise d'activité

Covid-19

Dans le cadre de la crise 5 entreprises ont lancé des investissements de fiabilisation de leurs accès distants dans le cadre de la généralisation du télétravail.

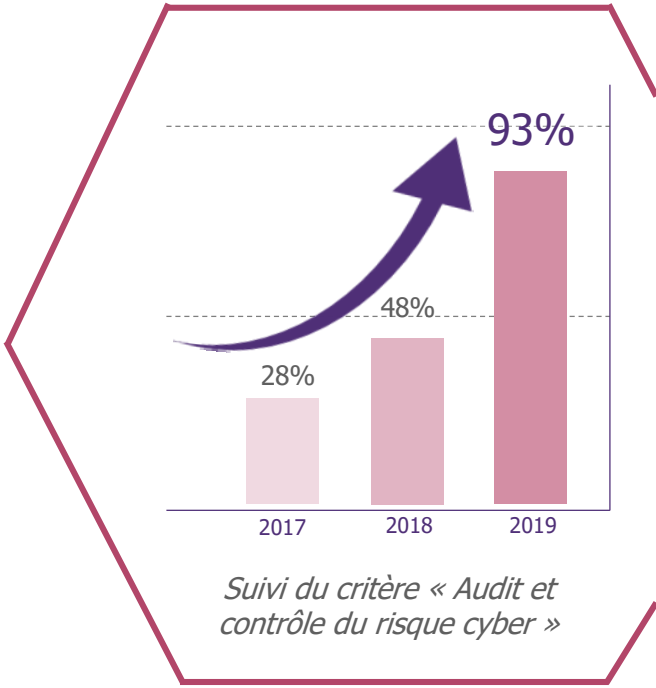
Une croissance exponentielle des audits et du contrôle



Disposent d'une équipe interne dédiée à l'audit sécurité

Procèdent régulièrement à des audits de sécurité sur leurs systèmes d'information

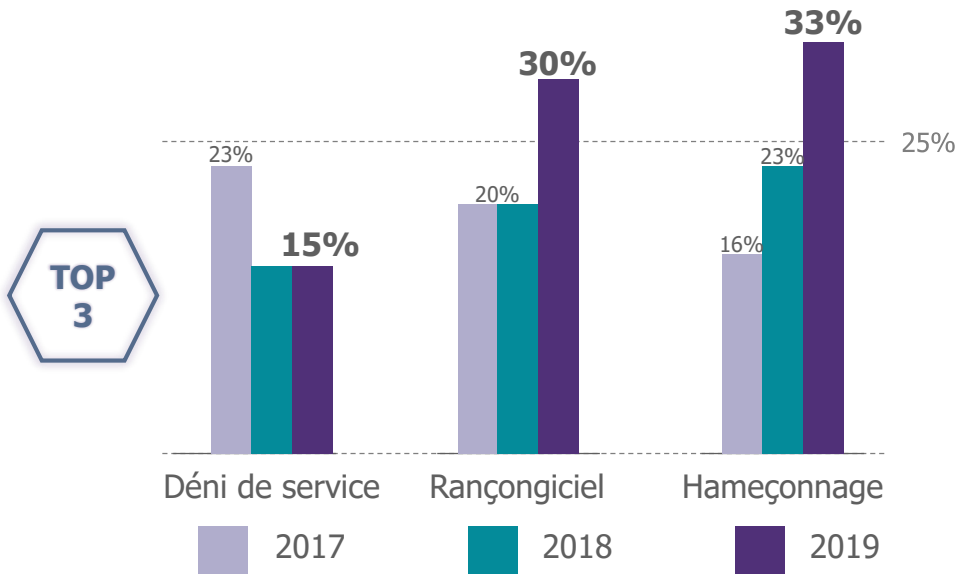
Mettent en œuvre des actions ponctuelles de contrôle



Suivi du critère « Audit et contrôle du risque cyber »

L'identification de la menace au travers de contrôles et d'audit permet la priorisation des investissements sur le volet cyber.

