www.pwc.com

Principales conclusions de l'étude « Global State of Information Security Survey® 2012 »

Tendances et enjeux de la sécurité de l'information

pwc

CIO Business Technology Leadership

CSO BUSINESS RISK LEADERSHIP

Les caractéristiques de l’enquête

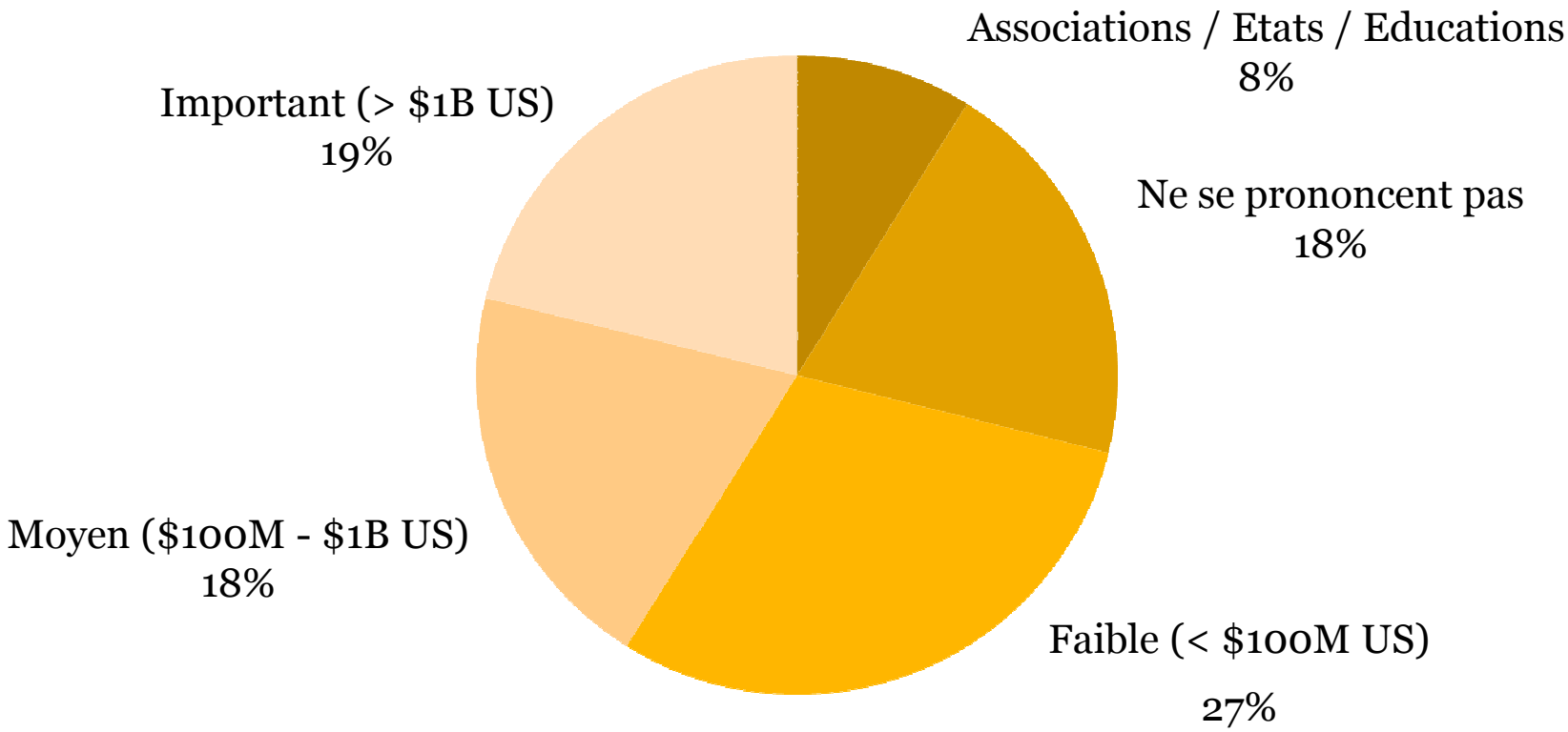
Une étude mondiale

L'enquête « Global State of Information Security Survey ® 2012 » est une étude mondiale menée par PwC en partenariat avec les publications « CIO magazine » et « CSO magazine », entre le 1 février 2011 et le 18 avril 2011.

- 14e année consécutive de réalisation de l'enquête par PwC, 9e année avec « CIO magazine » et « CSO magazine »
- Plus de 9 600 réponses de PDG, Directeurs Financiers, DSI, RSSI et responsables IT et sécurité, répartis dans 138 pays
- 560 réponses pour la France
- Plus de 40 questions relatives à la sécurité de l'information, à la protection des données et à leur alignement avec les besoins métiers

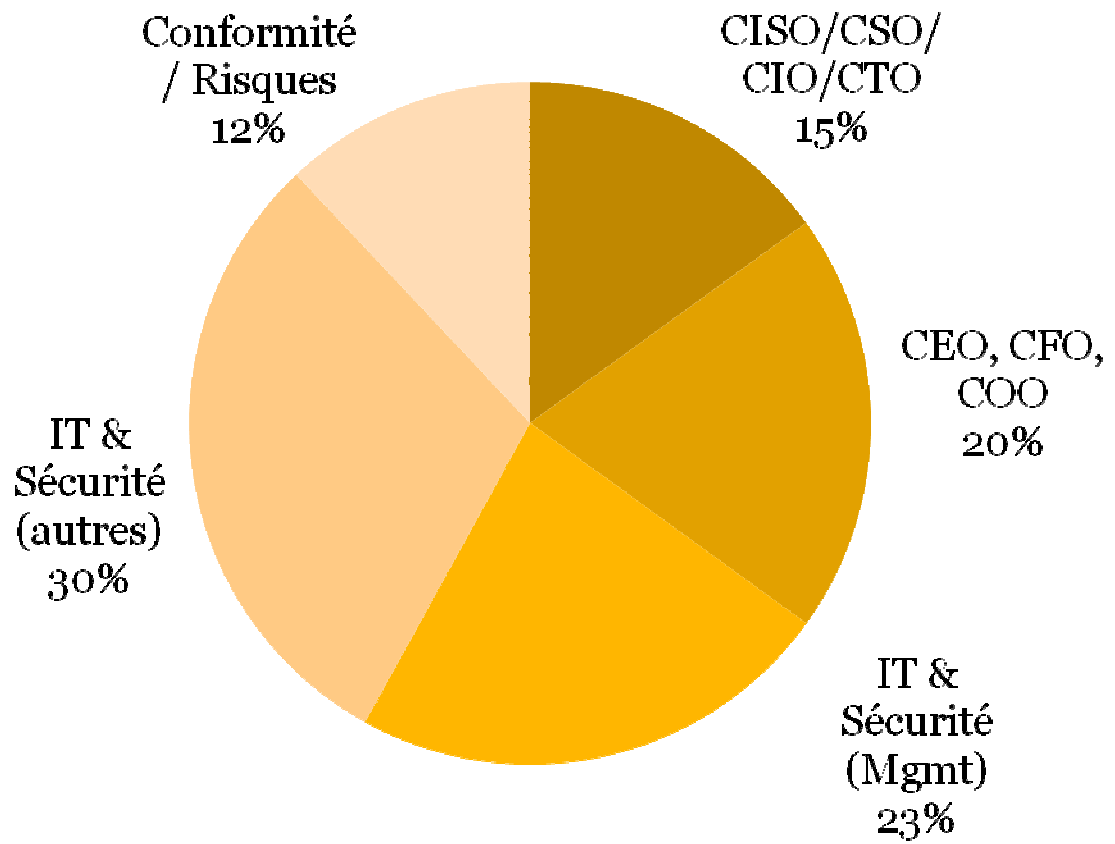
Des réponses provenant de responsables métiers, IT et sécurité de tous les secteurs d'activité dans 138 pays

Répartition de la taille des organisations



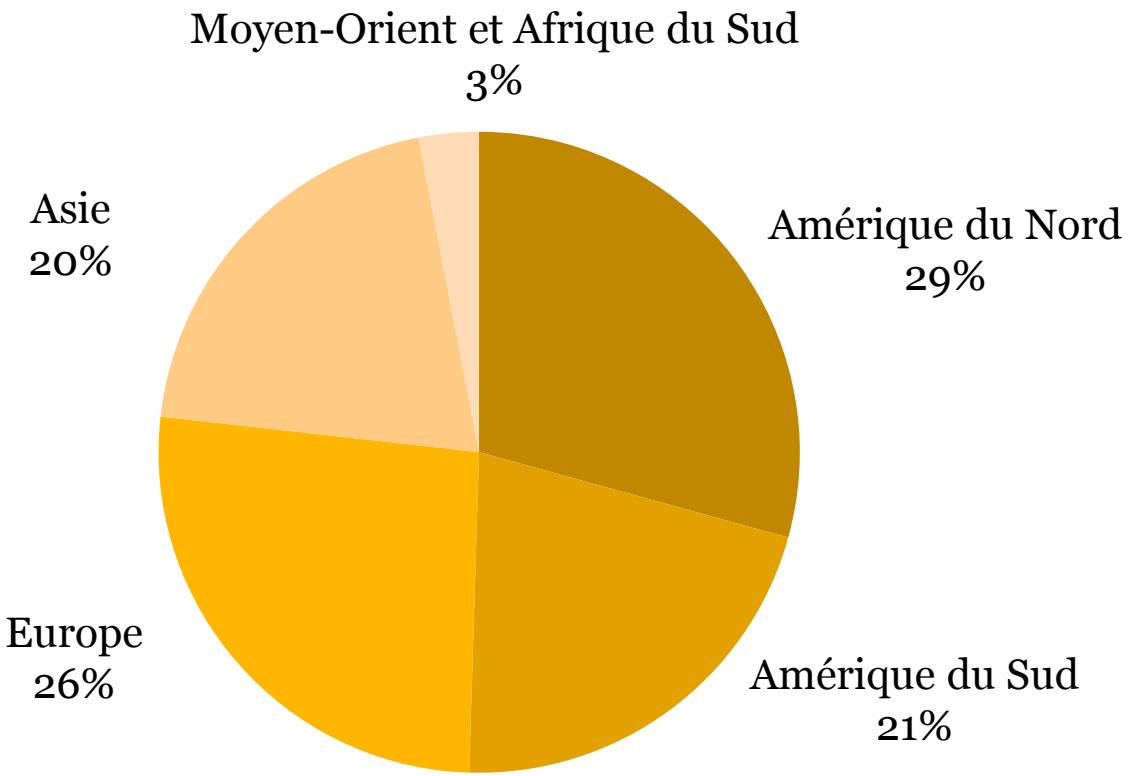
Des réponses provenant de responsables métiers, IT et sécurité de tous les secteurs d'activité dans 138 pays

Répartition des rôles des répondants



Des réponses provenant de responsables métiers, IT et sécurité de tous les secteurs d'activité dans 138 pays

Répartition géographique



Niveaux de réponses par secteur

	Nombre de réponses au niveau Monde	Nombre de réponses au niveau France
Technologie	1237	62
Services financiers	997	51
Industrie	880	45
Conseil et services professionnels	865	40
Produits de consommation et distribution	768	46
ONG	666	40
Ingénierie et construction	661	34
Industrie de la santé	626	37
Services publics	552	45
Télécommunication	499	27
Logistique et transport	404	36
Energie et services aux collectivités	363	13
Voyages et loisirs	357	27
Divertissement et media	335	13
Agriculture	206	15
Aérospatial et défense	195	22
Papier et emballage	83	7

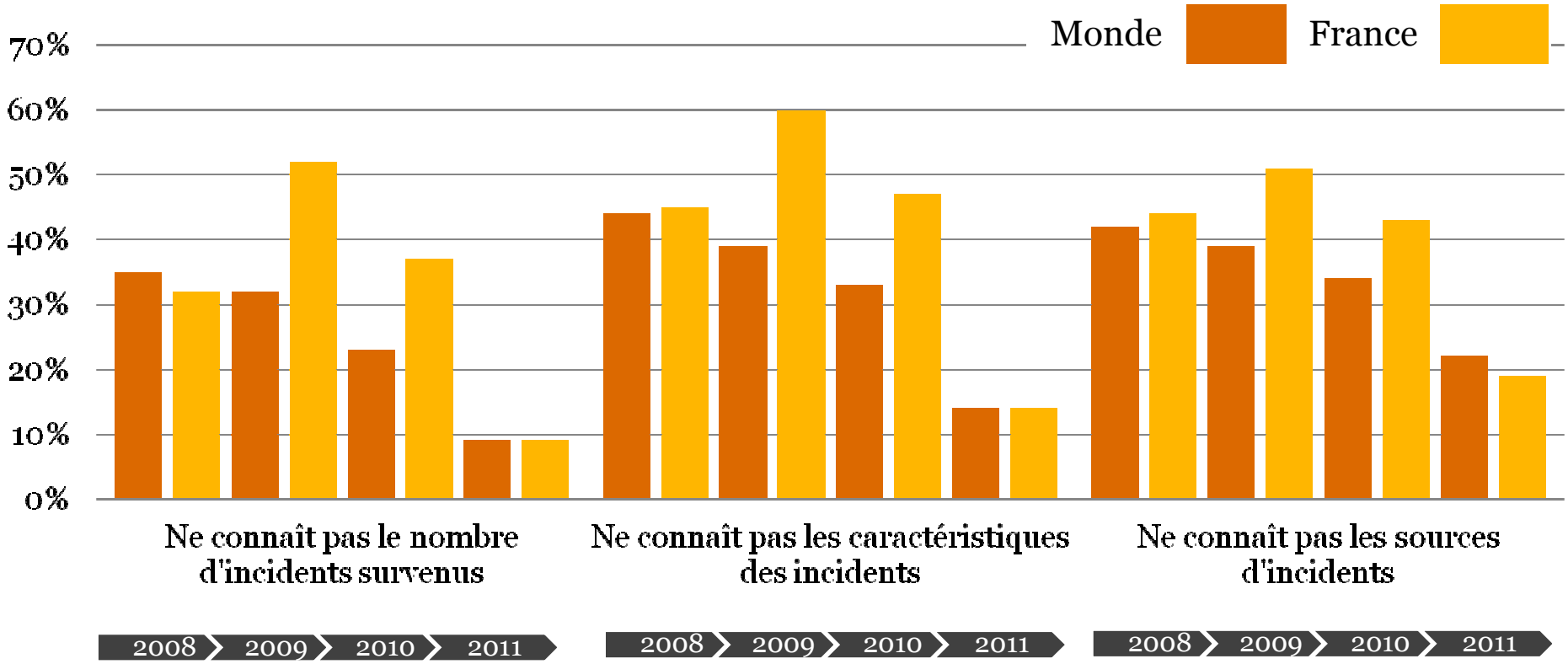
Des incidents de mieux en mieux identifiés, mais dont la gravité atteint des niveaux critiques pour les organisations

Patrick Pailloux, Directeur Général de l'ANSSI (audition à la Commission de la Défense Nationale et des Forces Armées)

« Nous vivons à l'heure des cybermenaces et il est difficile d'être optimiste sur leurs évolutions. Depuis quelques années, les attaques informatiques à des fins crapuleuses se multiplient. »

Des incidents de sécurité de mieux en mieux connus par les organisations

La tendance à l'amélioration de la connaissance par les organisations des incidents qui les frappent, de leurs caractéristiques et de leurs causes, se poursuit de manière spectaculaire



Pourcentage de réponses « ne savent pas » aux questions Q19: « Nombre des incidents de sécurité dans les 12 derniers mois. », Q20 « Quels type d'incidents de sécurité sont survenus? » et Q22: « Sources estimées des incidents » Les totaux peuvent dépasser 100%.

