www.pwc.com/gsiss2014

Global State of Information Security Survey® 2014

Defending yesterday

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

12 décembre 2013

pwc

Agenda

Méthodologie de l'enquête

1

Global State of Information Security Survey ® 2014 en chiffres

16e étude mondiale menée entre le **1er février et le 1er avril 2013** par PwC en partenariat avec « CIO magazine » et « CSO magazine »

Plus de **9 600** réponses de PDG, Directeurs Financiers, DSI, RSSI et responsables IT et sécurité, répartis dans **115** pays

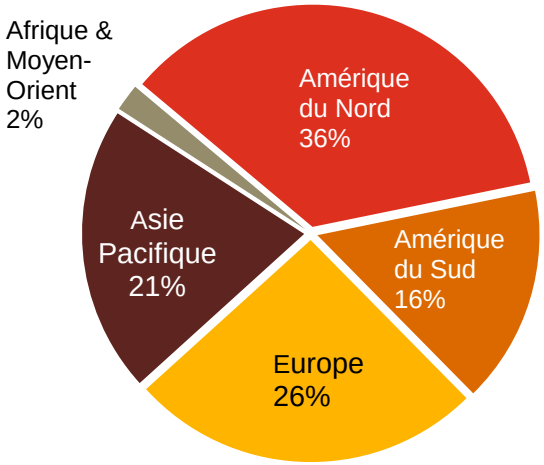
Plus de **40** questions relatives à la sécurité de l'information

391 réponses pour la France

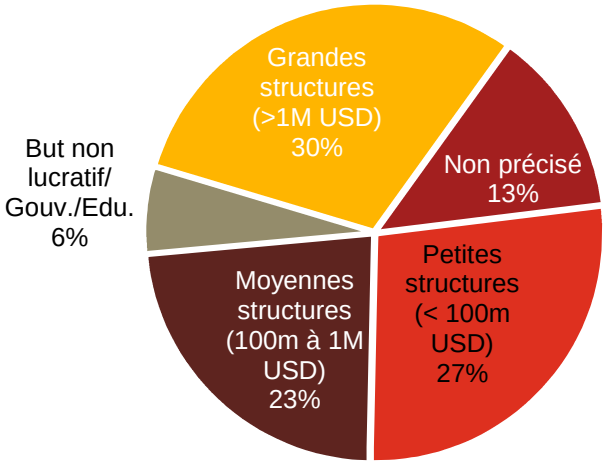
Démographie de l'échantillon

30% des répondants travaillent pour de grandes organisations (plus 1 milliard de dollars de chiffre d'affaires), soit une croissance de 22% par rapport à l'an dernier.

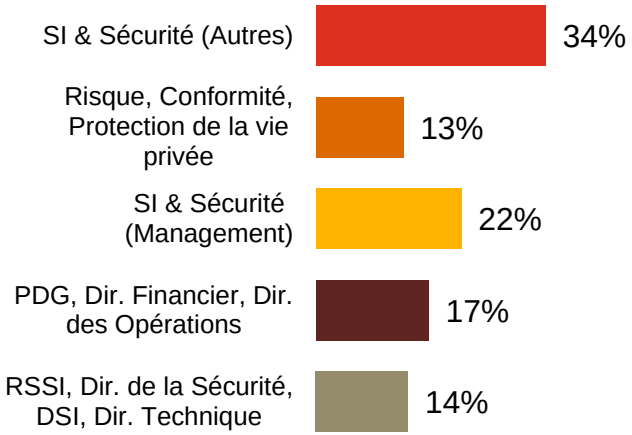
Réponses par zones géographiques



Réponses par chiffre d'affaires des entreprises



Réponses par fonctions



(Les chiffres sont donnés aux erreurs d'arrondi près)

Niveau de réponse par industrie

Nombres de réponses cette année	Monde	France
Technologie	1226	40
Services financiers	993	25
Produits industriels	880	29
Produits de consommation et distribution	820	33
Services publics	694	45
Santé et pharmaceutique	672	16
Télécommunications	456	18
Energie, Utilities, Mining	338	13
Divertissement et média	221	11
Aérospatial et défense	193	14
Autres	3188	147

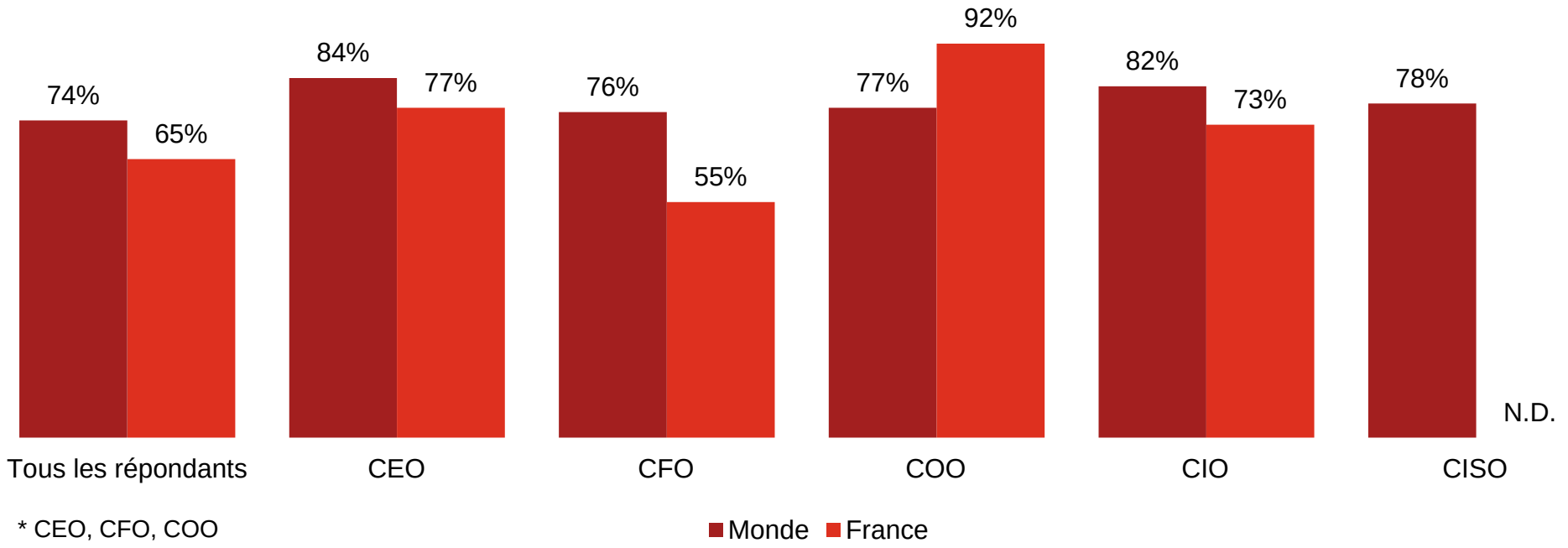
Les entreprises restent confiantes face à des risques toujours plus présents

2

Les entreprises restent confiantes : 74% des répondants croient que leurs activités de sécurité sont efficaces. Les dirigeants sont encore plus optimistes.