Plus de transparence sur les menaces mais les attaques vécues sont toujours taboues



Suivi de l'évolution des mentions des menaces dans les rapports

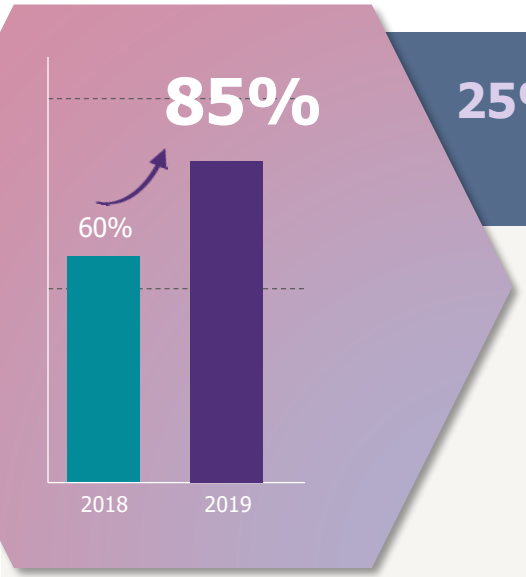
43% (*VS 30% en 2018*) des sociétés présentent les menaces cyber auxquelles elles sont exposées, avec des **menaces visant davantage les employés**.

Depuis 2017, **5 entreprises** du CAC 40 indiquent avoir été victimes de cyber attaques impactant significativement les opérations

Covid-19

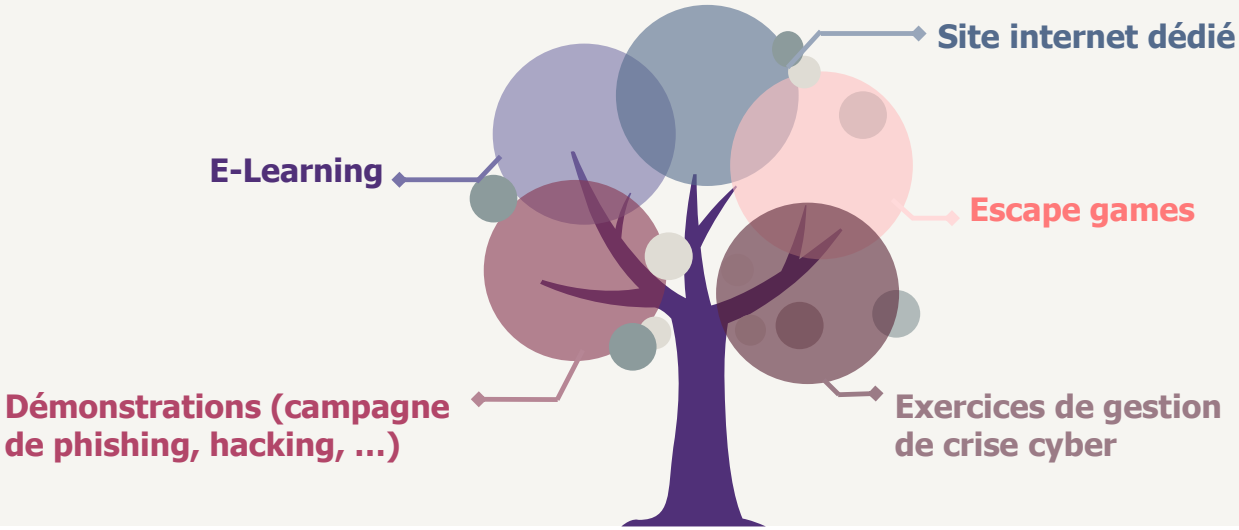
Seules deux entreprises mentionnent une activité plus importante des attaques cyber dans le contexte actuel.