En corollaire, plus d'organisations déclarent subir des incidents de sécurité

Une augmentation du nombre d'organisations qui déclarent ne pas avoir subi d'incidents de sécurité, sans doute due à une meilleure connaissance des incidents, et une capacité à mieux qualifier ce qui constitue réellement un incident de sécurité.

Parallèlement, une augmentation de 20 points de base de la part des organisations déclarant avoir connu des incidents depuis 2008.

Nombre d'incidents de sécurité	2008 Monde	2008 France	2009 Monde	2009 France	2010 Monde	2010 France	2011 Monde	2011 France	Variation Monde	Variation France
Pas d'incident	25%	26%	19%	19%	27%	25%	31%	30%	*+ 6 pts*	*+4 pts*
Au moins un incident	41%	41%	49%	28%	49%	39%	61%	61%	*+20 pts*	*+ 20 pts*
1 à 9 incidents	30%	32%	35%	18%	37%	29%	40%	36%	*+10 pts*	*+4 pts*
10 à 49 incidents	7%	6%	9%	6%	7%	6%	9%	12%	*+2 pts*	*+6 pts*
50 incidents ou plus	4%	3%	5%	4%	5%	4%	12%	13%	*+8 pts*	*+10 pts*

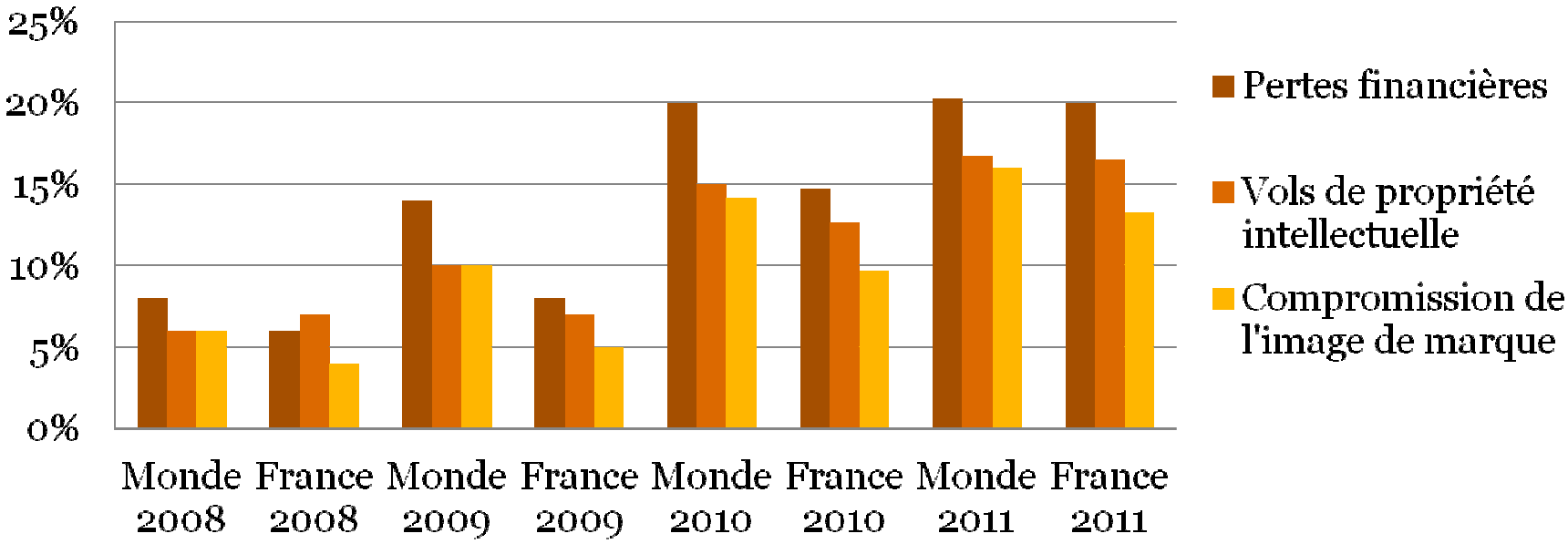
Q19: « Nombre des incidents de sécurité dans les 12 derniers mois ? »

Cette croissance du nombre d'incidents s'accompagne d'une augmentation continue de leurs impacts

Deux explications à cette tendance :

Les organisations connaissent mieux leurs incidents et donc leurs impacts

La menace et la surface d'exposition des entreprises augmentent



Q23 « quels ont été les impacts métiers des incidents ? » (pourcentage par rapport au nombre total d'entreprises ayant répondu à l'enquête)

Les Directions Générales veulent aujourd'hui s’assurer que la question de la sécurité de l’information est sous contrôle

Professeur Udo Helmbrecht
Directeur exécutif de l'ENISA

« **Gagner et maintenir la confiance** de nos citoyens dans le fait que leurs données sont protégées est un **facteur important pour le développement** et l'adoption de nouvelles technologies et des services en ligne en Europe. »

Les dirigeants découvrent un nouveau monde

Les dirigeants réalisent aujourd'hui que le cyberespace recèle d'énormes opportunités, mais aussi d'énormes risques, pouvant frapper très durement les entreprises.

Ce monde se caractérise par :

L'aspect global : un attaquant opérant depuis n'importe quel point du globe peut mettre en danger les systèmes d'information des entreprises

L'asymétrie : peu de gens avec peu de moyens peuvent provoquer en quelques heures des dégâts considérables pour les entreprises

L'effacement des frontières organisationnelles et techniques, du fait de nouveaux usages et modes de travail (cloud, virtualisation, etc.)

Les Directions Générales veulent aujourd'hui s'assurer que les risques Métiers liés à la sécurité des informations sont sous contrôle

- Le dispositif en place apporte-t-il le niveau approprié de maîtrise des risques Métiers liés à la sécurité des systèmes d'information ?
- Les risques liés aux nouvelles technologies, nouveaux marchés, nouveaux canaux et nouveaux usages sont-ils pris en compte ?
- Le Top Management dispose-t-il de la vision lui permettant de prendre les bonnes décisions stratégiques ?
- La sécurité aide-t-elle les Métiers à se développer de manière sécurisée ?
- La démarche Sécurité est-elle performante, efficace et efficiente ?

Une illustration de la perception des risques liés à la sécurité de l'information

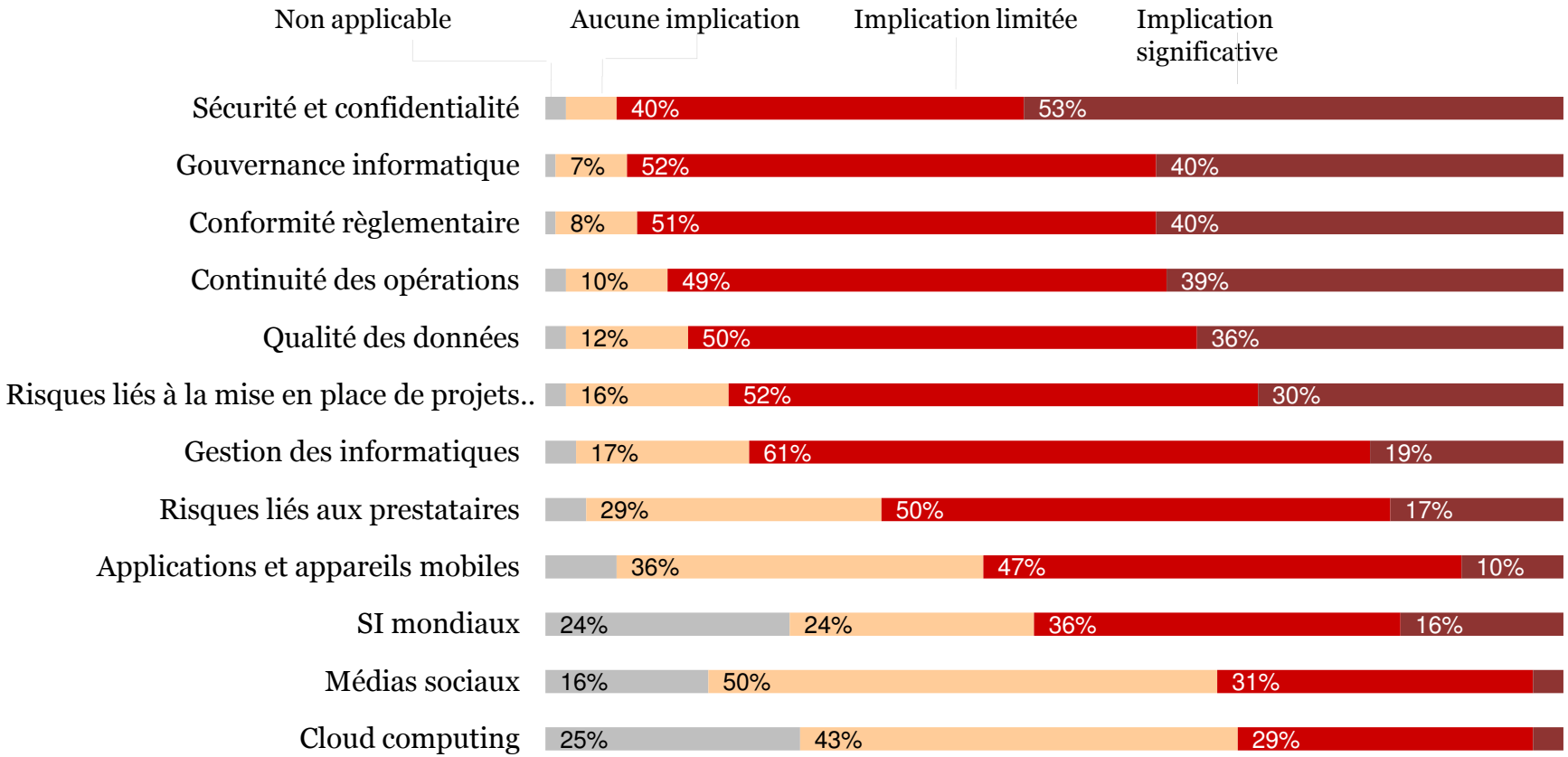
- Etude « World Economic Forum Global Risks 2011 Sixth Edition »
- Basée sur les réponses de 580 dirigeants et experts, venant du monde des affaires, gouvernemental ou académique
- Identifie 5 « risques à surveiller », ainsi classifiés en raison :

1) D'un haut niveau de variance dans les réponses
2) De niveaux de confiance faibles dans les réponses
3) D'impacts jugés sévères, inattendus ou sous-estimés.

L'un de ces cinq risques correspond à la sécurité dans le cyberespace.

Les fonctions de contrôle ne savent pas aujourd'hui répondre à toutes les questions des Directions Générales

« Quel est le niveau d'implication de l'Audit Interne sur les risques technologiques suivants ? »



Enquête PwC 2011 sur l'audit interne (disponible sur demande)

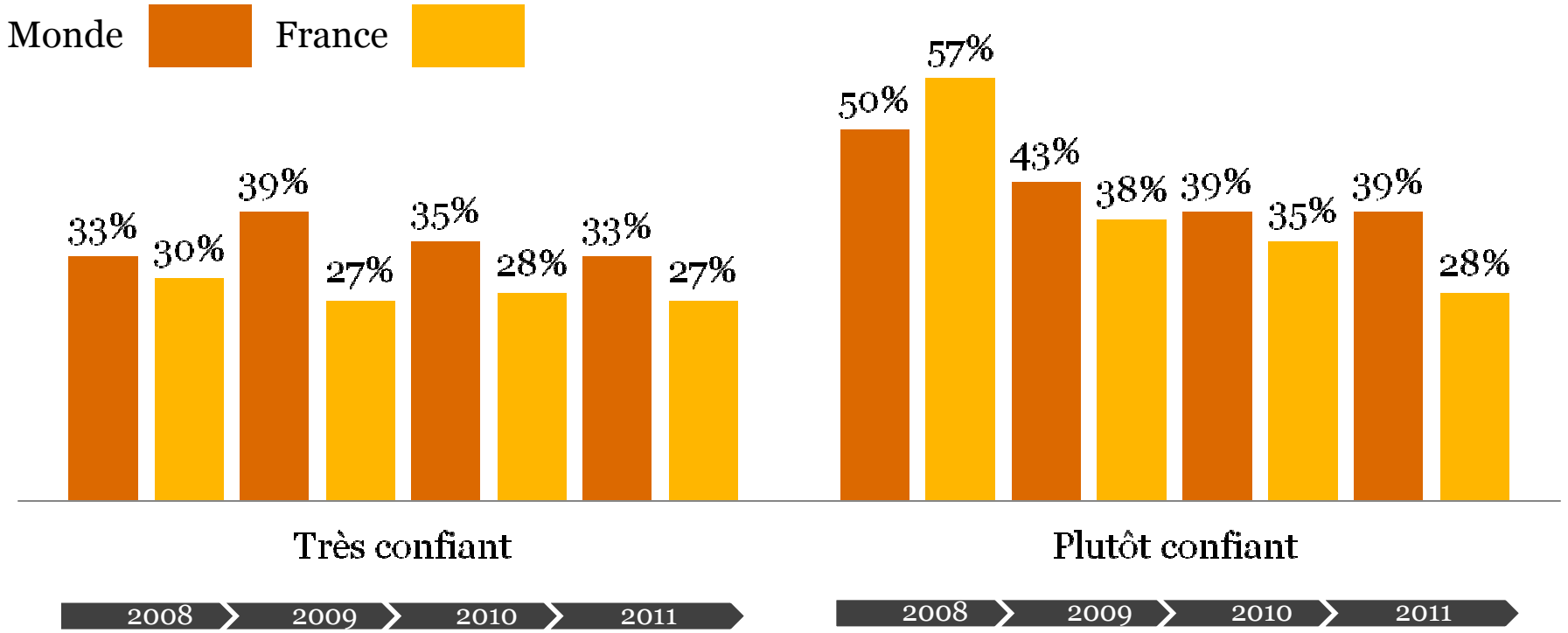
Et pourtant, le niveau de confiance des répondants dans l'efficacité de leur dispositif de sécurité est élevé

	Monde 2011	France 2011
Très confiant	33%	27%
Plutôt confiant	39%	28%
Total	72%	55%

Q35: « quel est le niveau de confiance quand à l'efficacité de vos activités en termes de sécurité de l'information »

… mais ce niveau de confiance décroit depuis plusieurs années

La décroissance du niveau de confiance concerne surtout les organisations « plutôt confiantes », c'est-à-dire celles qui n'ont pas mis en place de dispositif permettant d'objectiver ce niveau de confiance.