Au sein des postes de direction*, 84% des CEO disent avoir confiance en leur programme de sécurité. Notons que les CFO sont les membres de la direction les moins confiants.

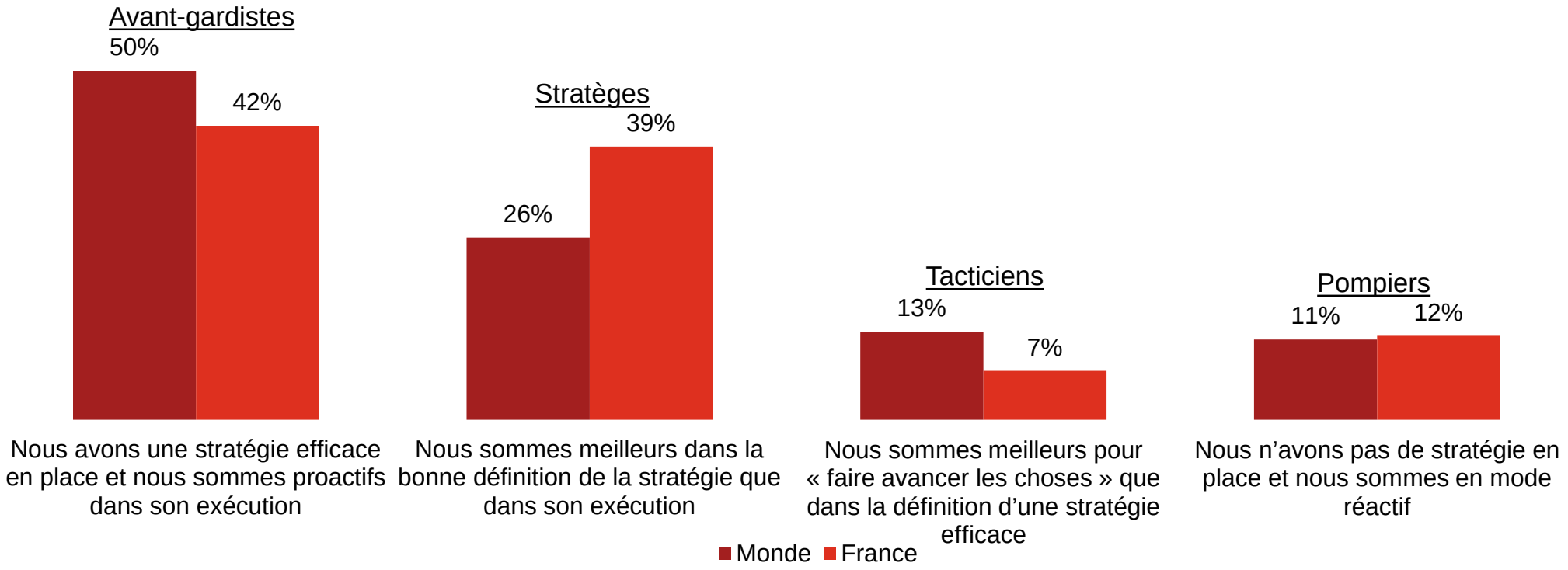
Confiance des dirigeants dans l'efficacité de leurs activités de sécurité (plutôt ou très confiants)



Question 39 : "Quelle confiance avez-vous dans l'efficacité des activités de sécurité de l'information de votre organisation ?" (Répondants ayant répondu "Plutôt confiants" ou "Très confiants") Question 1 : "Quel poste occupez-vous ?"

La moitié des répondants se considèrent comme "avant-gardistes" en termes de stratégie et de pratiques de sécurité.

50% disent avoir mis en place une stratégie efficace et se disent proactifs dans son implémentation, soit une croissance de 17% par rapport à l'an dernier. Environ un quart (26%) se pensent meilleurs en terme de stratégie qu'en terme d'exécution.



Question 27 : "Quelle proposition caractérise le mieux l'approche de votre organisation concernant la sécurité de l'information ?"

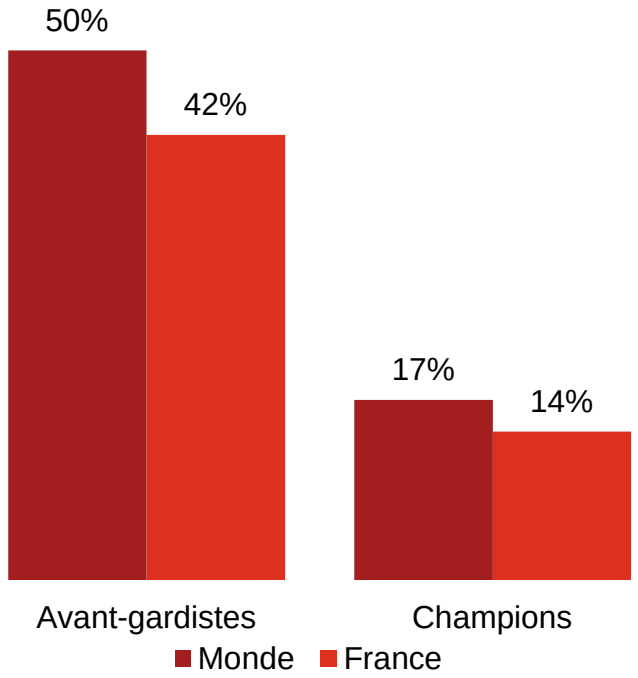
Mais une analyse plus poussée montre que les véritables champions sont bien moins nombreux que les avant-gardistes.

Nous avons analysé les déclarations des répondants selon quatre critères clefs qui, selon nous, caractérisent les champions en termes de sécurité de l'information.

Pour être un champion, une entreprise doit :

- Avoir une stratégie globale de sécurité de l'information,
- Employer un CISO ou équivalent qui rend des comptes directement au CEO, CFO, COO, CRO ou à un conseiller juridique
- Avoir mesuré et revu l'efficacité de sa sécurité sur l'année passée,
- Comprendre exactement quel type d'événements de sécurité sont survenus sur l'année écoulée.