Une forte progression sur la sensibilisation



25% des entreprises du CAC 40 qui introduisent la mention de programme de **sensibilisation** ou de **formation** dans leur rapport

Des **moyens** de plus en plus **innovants** pour sensibiliser

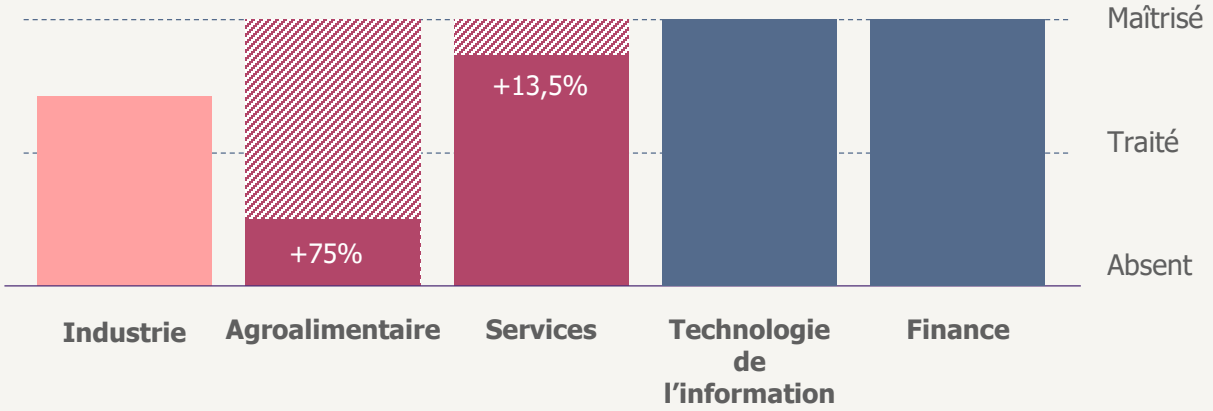


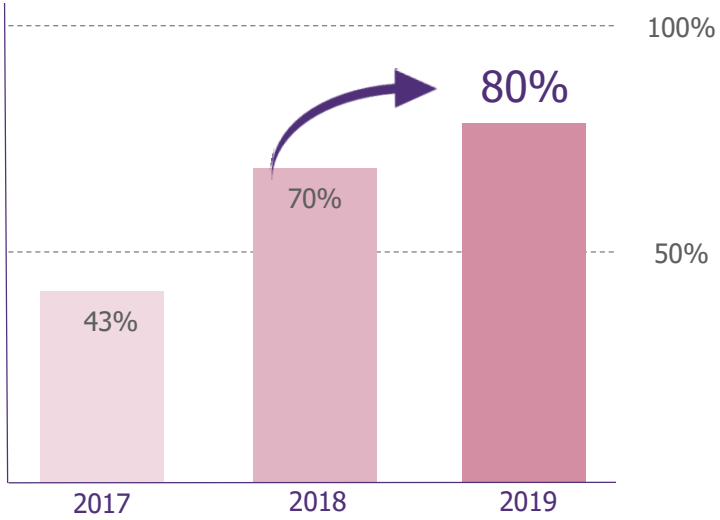
20% des entreprises **pilotent leur taux global** de sensibilisation des employés

5% vont jusqu'à **sensibiliser les fournisseurs**

L'ensemble du CAC 40 mobilisé sur le sujet de la protection des données personnelles

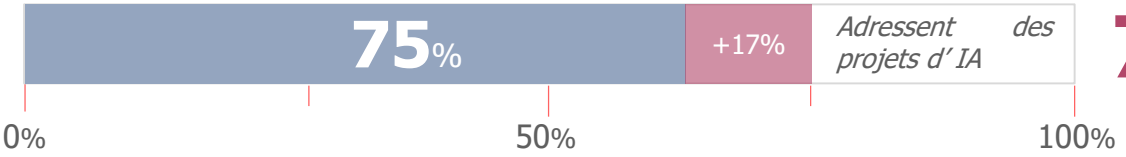
Le secteur de l'agroalimentaire réalise des **efforts conséquents** alors que l'industrie reste le seul **secteur en retrait**