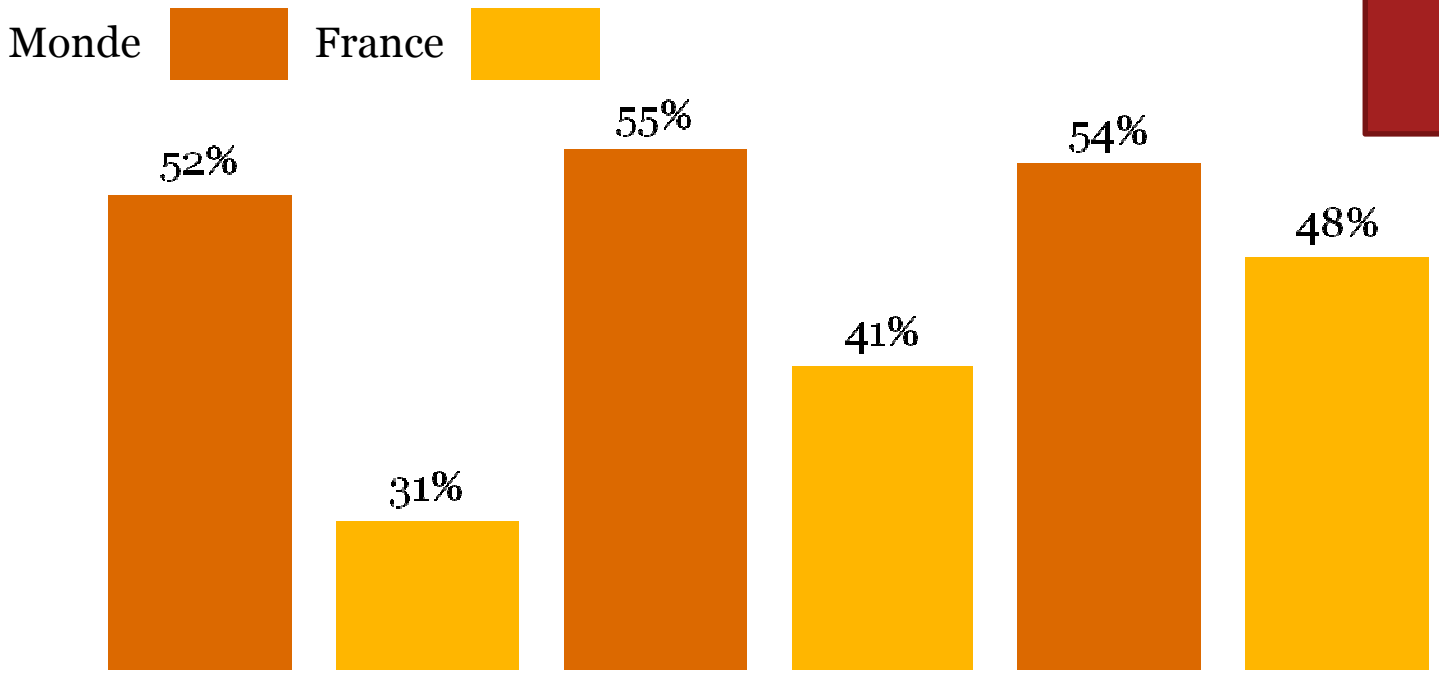


Q35: « Quel est le niveau de confiance quand à l'efficacité de vos activités en termes de sécurité de l'information ? «

Quel positionnement de la fonction Sécurité des Systèmes d'Information par rapport à ces évolutions ?

Une pérennisation du positionnement de la fonction sécurité des SI comme partenaire reconnu au sein des entreprises …

Le rattrapage de la France se poursuit



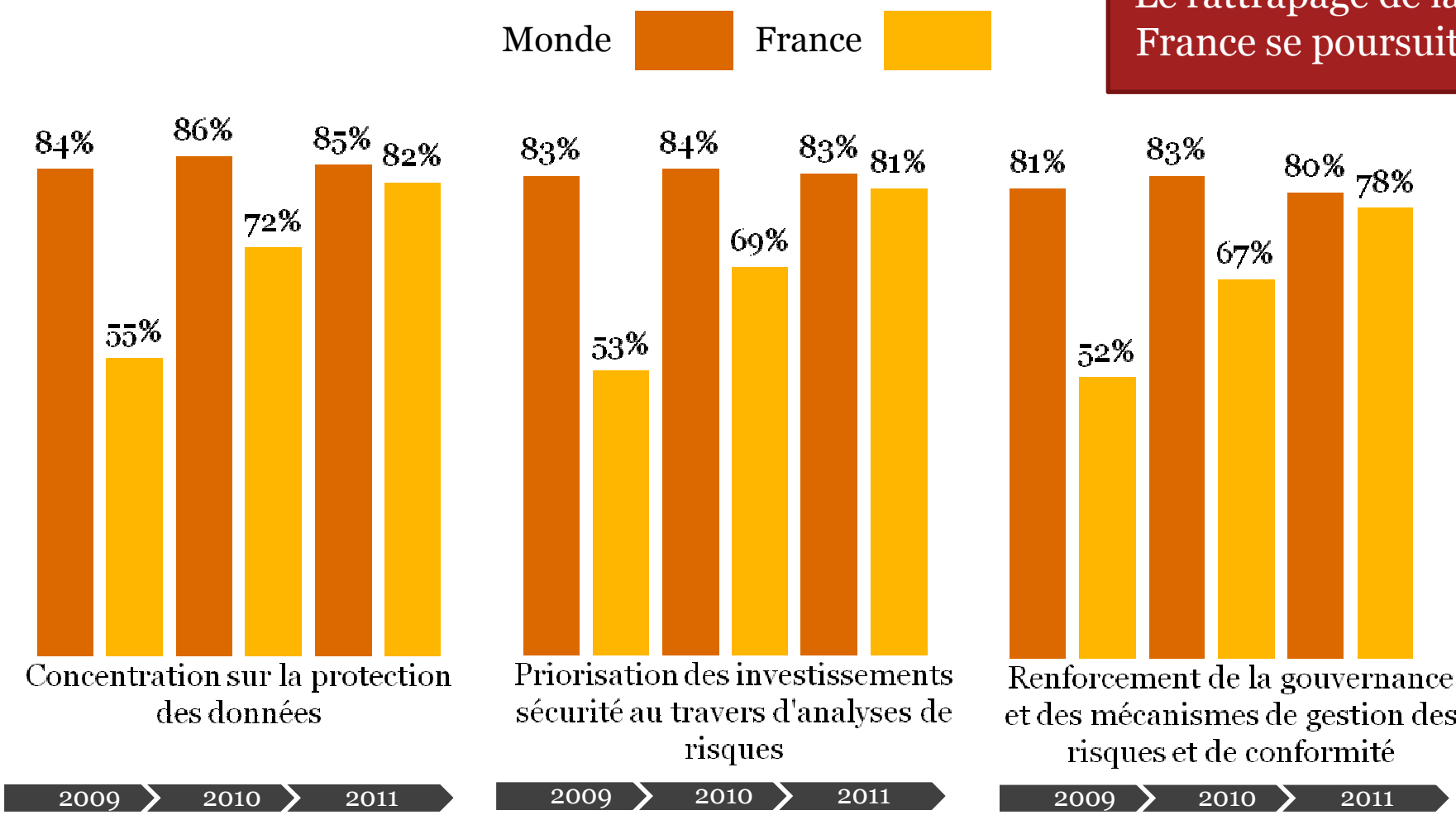
« Oui, l'augmentation des risques a mis en exergue le rôle et l'importance de la fonction sécurité »

2009 2010 2011

Q10 : « Quels impacts la crise économique actuelle a-t-elle eu sur la fonction sécurité de votre entreprise ? » : réponse « « L'augmentation des risques a mis en exergue le rôle et l'importance de la fonction sécurité »

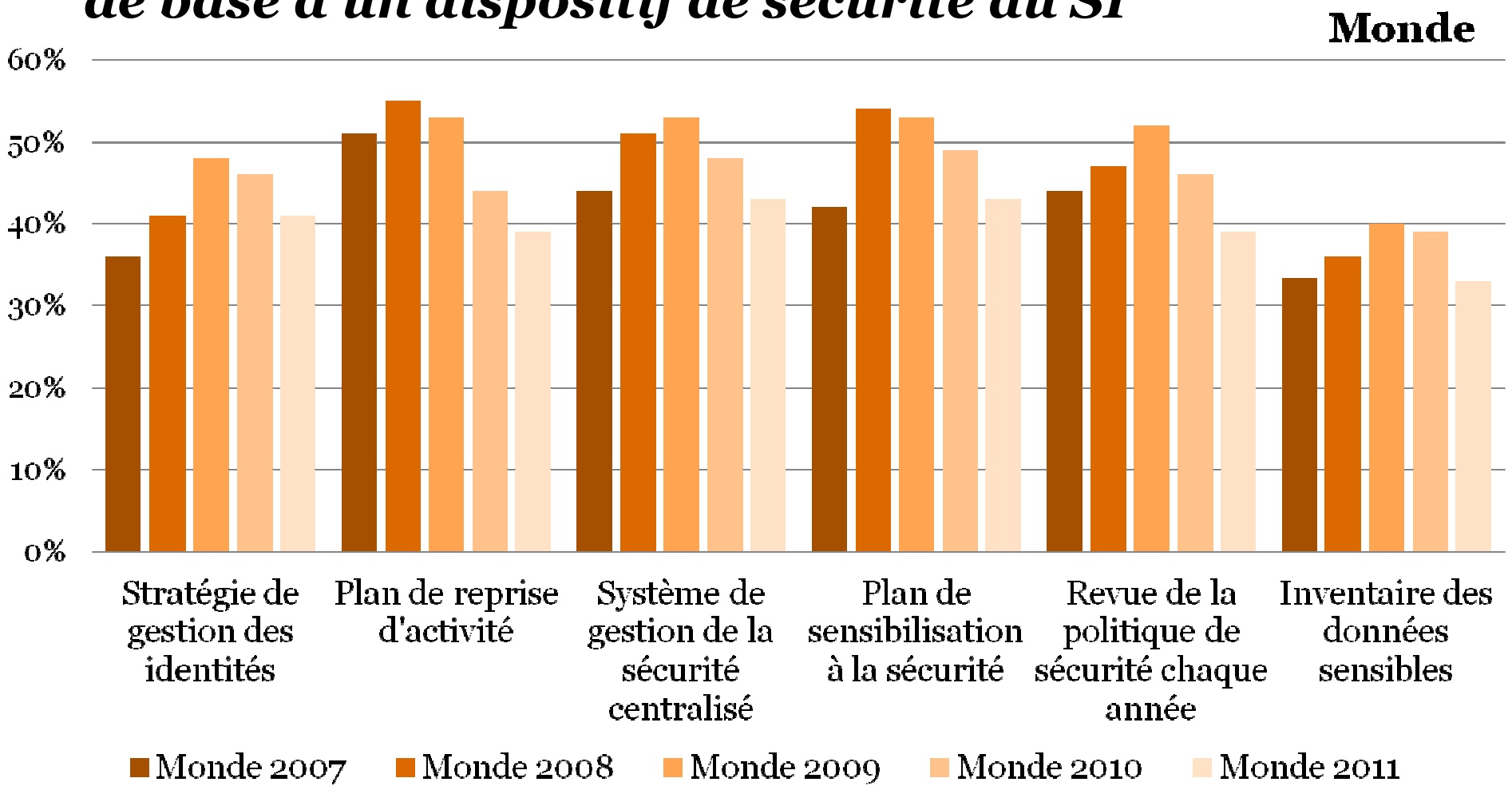
… couplée à une approche se focalisant sur les risques prioritaires

Le rattrapage de la France se poursuit



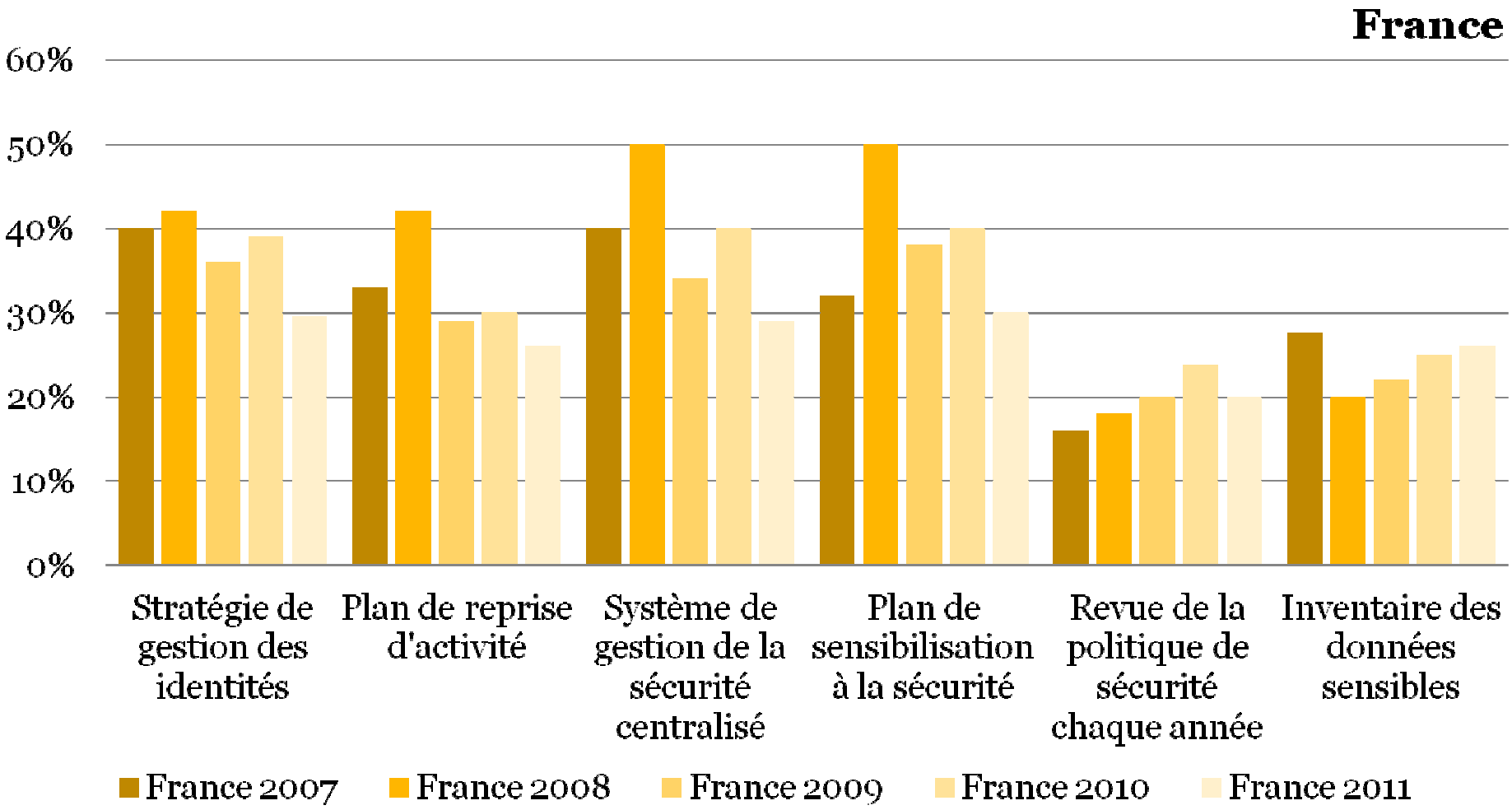
Q11 : « Quelle est l'importance des stratégies suivantes pour vous permettre d'atteindre vos objectifs de sécurité dans ce contexte de crise économique ?