Notre analyse montre qu'il y a encore sensiblement moins de champions que d'avant-gardistes auto-proclamés.

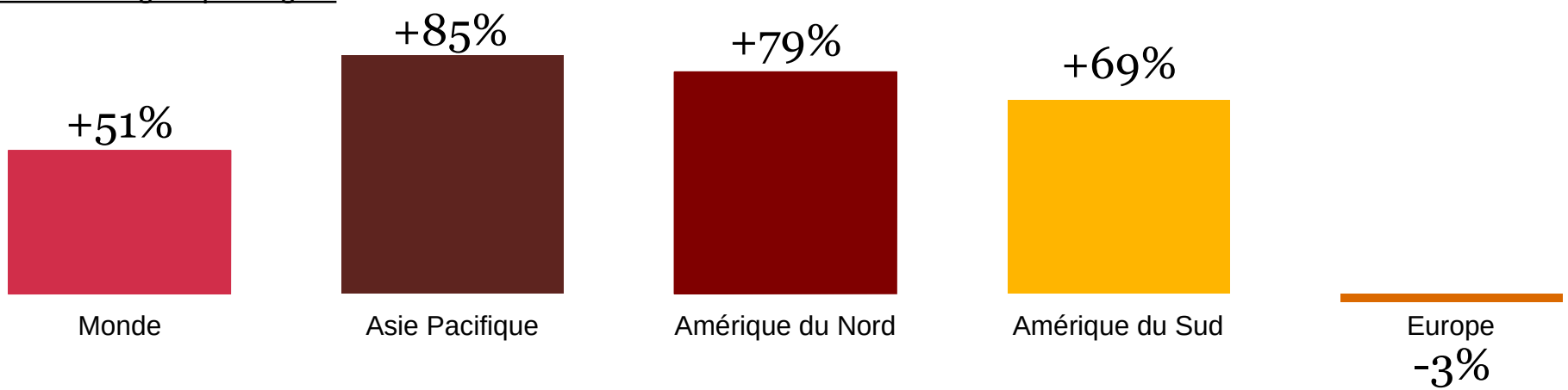


Les champions sont identifiés par les réponses aux questions 13A : "Où / à qui votre RSSI, Directeur de la Sécurité, ou responsable équivalent de la direction rend-il des comptes ?", 14 : "Quelles mesures de sécurité de l'information liées aux processus sont actuellement en place dans votre organisation ?", 19 : "Quels types d'incidents de sécurité sont survenus ?", 31 : "Au cours de l'an passé, votre entreprise a-t-elle mesuré et revu l'efficacité de sa politique et de ses procédures de sécurité de l'information ?"

Les budgets de sécurité de l'information connaissent une hausse significative, sauf en Europe.

Le budget moyen consacré à la sécurité de l'information cette année est en hausse de 51% par rapport à 2012. Les organisations ont compris que le niveau de menace aujourd'hui élevé appelait une augmentation substantielle des investissements.

Evolution des budgets par région



Répondants anticipant une hausse des budgets sur les 12 prochains mois

Question 8 : "Quel est le budget total consacré à la sécurité de l'information dans votre organisation pour l'année 2013 ?"

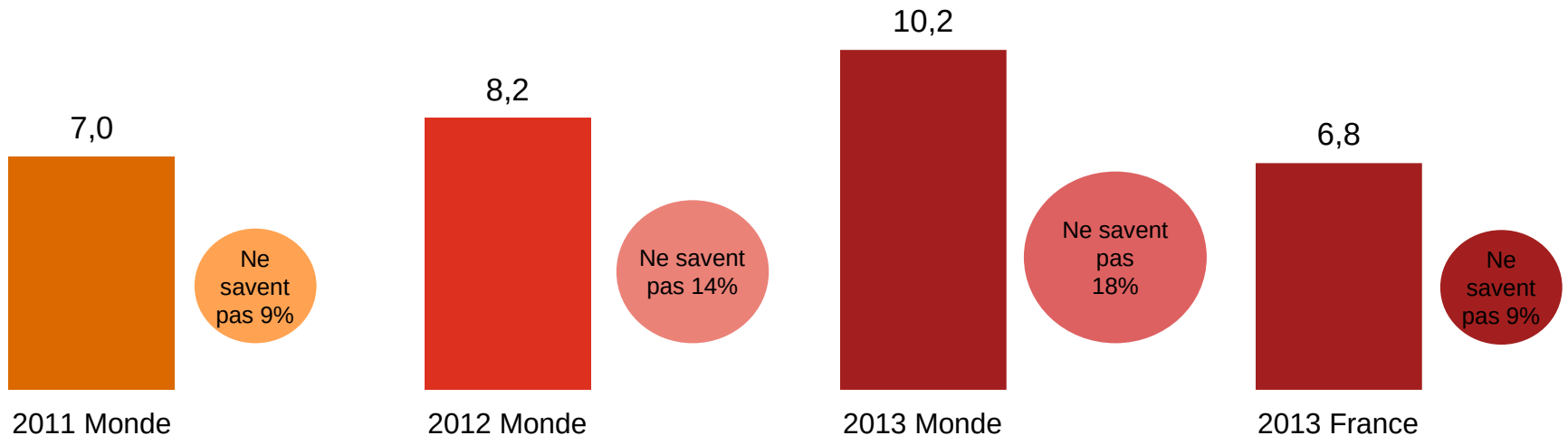
Incidents d'aujourd'hui et stratégies d'hier

3

Les répondants détectent plus d'incidents de sécurité.

Le nombre d'incident détectés au cours des 12 derniers mois a augmenté de 25% par rapport à l'an dernier, ce qui peut être révélateur du niveau de menace élevé de l'environnement actuel. Il est troublant de constater que les répondants qui ignorent le nombre d'incidents qu'ils ont subi a quant à lui doublé. Cela pourrait être dû au maintien d'investissements dans des produits de sécurité basés sur des modèles obsolètes.