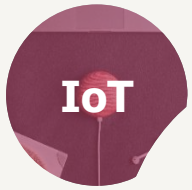
Le nombre de **DPO *(Data Protection Officer)*** toujours en augmentation depuis 2017 sans pour autant atteindre les 100%

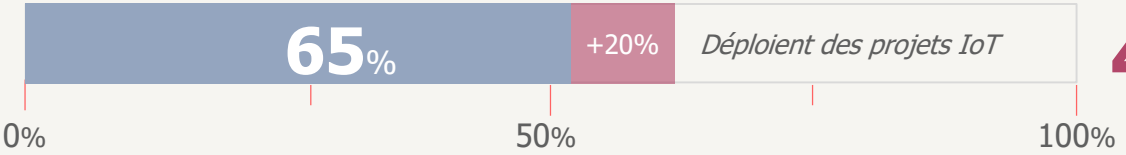
Une intégration timide de la cybersécurité dans les projets d'innovation



7 **vs 2**

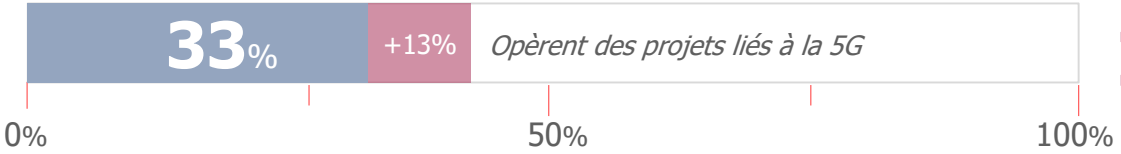
prennent en compte des mesures de cybersécurité





4 **vs 2**

font le lien avec la cybersécurité

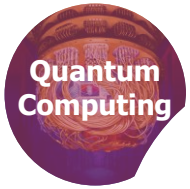


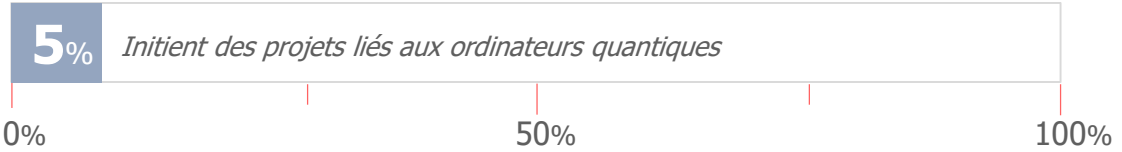
1 **vs 1**

étudie les potentiels risques associés

1 **vs 0**

la mentionne à des fins de traçabilité, de confiance et de transparence





0

adresse le sujet cybersécurité

Des tendances en cybersécurité qui sont de mieux en mieux appréhendées

Détection des incidents de sécurité

26 entreprises du CAC 40 mettent en œuvre des **mesures pour détecter les incidents de sécurité,**

17 d'entre elles mentionnent un ***Security Operation Center*** **(SOC).**

Cyber résilience

21 entreprises ont souscrit **une assurance contre les risques cyber,**

13 adoptent **un plan de continuité/reprise d'activité.**

Cybersécurité dans les processus de fusion/acquisition

4 entreprises de l'indice prennent en compte les **risques liés aux nouvelles acquisitions,**

1 inclue des **dispositions de cybersécurité dans les processus d'acquisition.**

TENDANCES DE FOND | **SUJETS ÉMERGENTS**

24 sociétés considèrent **les risques liés aux fournisseurs, partenaires et prestataires de services,**

11 présentent **des dispositions de cybersécurité** prises vis-à-vis de leurs **fournisseurs**, **partenaires et/ou prestataires de services.**

Cybersécurité de la *supply chain*

18 entreprises **s'inspirent des normes ou des framework** pour établir leur politique de cybersécurité,

6 indiquent être **certifiées ISO 27001** sur des périmètres précis.