Mais une tendance à la stagnation, voire à la dégradation des taux d'adoption des composants de base d'un dispositif de sécurité du SI



Q28 « Lesquels des éléments suivants sont inclus dans votre politique de sécurité ? ». Q17 « Quels processus de sécurité avez-vous mis en place ? ». Q18 « Quels dispositifs de sécurité avez-vous mis en place ? »

Tendance identique en France, avec des taux d'adoption largement inferieurs



Q28 « Lesquels des éléments suivants sont inclus dans votre politique de sécurité ? ». Q17 « Quels processus de sécurité avez-vous mis en place ? ». Q18 « Quels dispositifs de sécurité avez-vous mis en place ? »

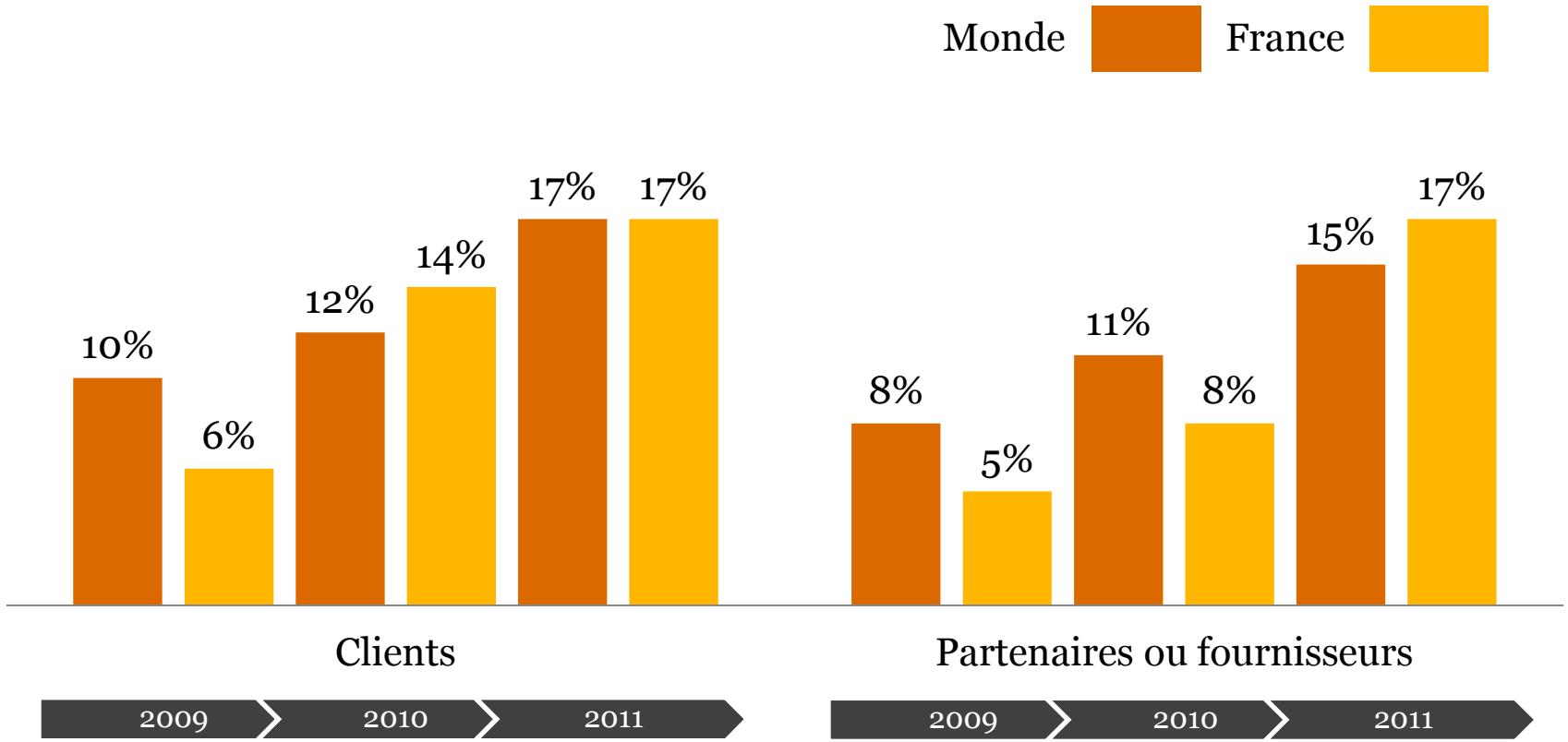
Ouverture du SI, mobilité, média sociaux, cloud computing : quelles approches et quels dispositifs ?

Dr. Gunter Bitz, Directeur de sécurité des produits, SAP AG

« La marche des affaires dans le cyberespace entraîne une modification **en profondeur** de notre façon de penser. Les utilisateurs deviennent de plus en plus nomades, dans un contexte de collaboration, de communication et de coopération poussée entre les organisations. Le rôle de la sécurité de l'information est de permettre aux utilisateurs de travailler de façon **sécurisée** en **tout lieu**, depuis n'importe quelle **plateforme** et avec **tout le monde**. »

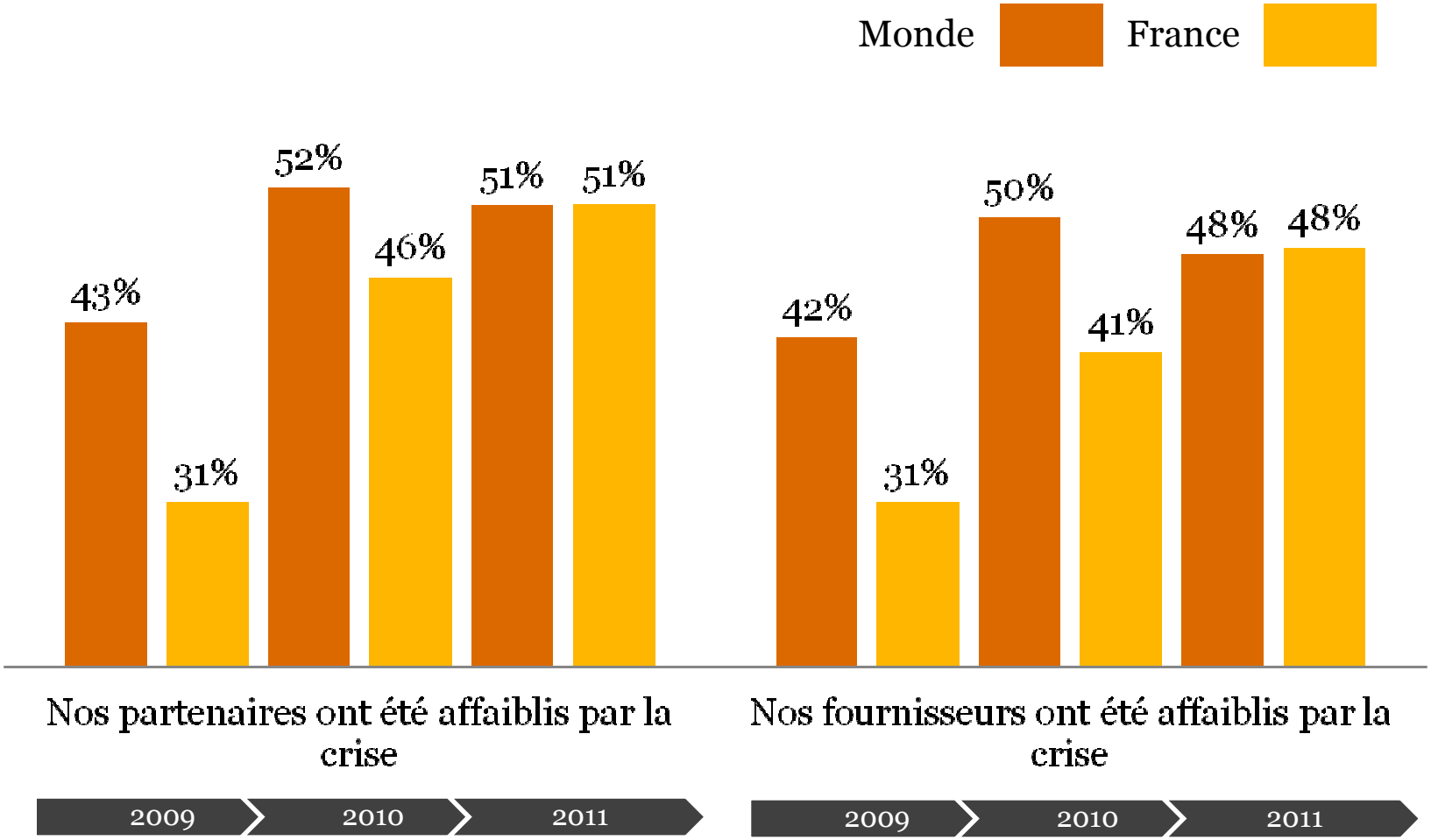
La gestion des risques de sécurité associés aux clients, partenaires et fournisseurs s'impose comme un sujet majeur

En quelques années, le nombre d'incidents liés à des partenaires, fournisseurs ou clients, a quasiment doublé.



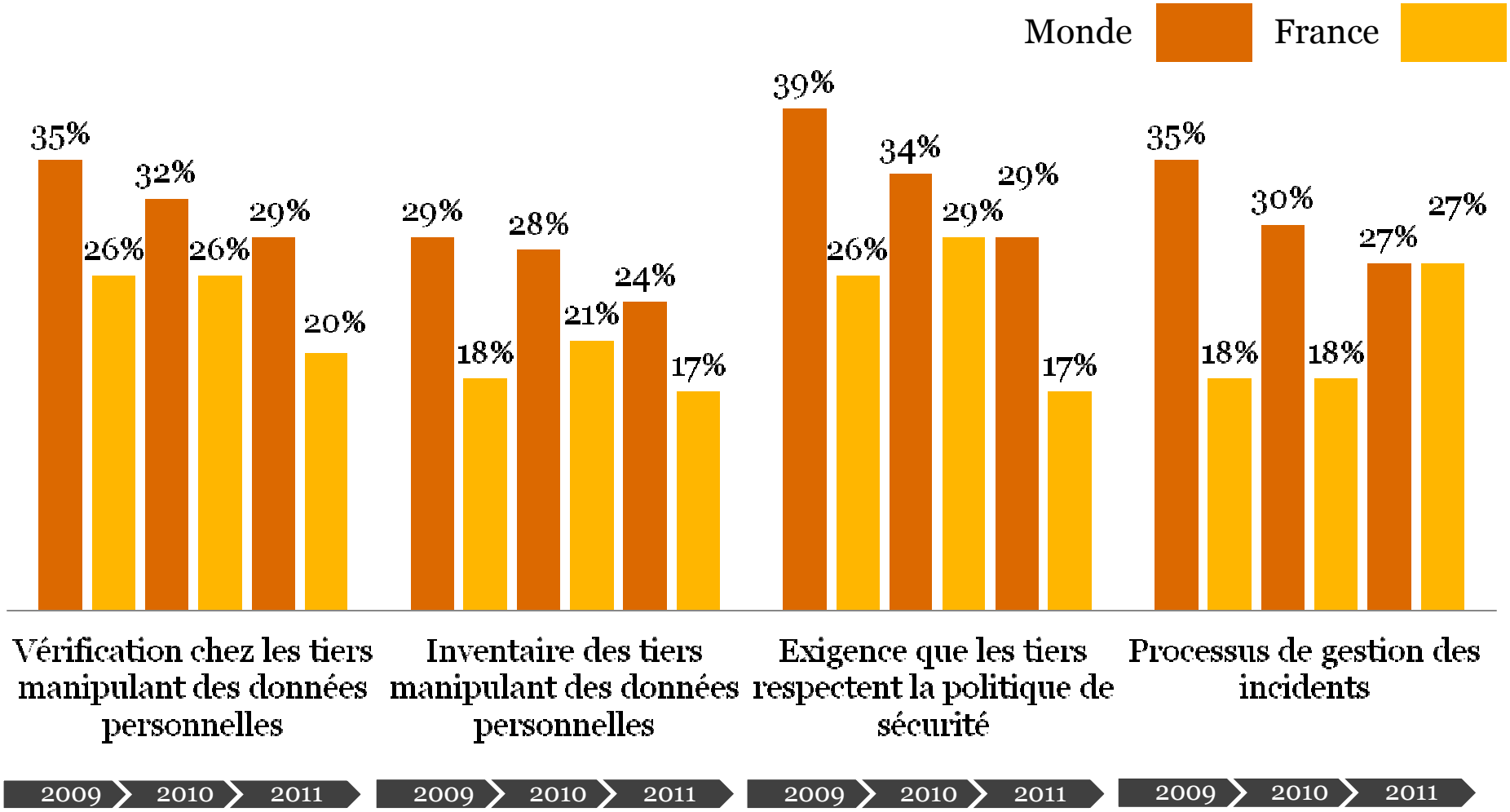
Q22: « Quelle est la source estimée des incidents ?»