Nombre d'incidents moyen par jour sur les 12 derniers mois

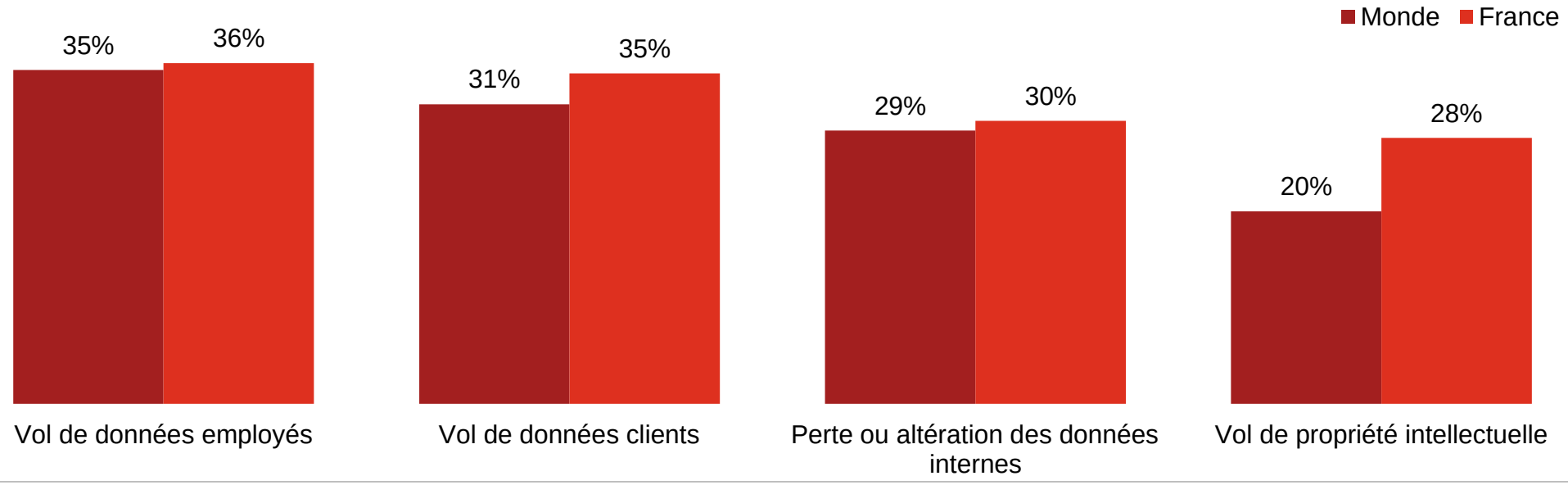


Question 18 : "Quel a été le nombre d'incidents de sécurité détectés au cours des 12 derniers mois ?"

Les données des employés et des clients restent des cibles privilégiées.

La compromission des données des employés et des clients restent les conséquences d'incidents qui reviennent le plus souvent, mettant potentiellement en danger les relations les plus précieuses des organisations. Par ailleurs, la perte ou l'altération de données internes ont bondi de plus de 100% sur l'année écoulée.

Impact des incidents de sécurité

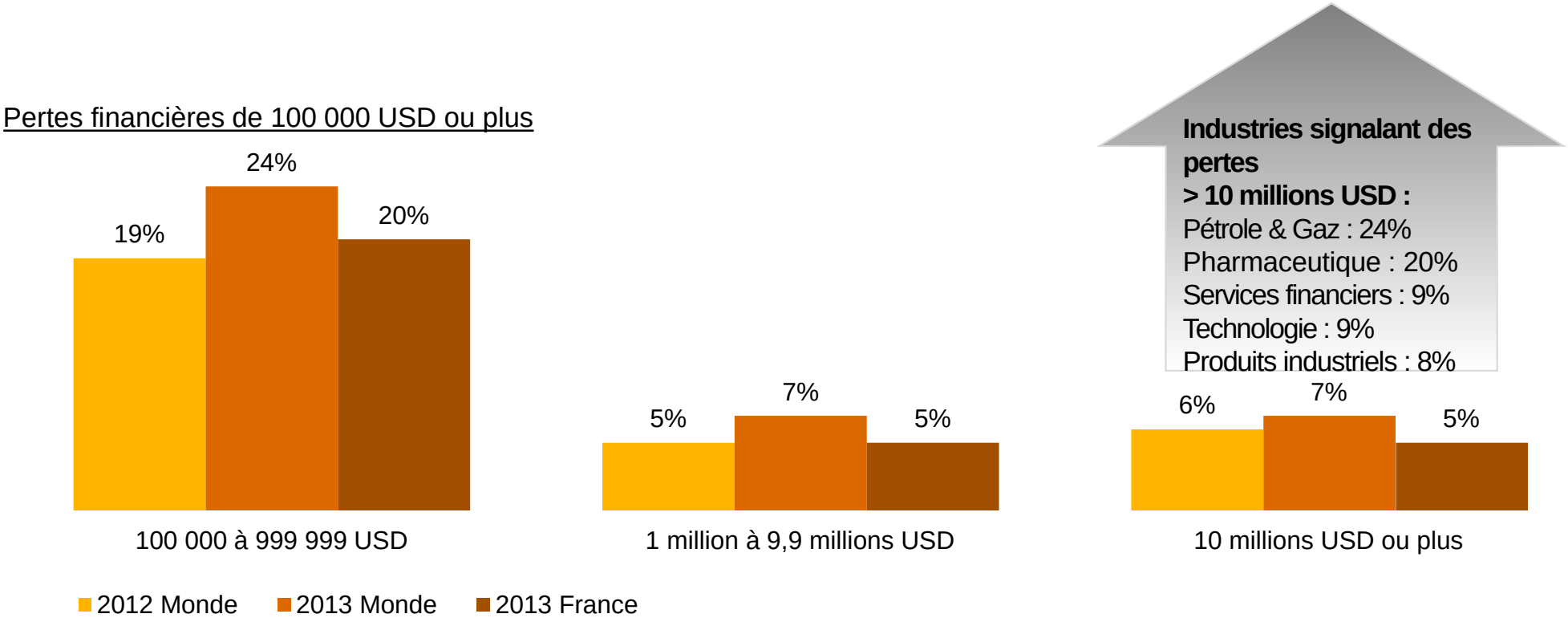


Question 22 : "Comment votre organisation a-t-elle été impactée par les incidents de sécurité ?" (Seule une partie des facteurs sont présentés ici.)

Le coût financier des incidents est en hausse.

Les pertes moyennes ont crû de 18% en un an.

Les pertes importantes augmentent plus vite que les pertes mineures : +51% depuis 2011 pour les pertes de plus de 10 millions USD.