Norme et Framework (ISO 27001, NIST, PCI-DSS, SMSI,…)

3 organisations mentionnent l'utilisation d'outils **d'anonymisation des données.**

Données synthétiques

La France en tête sur les problématiques de cybersécurité

	CAC 40	Dow Jones	FTSE 100	BEL 20
Score global	12,0/20	11,2/20	10,2/20	9,6/20
Secteurs en tête	IT 14,0 ; Finance 16,4 ; Services 11,9	IT 11,9 ; Finance 14,9 ; Services 11,2	Services 11,2 ; IT 13 ; Finance 11	Finance 10,3 ; IT 16,5 ; Industrie 9,4
Implication du COMEX	60%	64%	68%	45%
Investissements	43%	43%	51%	40%
Privacy	100%	93%	86%	90%

Et pour conclure

Le CAC 40 atteint l'âge de maturité avec des investissements toujours plus importants en termes de cybersécurité …

… mais ces entreprises gagneraient davantage à intégrer la sécurité dans les projets d'innovation.

Entre réductions des coûts et investissements renforcés, quelle tendance suite au Covid-19 pour 2021 ?

Quelle situation à l’international ?

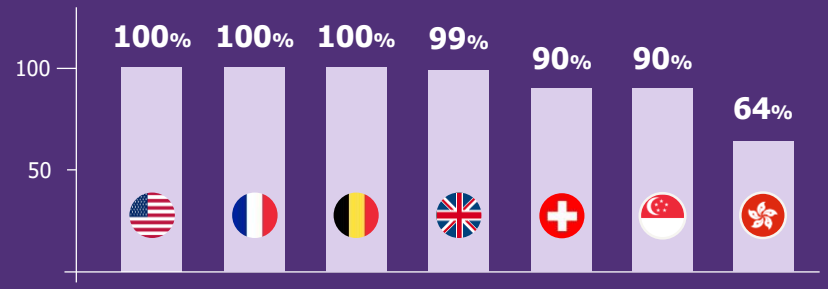
Une grande implication à l'échelle mondiale

Cette étude est basée sur une analyse factuelle des communications financières les plus récentes, publiées au 1er juin 2020, par les entreprises cotées dans les indices boursiers de 7 places financières majeures : Dow Jones, CAC 40, FTSE 100, BEL20, SMI, HSI, STI, représentant un panel de 290 entreprises.

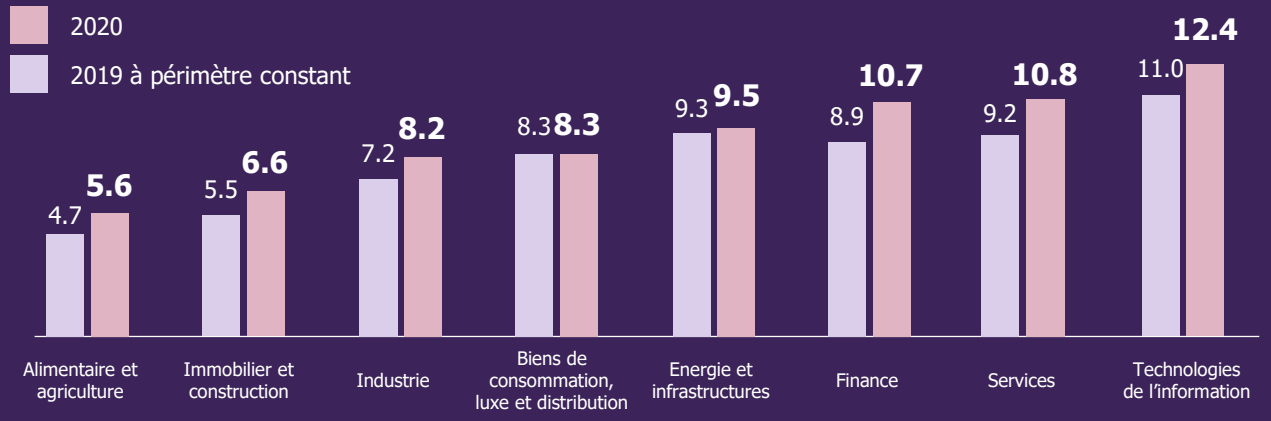
92%

des entreprises agissent en matière de cybersécurité

+2 points VS 2019 à périmètre constant



Le secteur des Technologies de l'information en tête
devant les secteurs des services et de la finance