La perception des risques liés aux partenaires et fournisseurs en augmentation notable pour la France



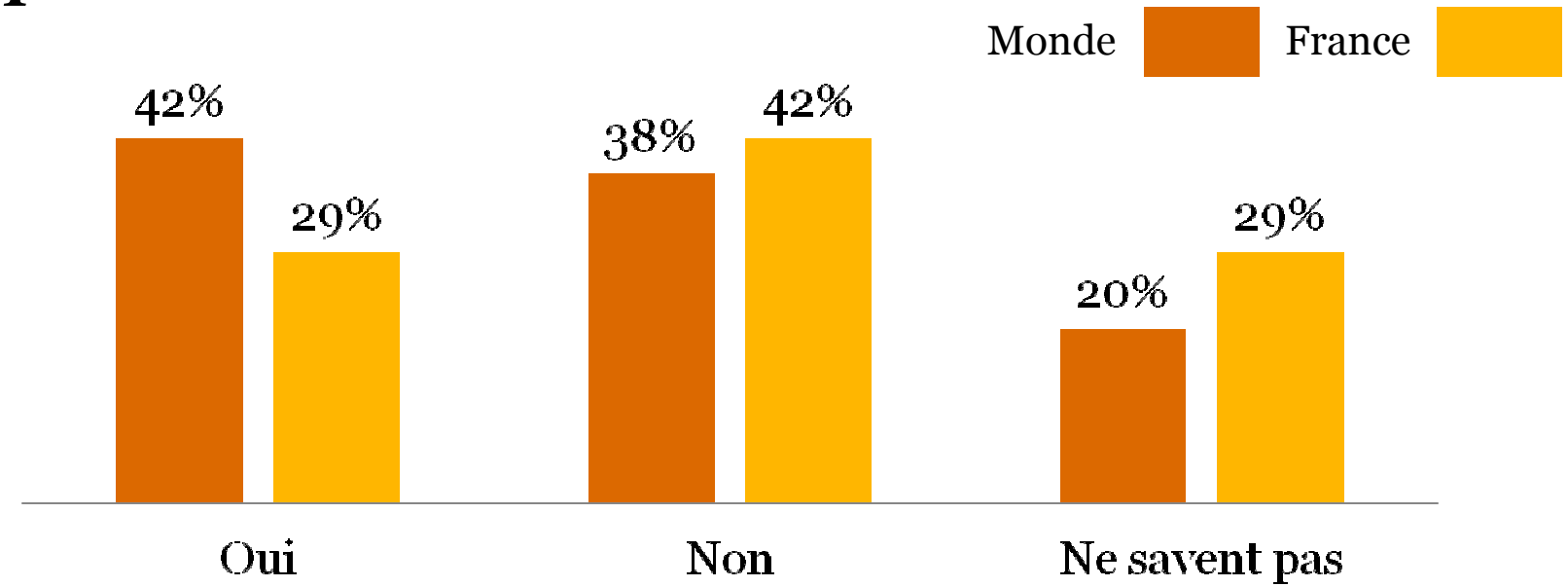
Q10: « Quels impacts les conditions économiques actuelles ont eu sur la fonction Sécurité ? »

Mais le niveau de préparation par rapport aux risques liés aux tiers se dégrade



Q15 : « quelles mesures de sécurité liée à la protection des données personnelles votre organisation a-t-elle mis en place ? »

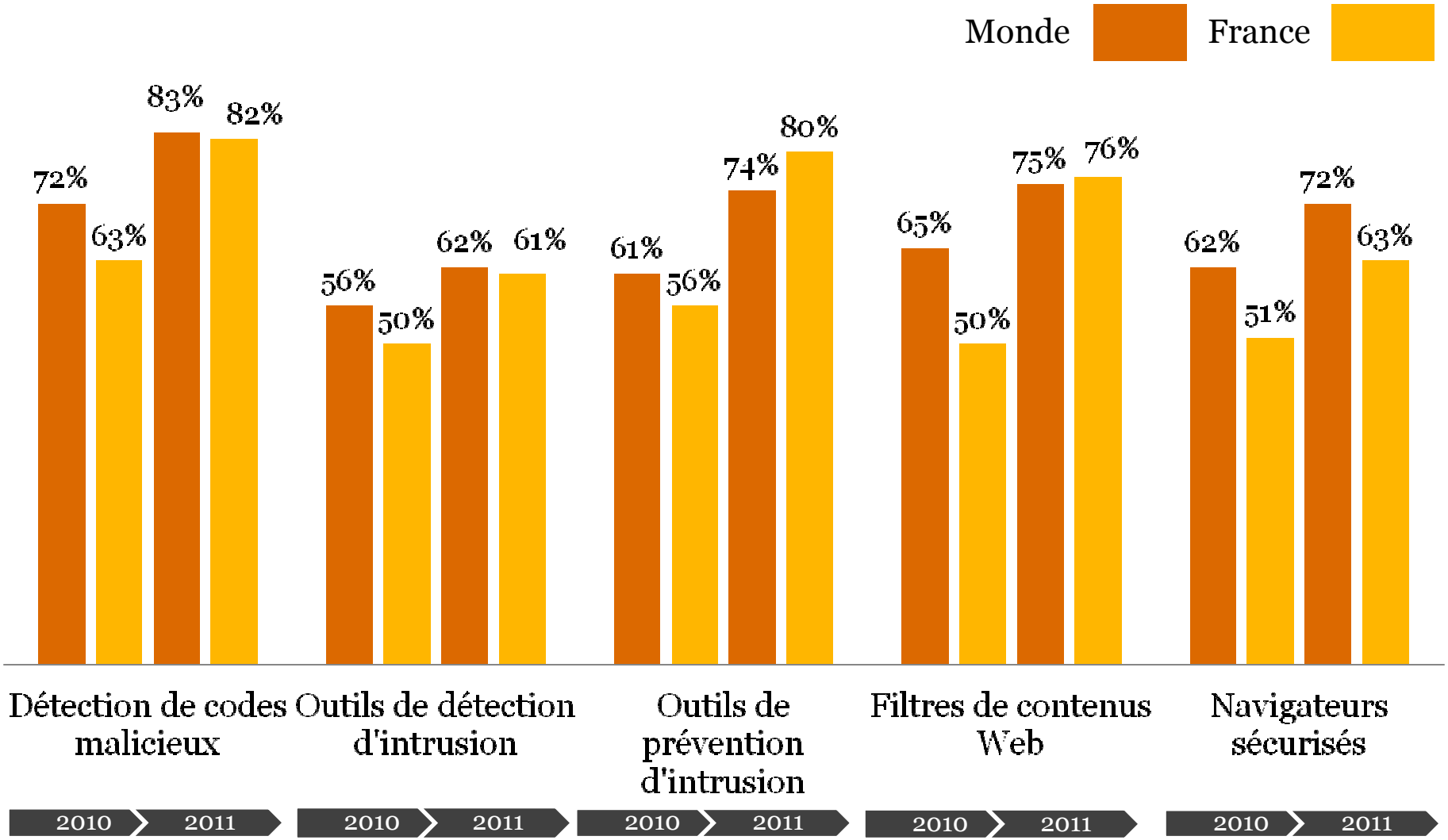
Le menace des Advanced Persistent Threats est un facteur de dépense pour une forte minorité de répondants



Advanced Persistent Threat : tentative sophistiquée et persistante d'accéder de façon ciblée à des informations au sein des SI

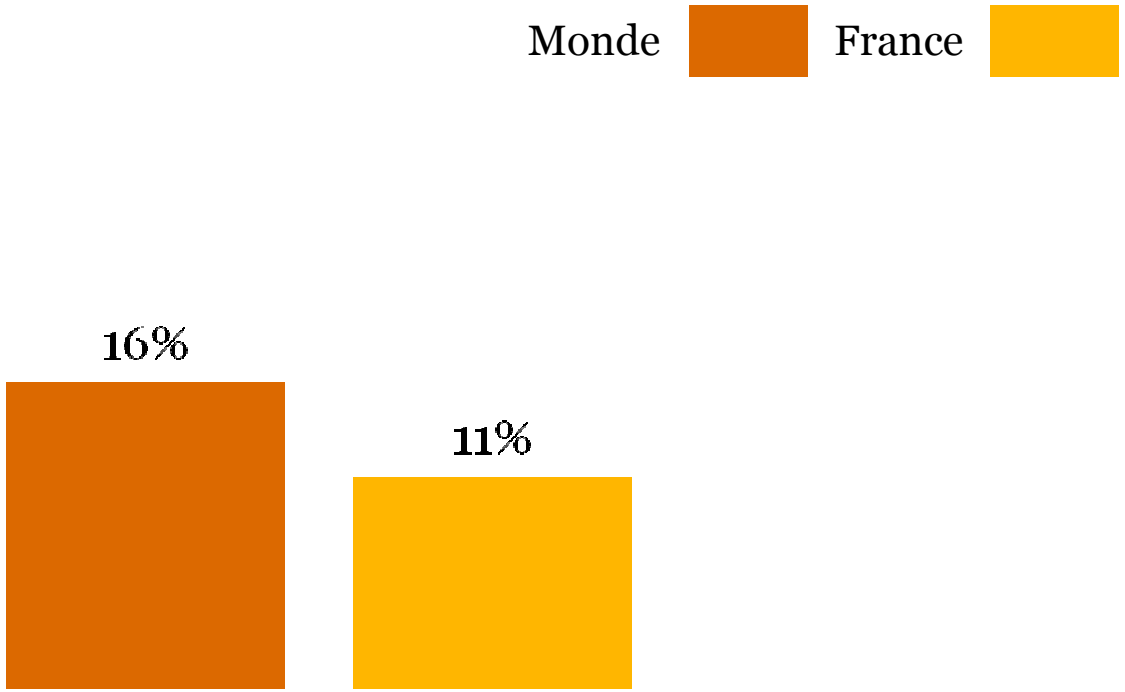
Q1Ret. « La menace APT influe-t-elle vos dépenses Sécurité ? »

… et l'adoption de dispositifs de lutte contre les APT est en croissance



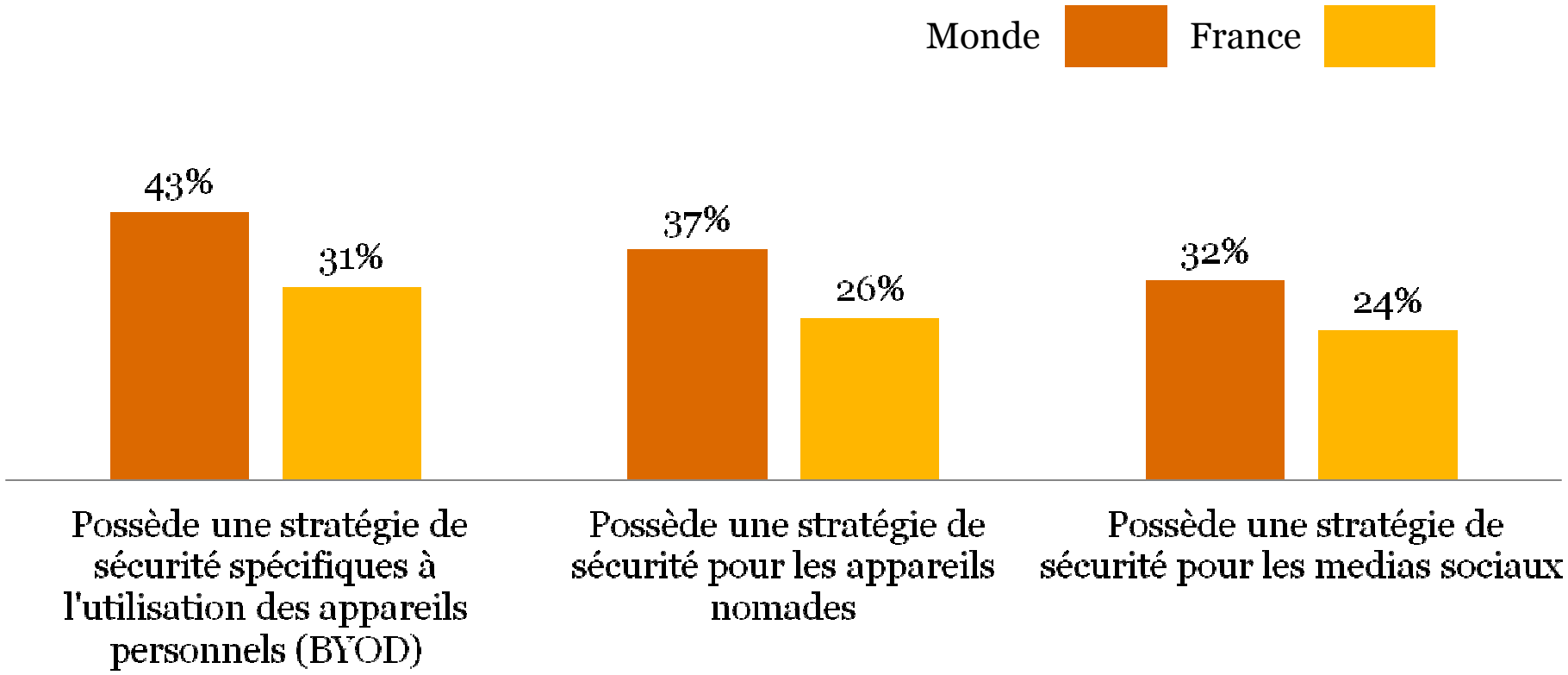
Q18 : « quelle s technologies de sécurité votre organisation a mis en place ? »

Mais peu d'organisations ont à ce jour défini une politique de sécurité spécifique aux APT



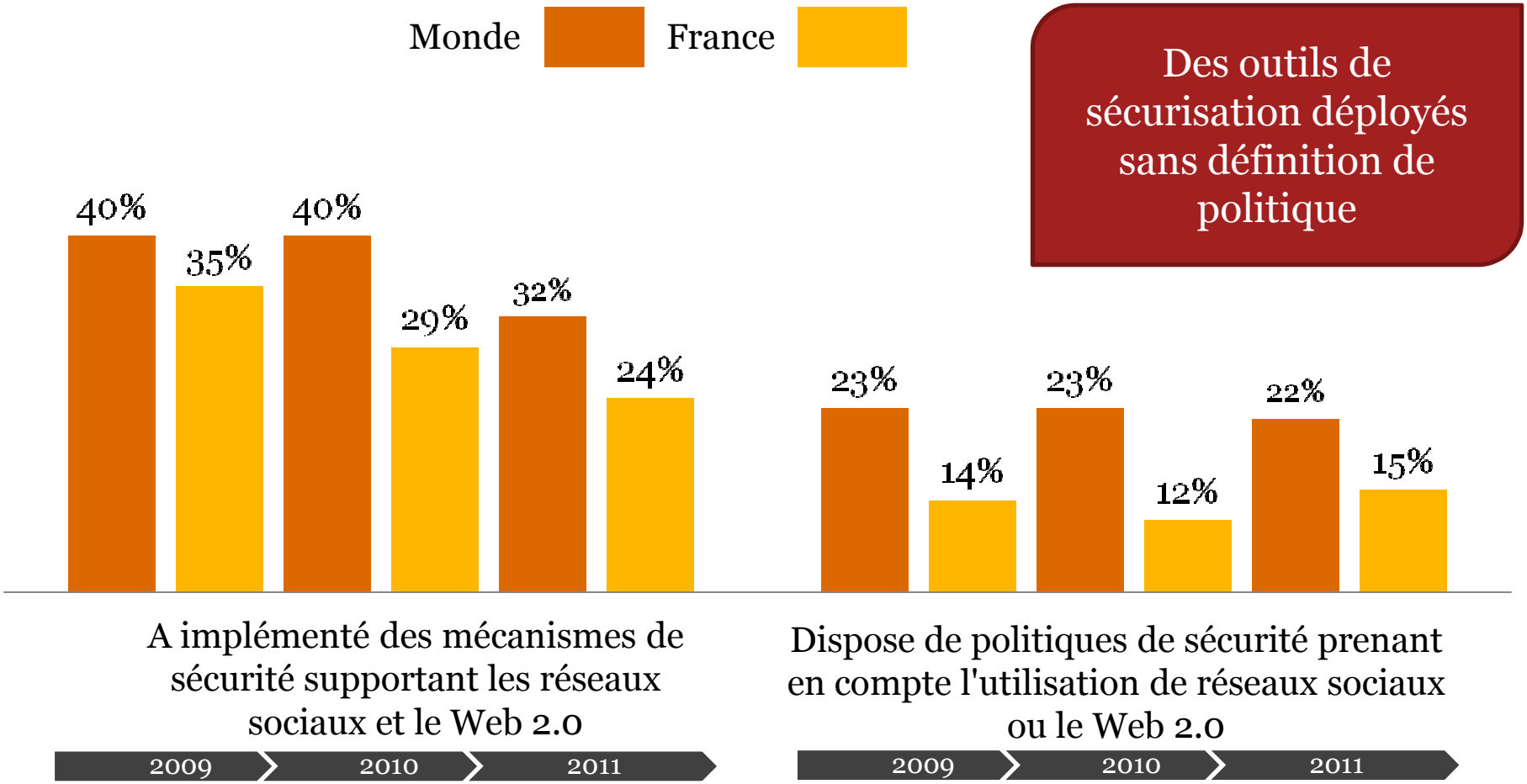
Q28. « Quels sont les éléments inclus dans votre politique de sécurité? » répondants ayant cité l'élément « APT »