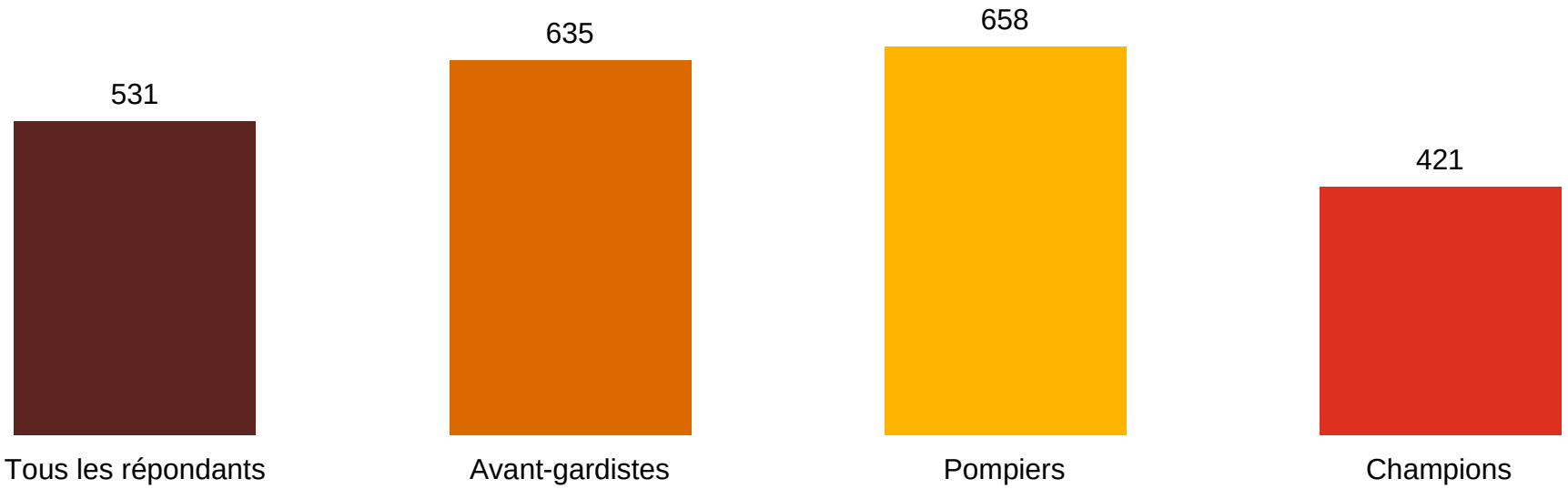


Question 22A : “Estimation du total des pertes financières résultant d’incidents de sécurité”

Les organisations qui se déclarent avant-gardistes relèvent un coût par incident de sécurité plus élevé que la moyenne. Les champions présentent, eux, le plus bas.

Les avant-gardistes dépensent quasiment autant par incident que les pompier, que l'on considère les moins bien préparés à mettre en place un programme de sécurité efficace.

Coût moyen par incident (en USD)

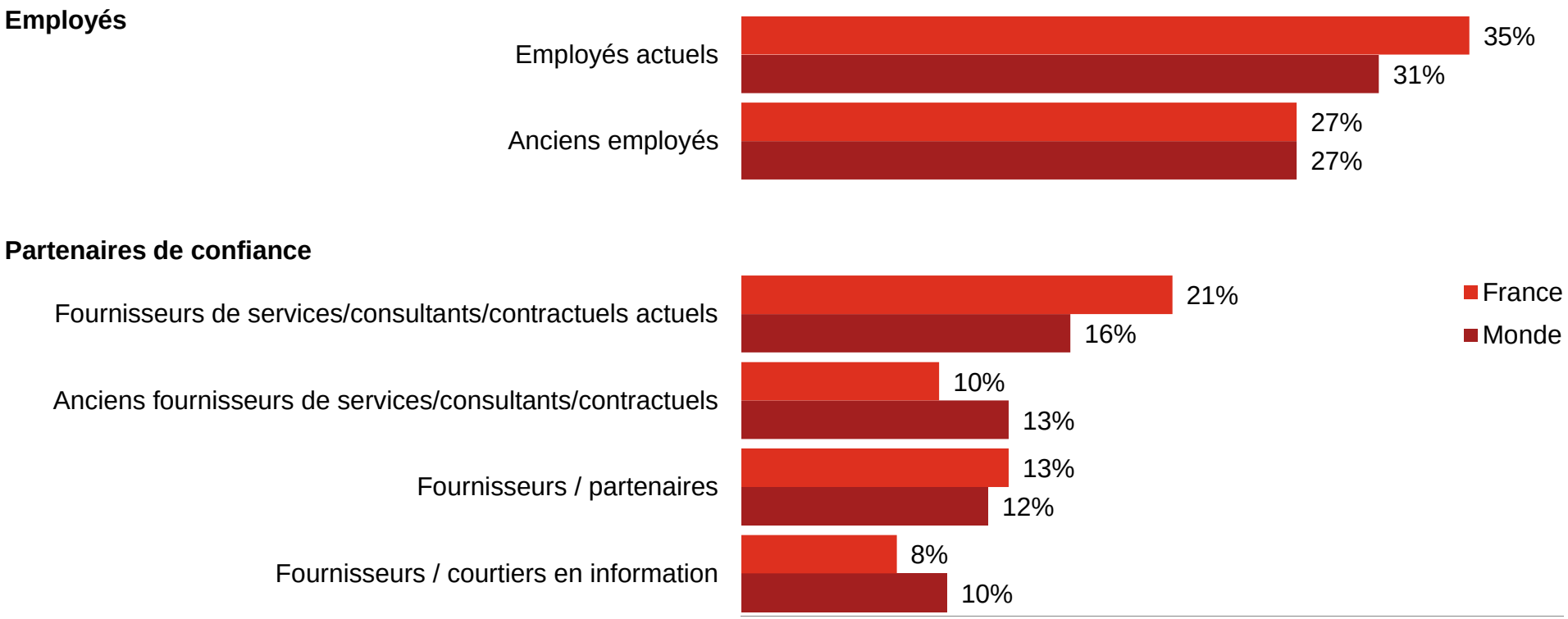


Question 18 : "Quel a été le nombre d'incidents de sécurité détectés au cours des 12 derniers mois ?" Question 22A : "Estimation du total des pertes financières résultant d'incidents de sécurité"

La plupart des répondants citent des sources internes comme causes des incidents de sécurité, en particulier les collaborateurs actuels ou anciens.

Les menaces les plus réelles se situent dans votre entourage : ce sont vos employés, actuels ou anciens, et tous ceux qui interagissent avec le cœur de l'organisation.