Wavestone's Top Companies Cybersecurity Index: 2020 Annual Reports /20

Analyse internationale

Les pays leaders atteignent un seuil de maturité

Le bas du tableau rattrape son retard

1.	France CAC 40	12.03	+1.97
2.	US Dow Jones	11.18	+1.03
3.	UK FTSE 100	10.20	+1.10
4.	Belgium BEL20	9.64	+1.07
5.	Singapore STI	7.73	+0.31
6.	Swiss SMI	7.32	+3.70
7.	Hong Kong HSI	5.15	+1.05

57% **abordent la cybersécurité au niveau du COMEX**

+3 points VS 2019 à périmètre constant

1.	UK FTSE 100	68%
2.	US Dow Jones	63%
3.	Singapore STI	63%

PRIVACY

80% mentionnent le RGPD, la vie privée ou la protection des données personnelles

+13 points VS 2019 à périmètre constant

1.	France CAC 40	100%
2.	US Dow Jones	93%
3.	Belgium BEL20	90%

Analyse internationale

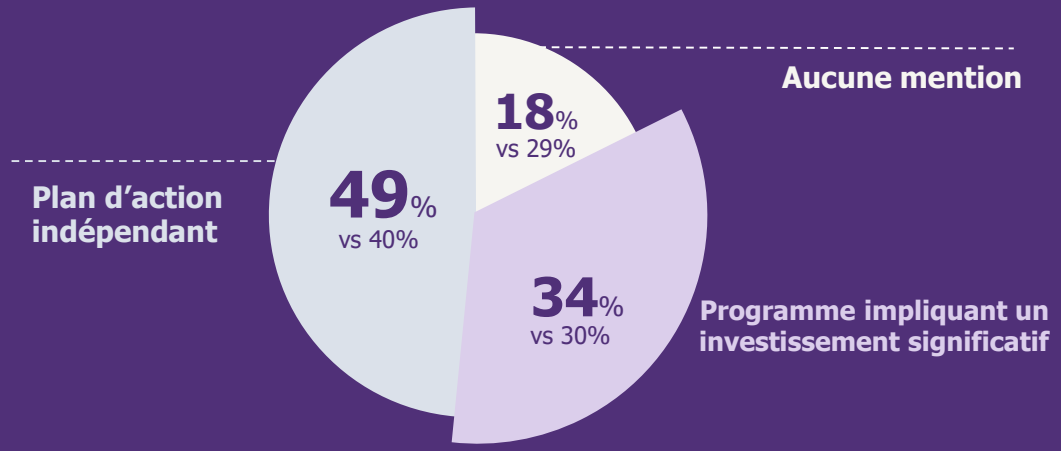
Qui domine sur chaque thématique ?

Pays #1 par critère

FORMATION & SENSIBILISATION		**85%** couvert
INVESTISSEMENT & PROGRAMMES CYBER		**100%** couvert
GOUVERNANCE CYBERSÉCURITÉ		**83%** couvert
AUDIT & GESTION DES RISQUES		**100%** couvert

Les investissements en cybersécurité restent fragmentés

Comparaisons à périmètre constant avec l'an dernier



Analyse internationale

Les investissements dans les projets innovants restent dynamiques,
mais le lien avec la cybersécurité est trop rarement fait.