La majorité des organisations n'a pas encore défini de stratégie face aux risques engendrés par les terminaux personnels, les appareils nomades et les média sociaux …



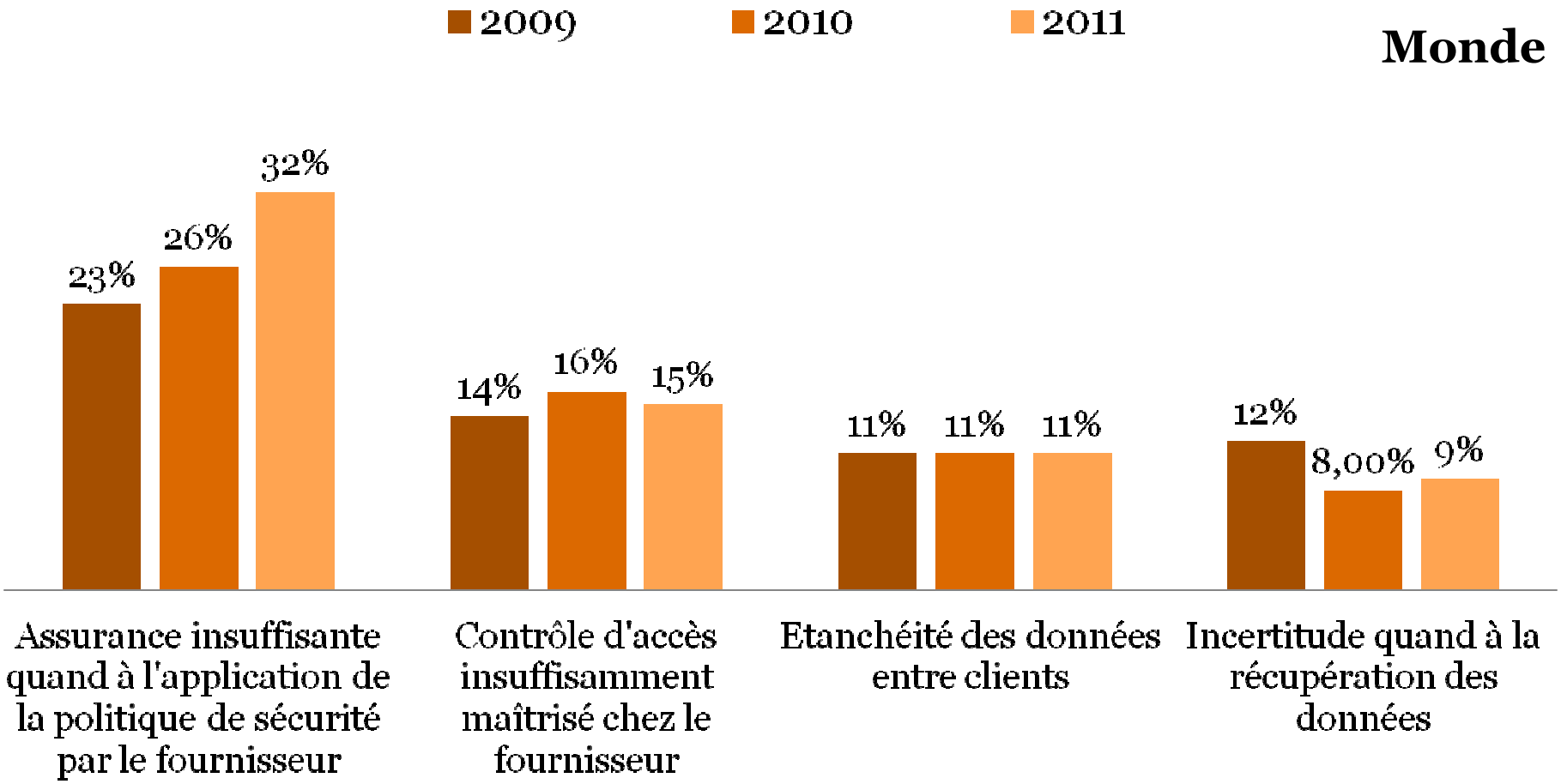
Q17: « quelles mesures de sécurité de type organisationnel votre organisation a mis en place ? »

… tandis que le taux d'adoption d'outils permettant de sécuriser ces technologies stagne



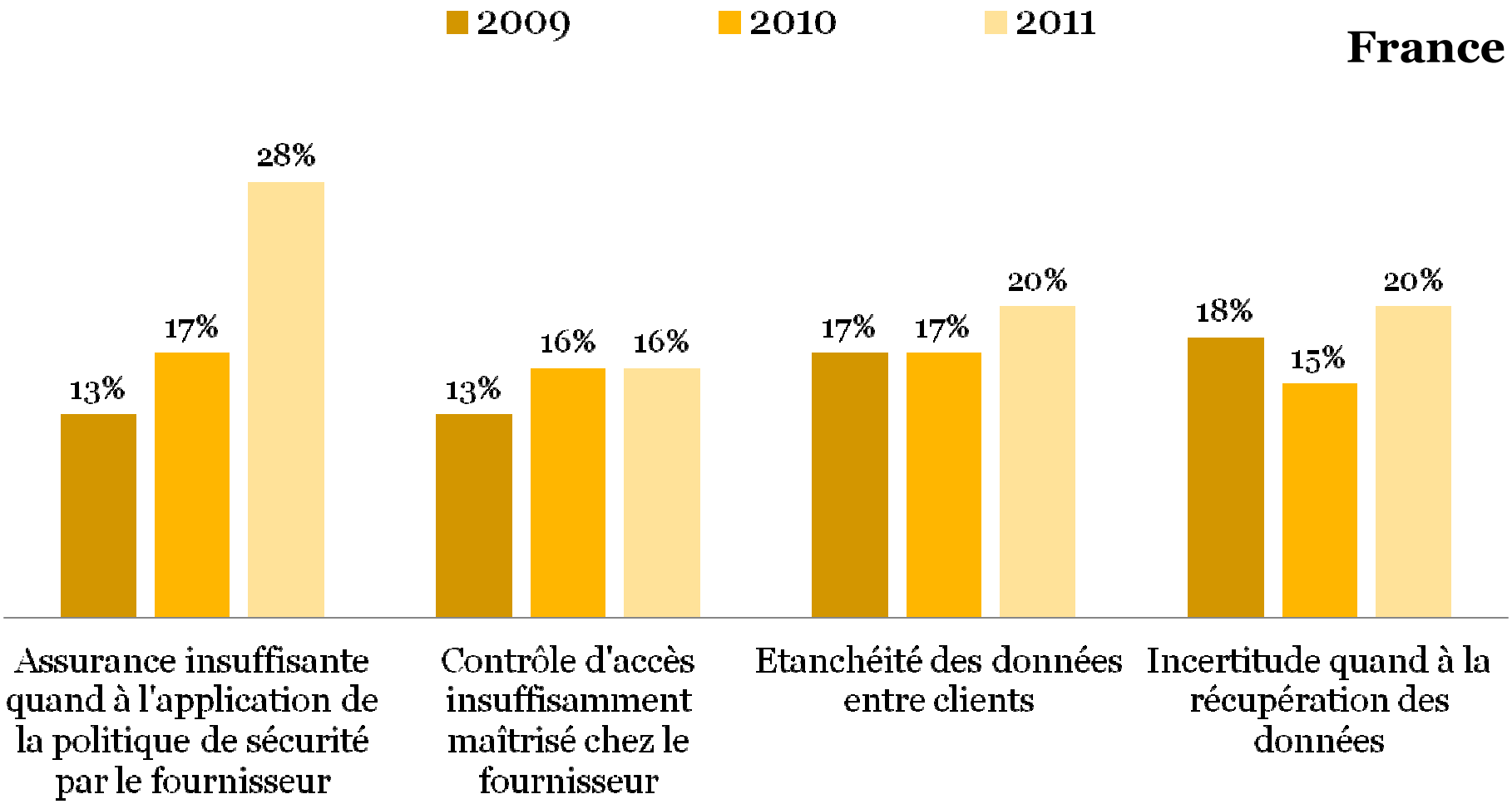
Q28. « Quels sont les éléments inclus dans votre politique de sécurité ? ». Q18 « Quels dispositifs de sécurité avez-vous mis en place ? ».

Les niveaux de risques perçus liés à la sécurité du Cloud Computing ne décroissent pas



Q42: « Quels sont les plus grands risques par rapport à votre stratégie Cloud Computing ? »

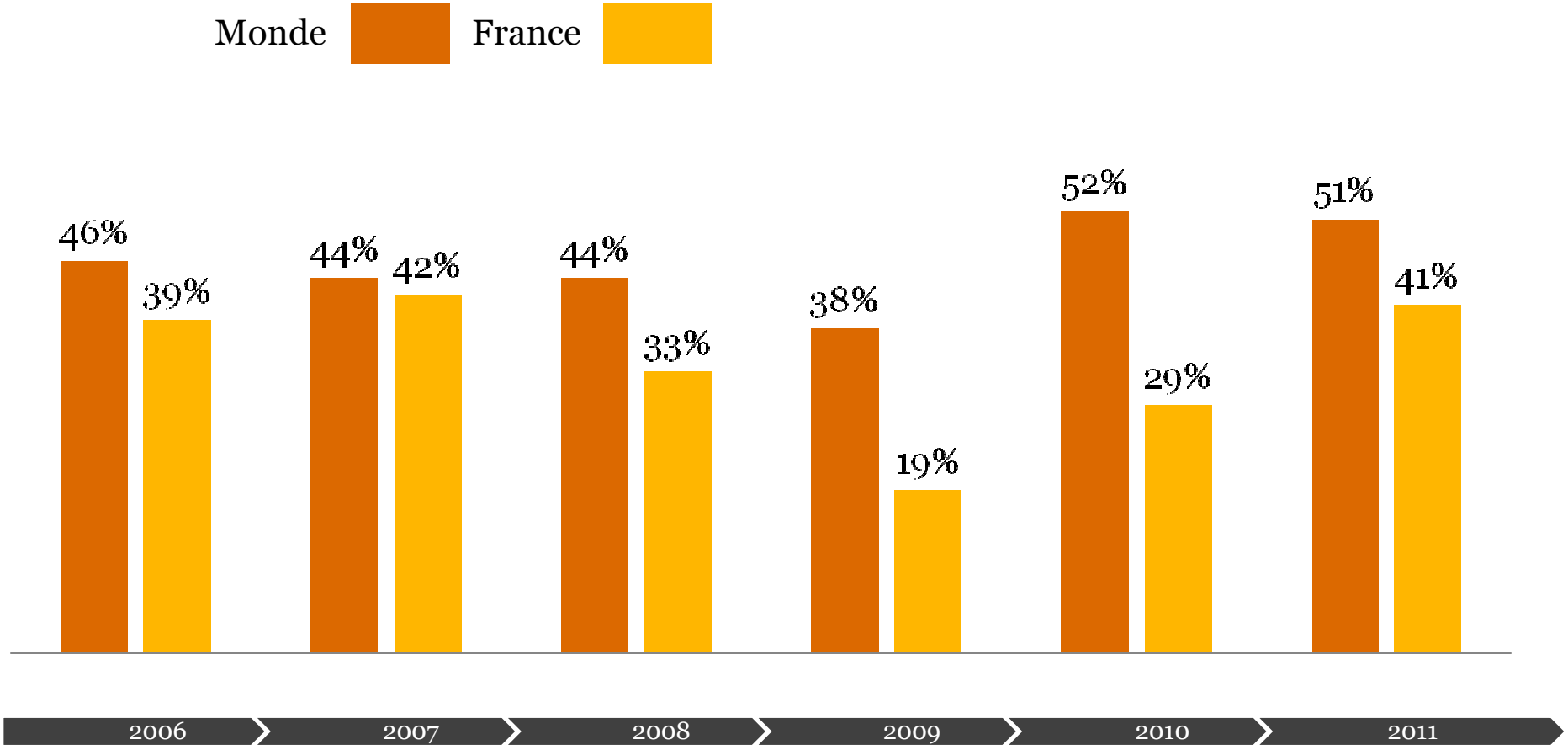
Les niveaux de risques perçus liés à la sécurité du Cloud Computing ne décroissent pas



Q42: « Quels sont les plus grands risques par rapport à votre stratégie Cloud Computing ? »

Quels facteurs d'influence et de contraintes pour la fonction Sécurité ?