Estimation de la source probable des incidents

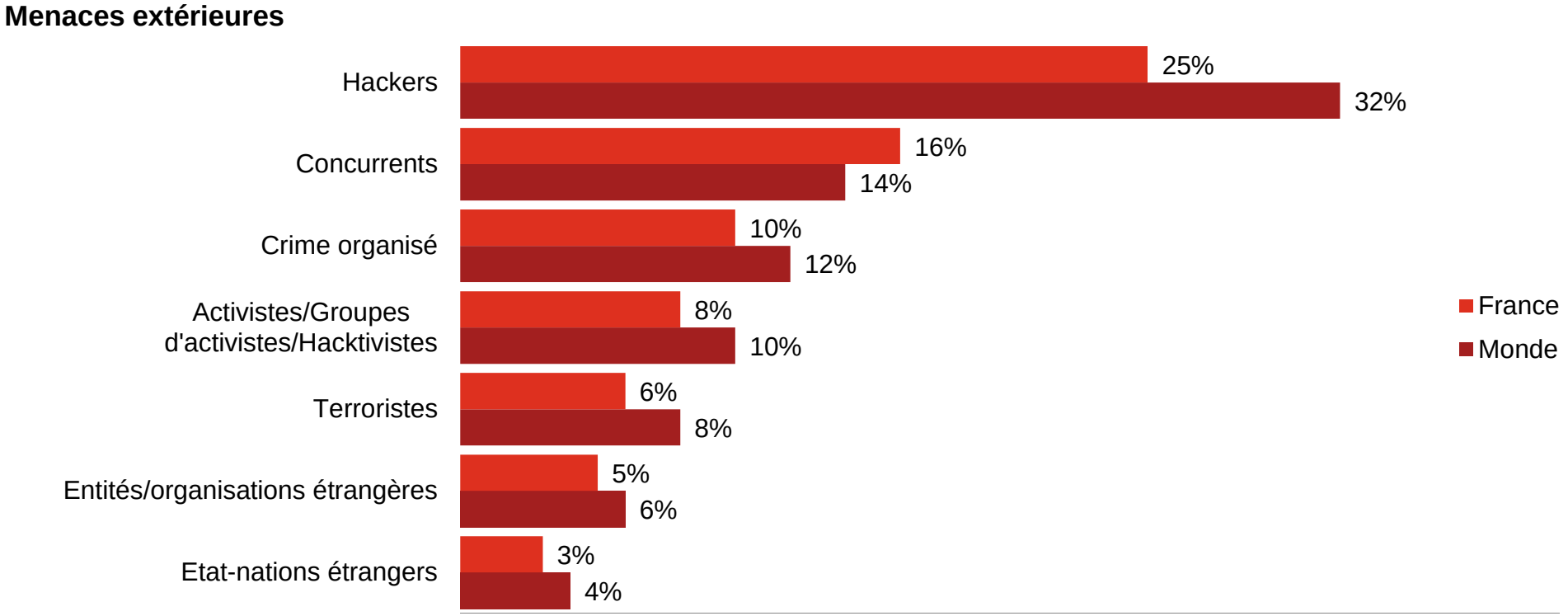


Question 21 : "Estimation de la source probable des incidents" (Seule une partie des facteurs sont présentés ici.)

Bien que les attaques soutenues par des Etat-nations fassent la une, il est plus vraisemblable que votre organisation soit touchée par d'autres menaces.

Seuls 4% des répondants disent avoir été victimes d'attaques perpétrées par des Etat-nations. Il reste beaucoup plus vraisemblable d'être victime de hackers.

Estimation de la source probable des incidents



Question 21 : "Estimation de la source probable des incidents" (Seule une partie des facteurs sont présentés ici.)

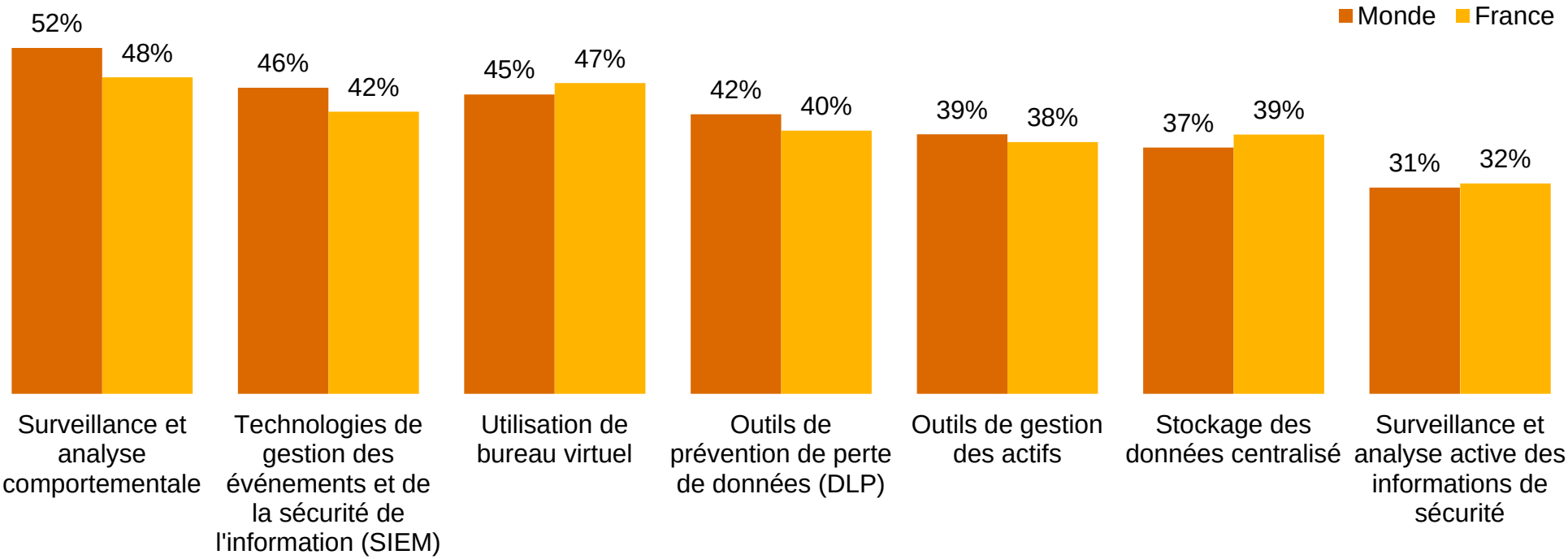
Une défense qui laisse à désirer

4

Beaucoup d'entreprises n'ont pas implémenté les technologies et processus permettant de se faire une idée claire des risques d'aujourd'hui.

Les mesures de sécurité qui pourraient permettre de surveiller les données et les actifs de l'organisation sont la plupart du temps absents. Ces outils renseigneraient pourtant l'organisation sur les vulnérabilités de l'écosystème et les menaces du moment.