AI

124 entreprises le mentionnent
18 font le lien avec la cybersécurité

IoT

87 entreprises le mentionnent
9 font le lien avec la cybersécurité

Blockchain

47 entreprises le mentionnent
3 font le lien avec la cybersécurité

5G

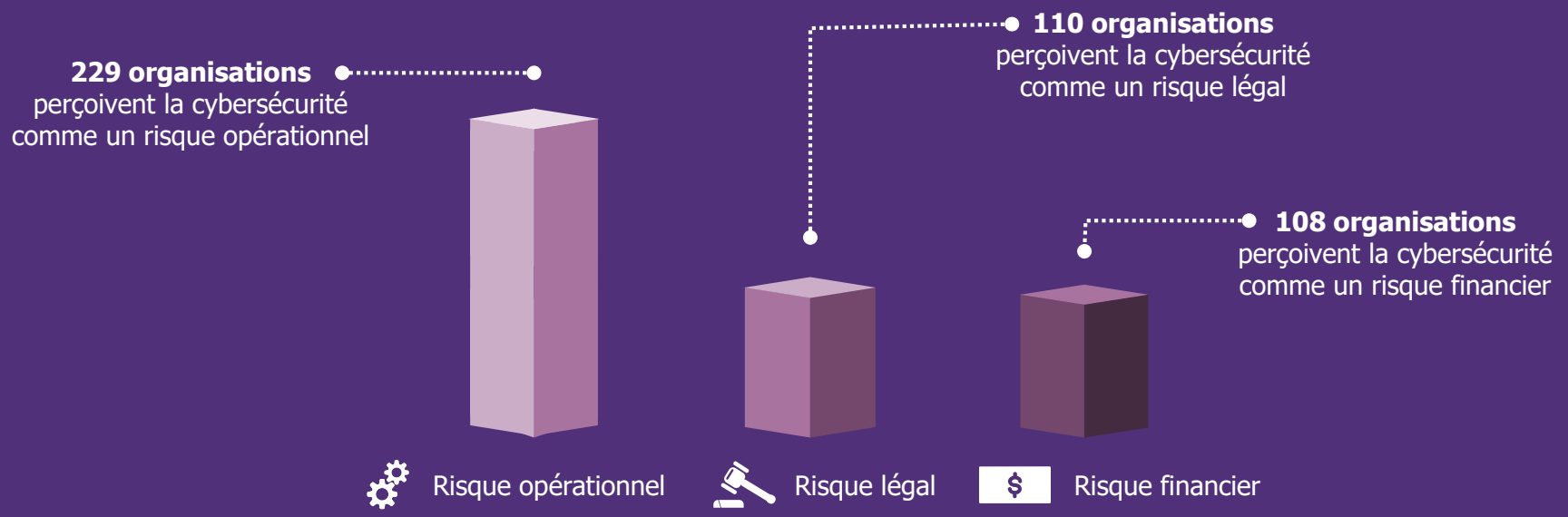
43 entreprises le mentionnent
3 font le lien avec la cybersécurité

Quantum computing

5 entreprises le mentionnent
0 font le lien avec la cybersécurité

Analyse internationale

La cybersécurité est souvent perçue comme un risque opérationnel



Sur quels sujets misent les entreprises leaders ?
Sujets cybersécurité émergeants

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 : investissement cybersécurité, 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 pour couvrir le risque cyber (*e.g.* un programme de cybersécurité de plusieurs années, plus d'une centaine d'ETP dédiée à la cybersécurité couvrant un nombre significatif de points de présence, un budget cyber de 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 hiérarchique du RSSI ou mention de la manière dont la fonction cybersécurité est organisée 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

Dominique YANG
Senior Consultant

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

Eudes DESCROIX
Consultant

M +33 (0)6 98 11 18 41
eudes.descroix@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS
LONDON
NEW YORK
HONG KONG
SINGAPORE *
DUBAI *
SAO PAULO *
LUXEMBOURG
MADRID *
MILANO *
BRUSSELS
GENEVA
CASABLANCA
ISTANBUL *
EDINBURGH
LYON
MARSEILLE
NANTES

* Partnerships

WAVESTONE