En termes de budget, l'optimisme est toujours de mise, et la France tend à rattraper son retard …



Q9: « Par rapport à l'année dernière, les dépenses de sécurité sur les 12 prochains mois vont : » total des réponses « augmenter de 0 à 10% », « augmenter de 11 à 30% », « augmenter de plus de 30% »

… mais les conditions économiques s'imposent comme le principal facteur d'influence des dépenses sécurité

Les autres facteurs « classiques » continuent leur décroissance au niveau Monde

Facteurs de dépenses	2008	2008 France	2009	2009 France	2010	2010 France	2011	2011 France	Tendance	Tendance France
Conditions économiques	n/a	n/a	39%	21%	49%	41%	**50%**	**41%**	***28%***	***95%***
Continuité d'activité	57%	54%	41%	23%	40%	22%	**34%**	**24%**	***-40%***	***-56%***
Image de l'entreprise	39%	32%	32%	20%	35%	23%	**32%**	**26%**	***-18%***	***-19%***
Conformité aux politiques internes	46%	43%	38%	34%	34%	27%	**29%**	**22%**	***-37%***	***-49%***
Conformité réglementaire	44%	45%	37%	29%	33%	33%	**27%**	**21%**	***-39%***	***-53%***
Besoin client	31%	22%	34%	24%	41%	30%	**38%**	**34%**	***23%***	***55%***

Q32: "Quels facteurs ou problématiques métiers influencent vos dépenses de sécurité? »

… et dans les faits, les contraintes budgétaires touchent plus d'entreprises, notamment en France

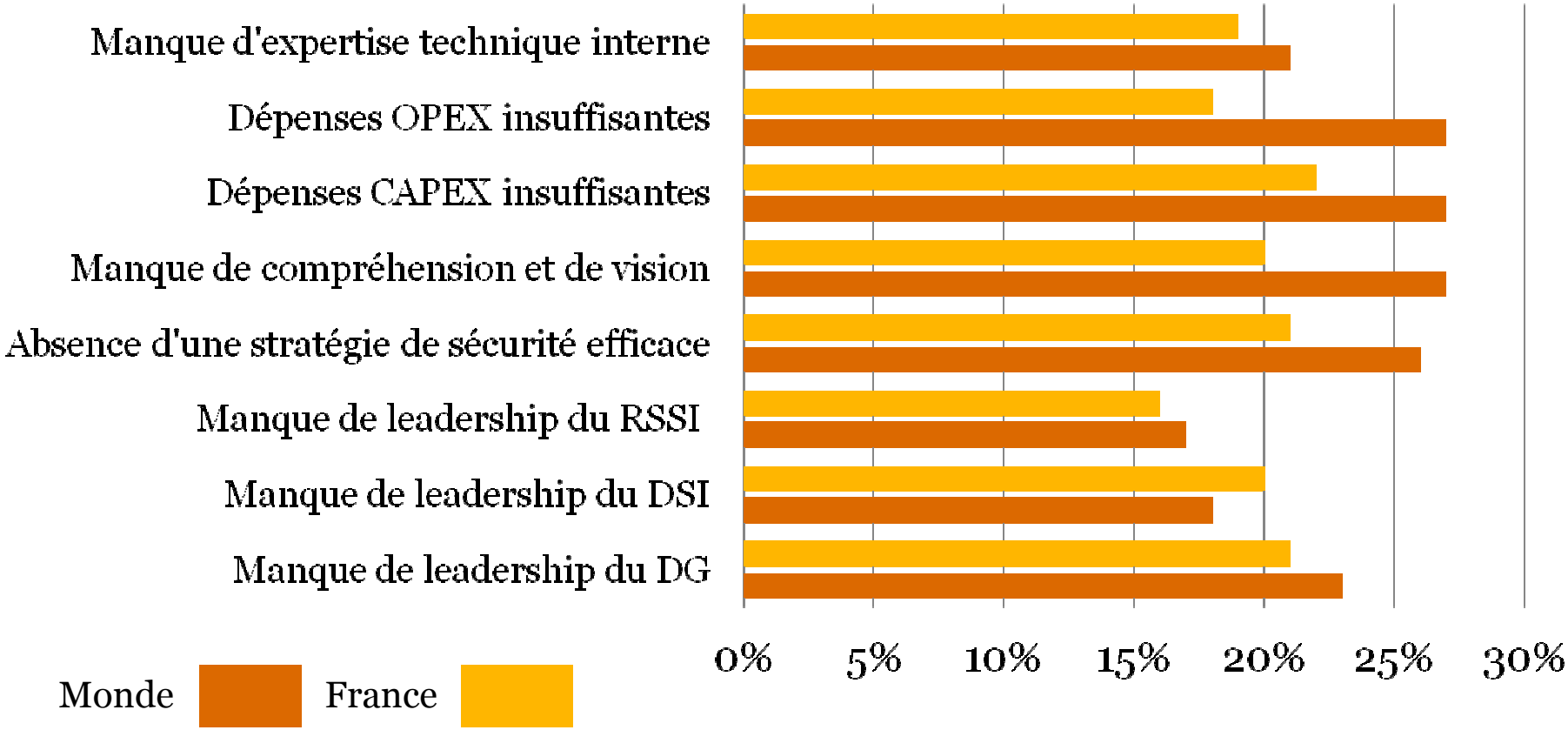
Votre entreprise a-t-elle différé des dépenses sécurité ?	2009	2010	2011
Investissements			
Global	43%	46%	**51%**
France	38%	42%	**54%**
Opérations courantes			
Global	40%	42%	**42%**
France	32%	38%	**55%**

Votre entreprise a-t-elle réduit ses dépense sécurité ?	2009	2010	2011
Investissements			
Global	47%	47%	**51%**
France	38%	42%	**57%**
Opérations courantes			
Global	46%	46%	**50%**
France	35%	40%	**56%**

Q12: "Votre entreprise a-t-elle repoussé des projets sécurité ?"

Q13: "Votre entreprise a-t-elle réduit des budgets sécurité ?"

Au-delà des budgets, les avis sur les obstacles majeurs à l'efficacité de la sécurité des SI sont variés



Q27n11. « Quels sont les plus grands obstacles à l'amélioration de l'efficacité de la fonction Sécurité »

La diversité des réponses selon les fonctions fait apparaître des lignes de forces intéressantes

	DG	DAF	DSI	RSSI
Manque de leadership du DG	25%	27%	25%	25%
Manque de leadership du DSI	14%	23%	18%	21%
Manque de leadership du RSSI	12%	22%	16%	17%
Absence d'une stratégie de sécurité efficace	18%	25%	25%	30%
Manque de compréhension et de vision	17%	25%	30%	37%
Budget CAPEX insuffisant	27%	23%	29%	29%
Budget OPEX insuffisant	23%	16%	23%	22%
Manque d'expertise technique interne	23%	19%	25%	23%
Système d'information peu intégré ou trop complexe	13%	14%	19%	30%

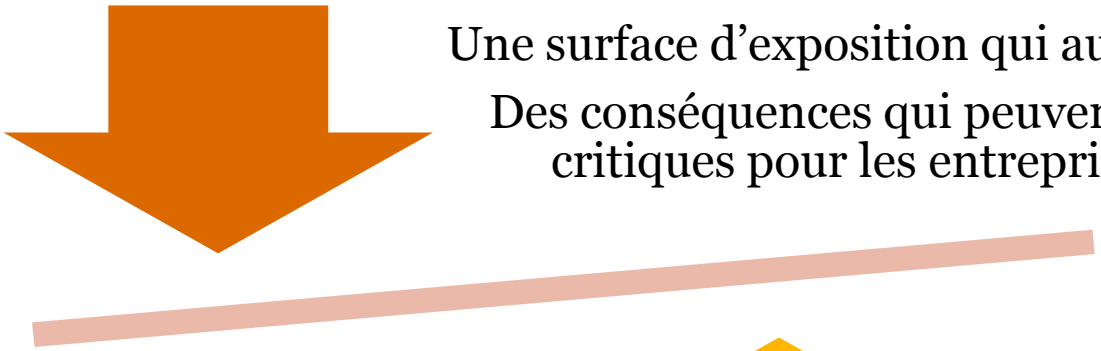
Le manque de CAPEX est vu comme important, notamment par les DG …

…mais le manque de vision et de leadership de la DG est également un facteur majeur

Q27n11. « Quels sont les plus grands obstacle à l'amélioration de l'efficacité de la fonction Sécurité »

Une nouvelle génération de leaders

Une équation difficile à résoudre



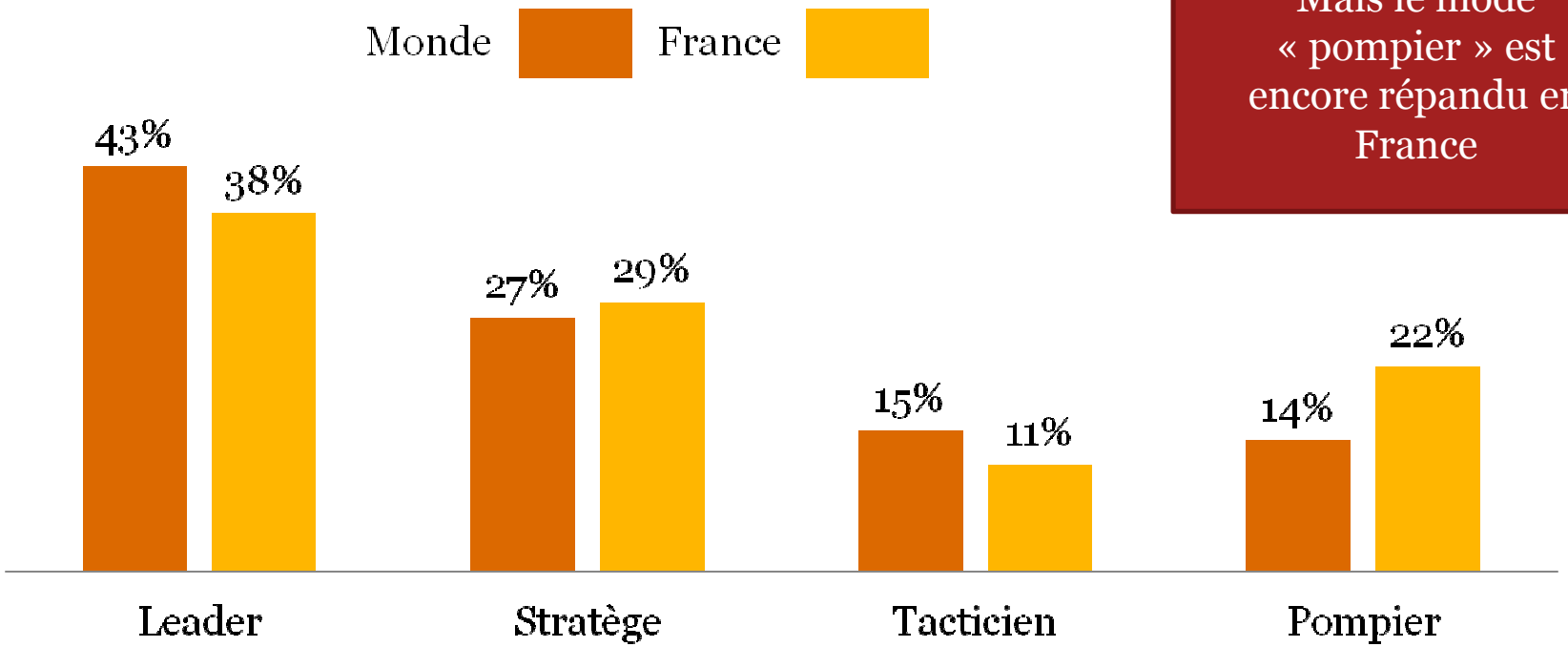
Une surface d'exposition qui augmente

Des conséquences qui peuvent être critiques pour les entreprises

Des moyens sous contraintes

Que peuvent nous apprendre les leaders ?

Une majorité des répondants se voit dans le groupe de tête en terme de performance de la fonction Sécurité



Mais le mode « pompier » est encore répandu en France

Quelle description correspond le mieux à l'approche de la sécurité de votre organisation ?

Pour les leaders, le "besoin client" est le facteur d'influence le plus important pour justifier les dépenses de sécurité

	Leaders	Stratèges	Tacticiens	Pompiers
Besoin client	50%	32%	27%	21%
Conformité réglementaire	45%	36%	44%	24%
Jugement professionnel	43%	36%	37%	22%
Exposition aux risques	41%	30%	40%	22%
Pratique de place	41%	35%	30%	17%

Q33. Comment les dépenses de sécurité sont justifiées dans votre organisation ?

Quatre point clefs pour viser le leadership

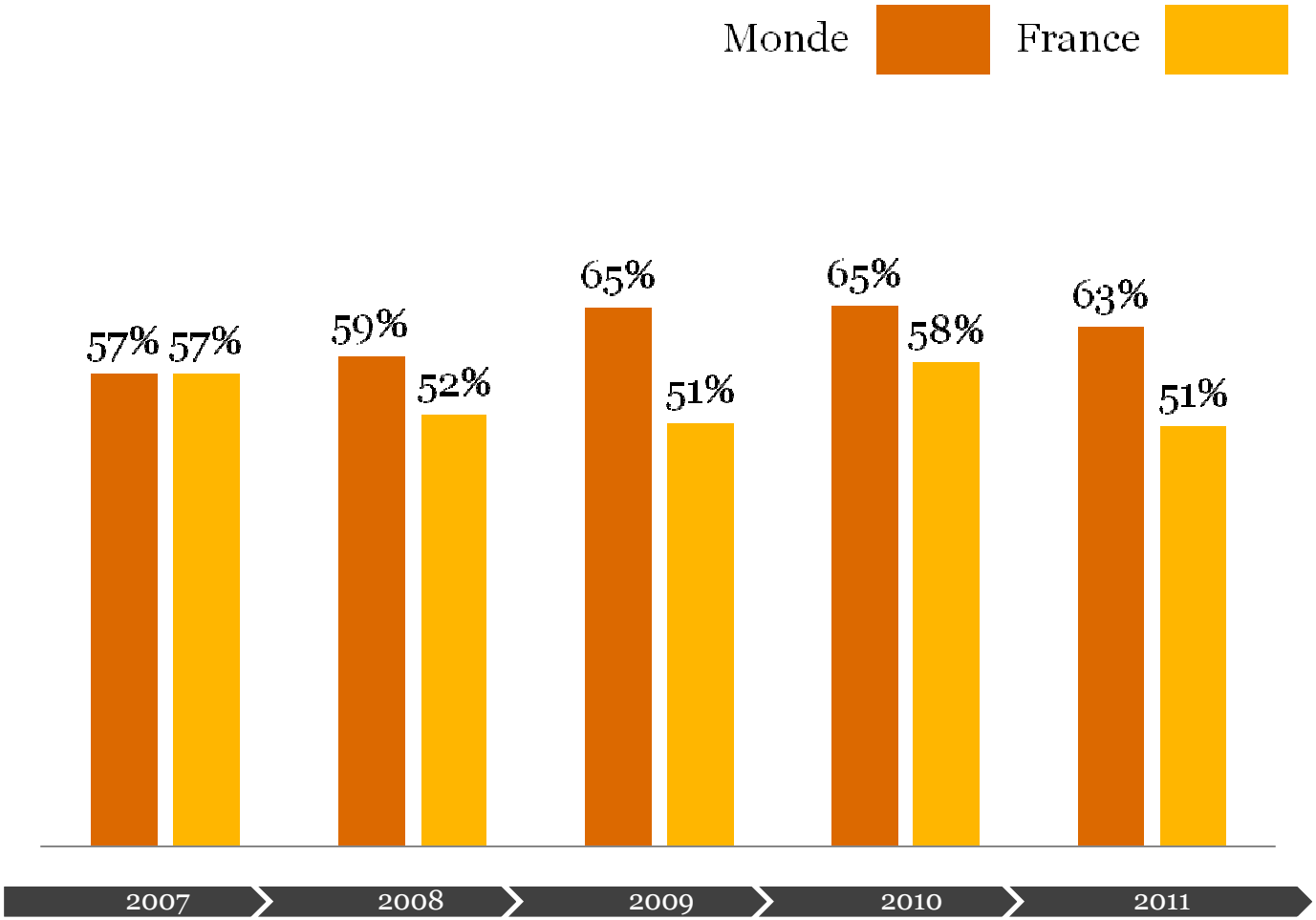
1. Une stratégie globale de sécurité de l'information

2. Une personne en charge de la sécurité de l'information qui rapporte à un membre du Top Mangement (DG, DAF, Secrétaire Général, …)