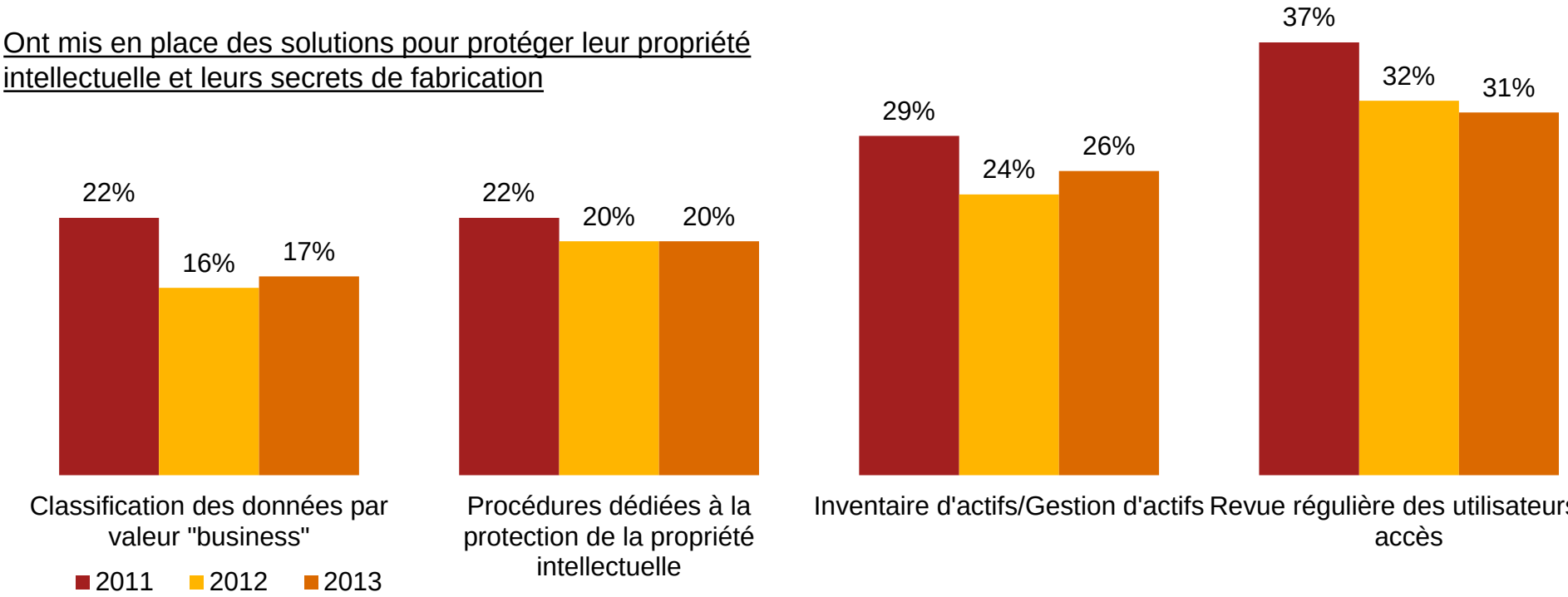
Répondants indiquant que les mesures suivantes NE SONT PAS en place actuellement



Question 14 : "Quelles mesures de sécurité de l'information liées aux processus sont actuellement en place dans votre organisation ?" Question 15 : "Quelles mesures technologiques de sécurité de l'information sont actuellement en place dans votre organisation ?" (Seule une partie des facteurs sont présentés ici.)

Malgré les conséquences potentielles, de nombreux répondants ne protègent pas suffisamment leurs informations sensibles.

Les organisations se doivent d'identifier, de prioriser et de protéger leurs « pépites ». Cependant, beaucoup d'entre eux n'ont toujours pas implémenté les politiques de sécurité de base nécessaires à la protection de leur propriété intellectuelle.



Question 32 : "Des éléments suivants, lesquels sont inclus dans la politique de sécurité de votre organisation ?" (Seule une partie des facteurs sont présentés ici.)

La mobilité a déclenché un déluge de données métier, mais le déploiement d'une sécurité appropriée n'a pas suivi le rythme imposé par les usages.

Les smartphones, tablettes et le « Bring Your Own Device » ont augmenté les risques en termes de sécurité. Et pourtant, les efforts pour implémenter un programme de sécurité sur la mobilité ne montrent pas d'évolution significative depuis l'an dernier, et restent en retard par rapport à la prolifération des périphériques mobiles.

La France régresse sur la majorité des mesures de sécurité relatives à la mobilité.

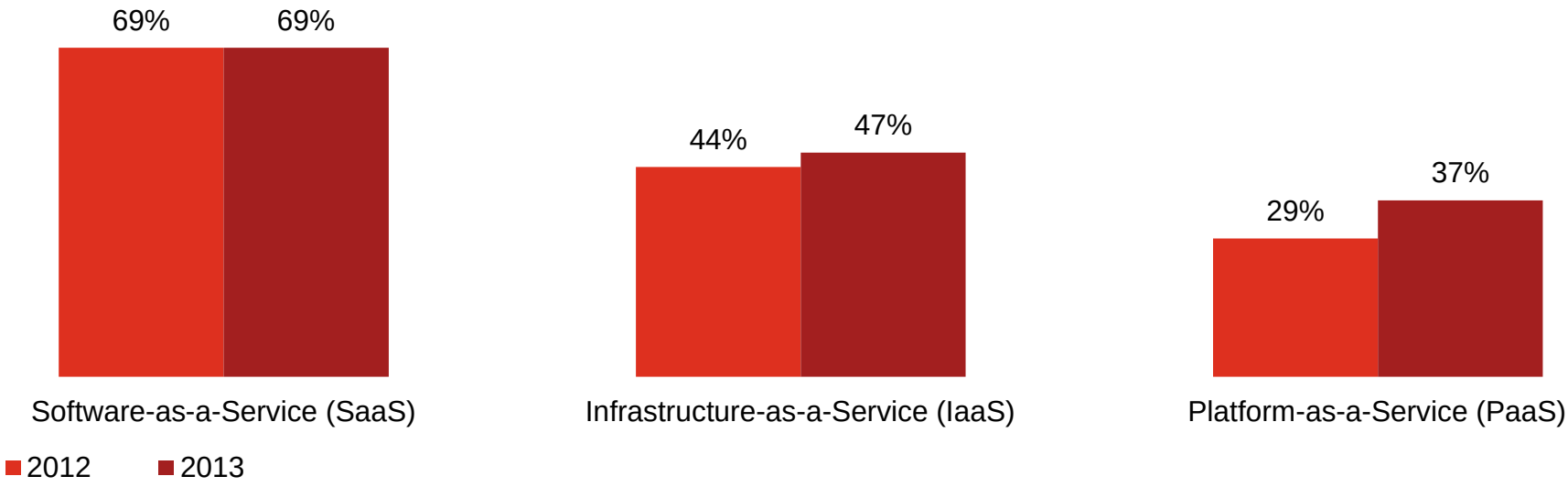
Initiatives prises en réponse aux risques liées aux technologies mobiles

Question 16 : "Quelles réponses votre organisation a-t-elle apporté aux risques de sécurité pour les technologies mobiles ?" (Seule une partie des facteurs sont présentés ici.)