3. Une revue annuelle de l'efficacité du dispositif de sécurité de l'information

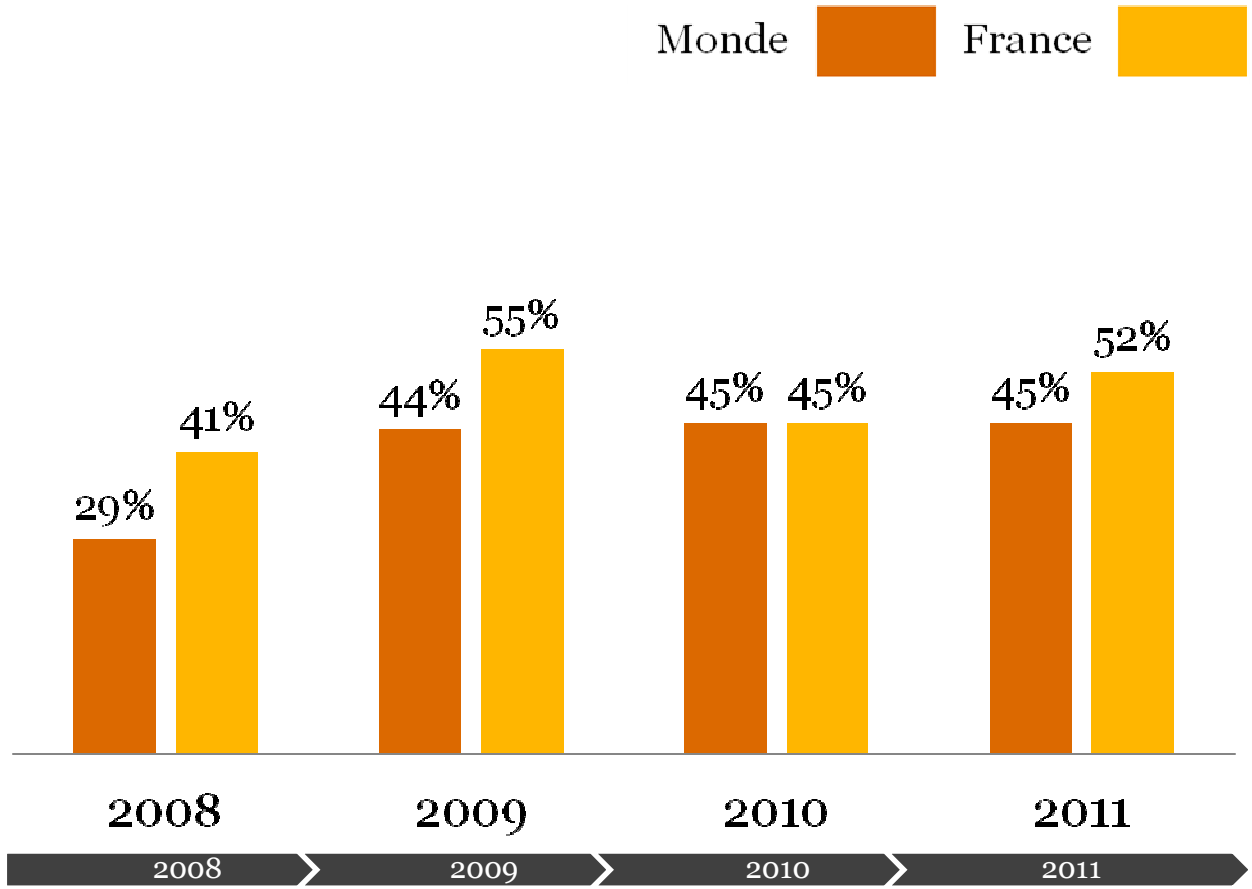
4. Une connaissance des incidents de sécurité ayant touché l'organisation

1. Une stratégie globale de sécurité de l'information



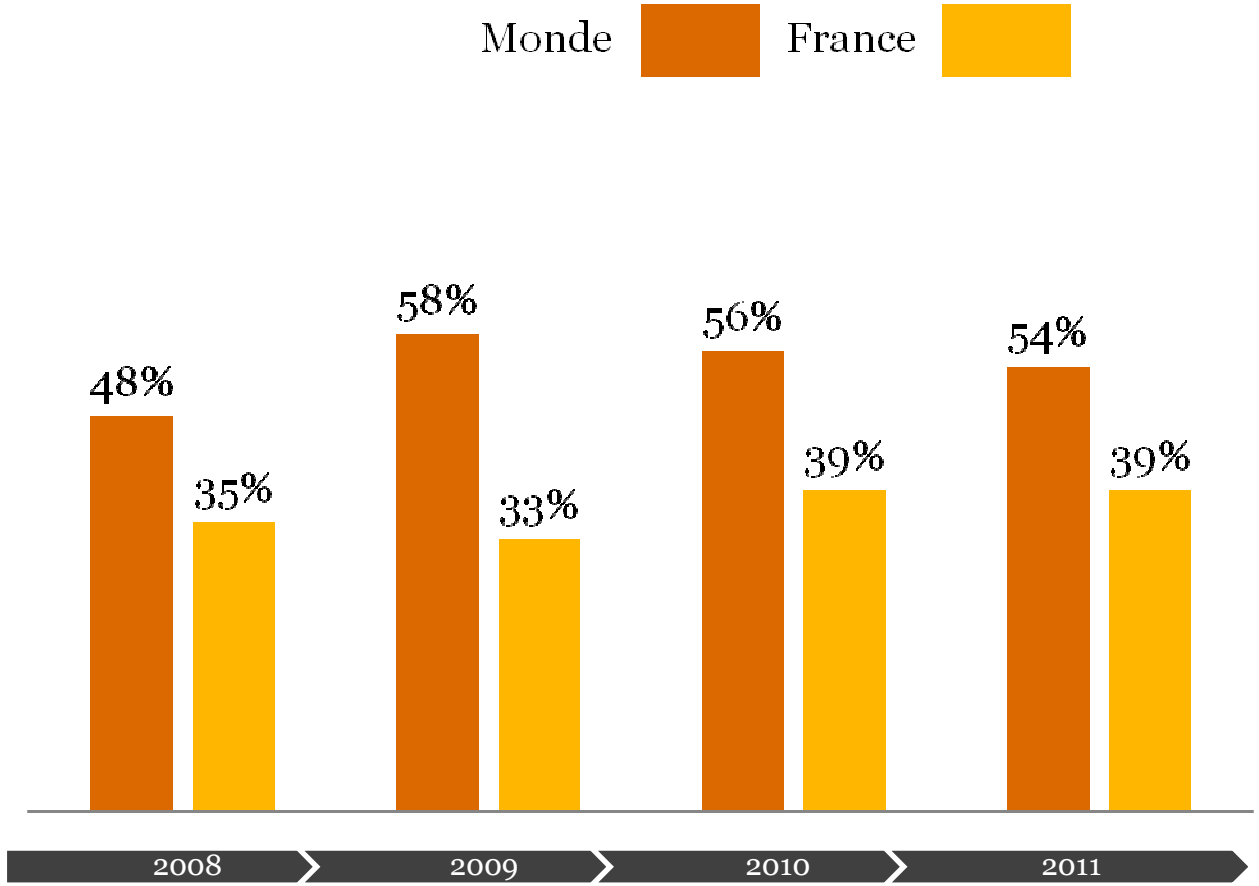
Q17 : « Quel processus de type stratégie et standard sont en place ? »

2. Une personne en charge de la sécurité de l'information qui rapporte à un membre du Top Management



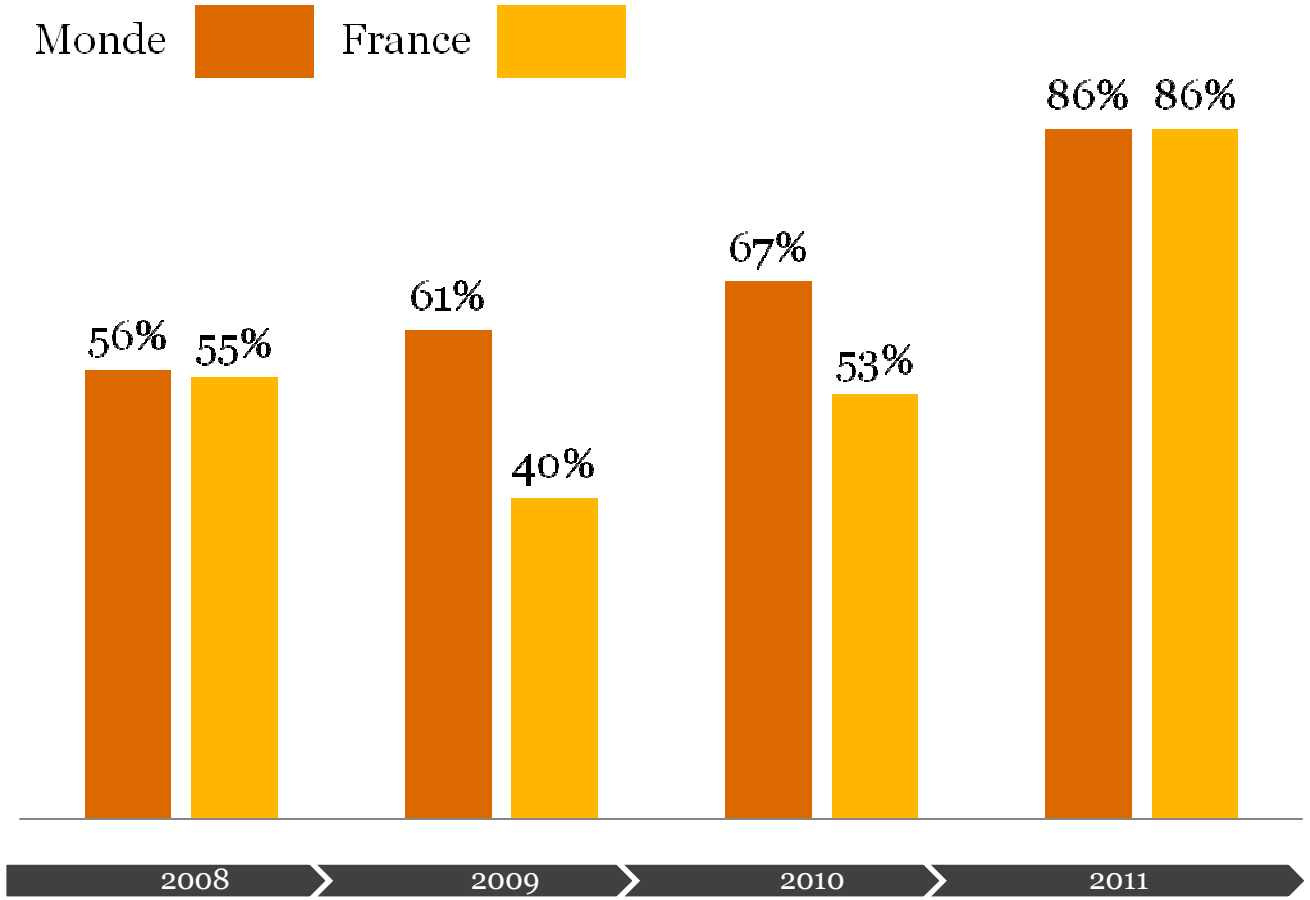
Q16a. « a qui rapporte le responsable de la fonction Sécurité »

3. Une revue annuelle de l'efficacité du dispositif de sécurité de l'information



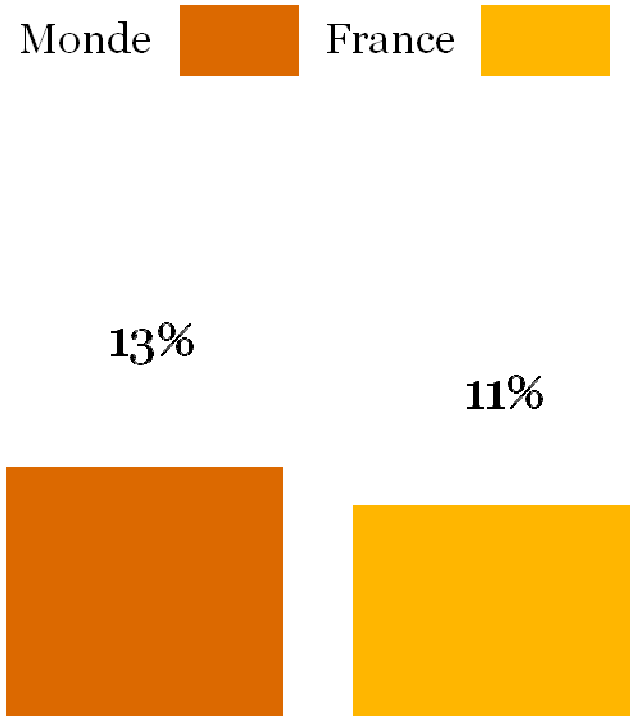
Q27. « Avez-vous durant l'année écoulée revu et mesuré l'efficacité de la politique de sécurité ? »

4. Une connaissance des incidents de sécurité ayant touché l'organisation



Q19: « Nombre des incidents de sécurité dans les 12 derniers mois. » réponses autres que « ne savent pas »

Seule une petite minorité des organisations met en œuvre ces quatre conditions



Le profil de ce nouveau type de leader

• Technologie	15%
• Industrie	13%
• Services financiers	10%
• Ingénierie/Construction	9%
• Télécommunications	8%
• Produits de consommation et distribution	8%
• Santé	4%
• Secteur public	4%
• Energie et services aux collectivités	4%
• Aérospatial et Défense	2%

Et en quoi ces leaders sont différents ?

	Leaders	Tous les répondants
Nombre d'incidents par an	1 274	2 562
Les dépenses sécurité vont augmenter l'année prochaine	76%	51%
Ont des personnes dédiées en charge de la sécurité dans les Directions Métiers	72%	46%
Sont confiants dans leur niveau de sécurité	93%	72%

Les leaders :

- Ont plus de moyens
- Connaissent moins d'incidents
- Sont plus connectés avec les métiers
- Au final, sont plus confiants dans leur sécurité

Conclusions : Quels enseignements pour votre fonction Sécurité ?

Les enjeux de la fonction Sécurité

- La fonction Sécurité doit être alignée sur les risques Métiers, mais elle doit en plus :

1. Apporter de la confiance aux dirigeants sur des sujets très évolutifs et difficilement palpables

2. S'assurer de couvrir le totalité du champ des possibles, dans un contexte très mouvant en termes de technologies, d'attentes des Métiers, de modes d'organisation et d'usages

3. Aider les organisations à tirer parti des opportunités existantes dans le cyberespace tout se protégeant des risques propres à ce monde

Les facteurs clefs de succès

1. Une sollicitation de la Direction Générale pour définir la vision et l'appétence aux risques

2. Au delà d'une politique statique, une stratégie qui décrit comment les menaces présentes et à venir sont traitées dynamiquement, tout en aidant les Métiers à se développer

3. Une implication des Métiers dans l'identification et le traitement des risques

4. Une boucle de contrôle permettant de vérifier que le dispositif de sécurité est efficace et efficient par rapport à la stratégie

5. Un reporting synthétique à la Direction Générale sur le niveau de maîtrise des risques

Contacts

Pour en savoir plus

Contacts :

Philippe Trouchaud
Associé
philippe.trouchaud@fr.pwc.com
+ 33 1 56 57 61 31

Vincent Maret
Directeur
vincent.maret@fr.pwc.com
+ 33 1 56 57 81 61

Notre site internet : www.pwc.fr/advisory