Près de la moitié des répondants utilisent le cloud, mais l'incluent rarement dans leurs politiques de sécurité.

Alors que 47% des répondants utilisent le cloud — parmi lesquels 59% disent que leur sécurité s'est améliorée — seuls 18% ont intégré la question du cloud dans leur politique de sécurité. Le cloud est le plus souvent utilisé sous la forme SaaS, mais le PaaS se développe de manière importante.

Type de service cloud utilisé

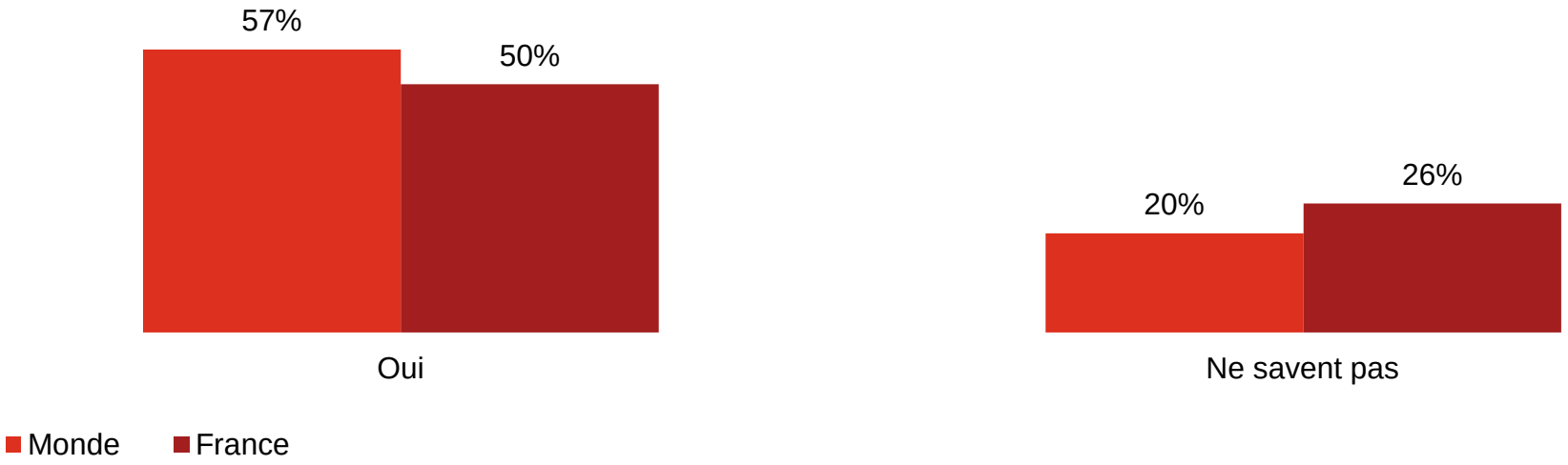


Question 32 : "Des éléments suivants, lesquels sont inclus dans la politique de sécurité de votre organisation ?" Question 42 : "Votre organisation utile-t-elle actuellement des services du cloud tels que : Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), ou Platform-as-a-Service (PaaS)?" Question 42A : "Quel type de service du cloud votre organisation utilise-t-elle ?" Question 42C : "Quel est l'impact du cloud sur la sécurité de l'information de votre entreprise ?" (Seule une partie des facteurs sont présentés ici.)

Dans un environnement mouvant, un nombre insuffisant de répondants ont mesuré et revu l'efficacité de leurs procédures et politiques de sécurité.

A peine plus de la moitié des répondants ont mesuré et revu l'efficacité de leurs procédures et politiques de sécurité dans les 12 derniers mois. 20% ne sont pas en mesure de dire si cette revue d'efficacité a été réalisée.

Revue annuelle des politiques et procédures de sécurité

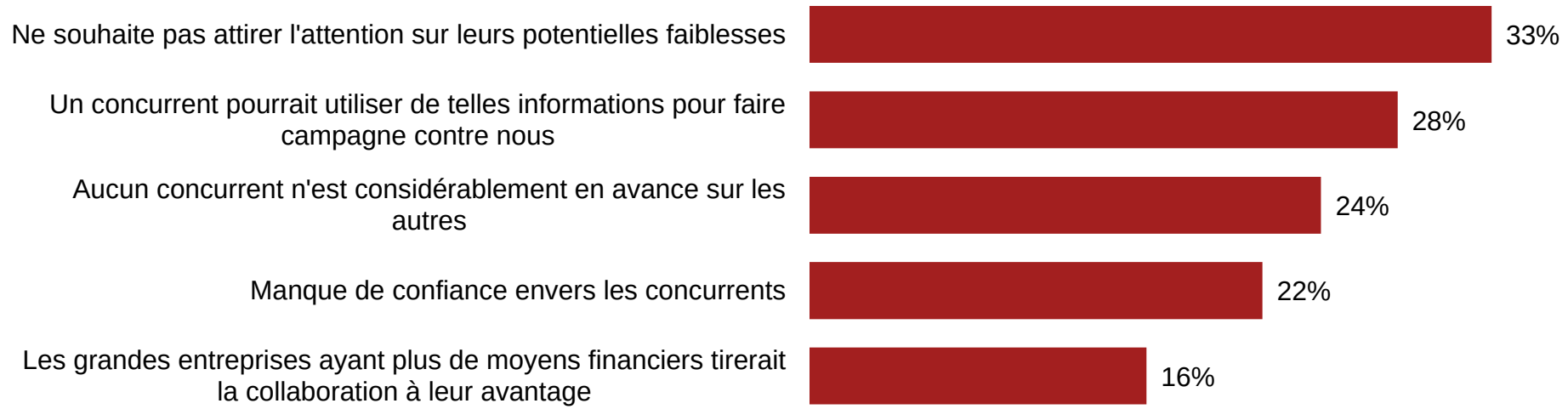


Question 31 : "Votre entreprise a-t-elle mesuré et revu l'efficacité de ses politiques et procédures de sécurité de l'information au cours de l'année écoulée ?"

28% des répondants ne collaborent pas avec d'autres entités pour améliorer leur sécurité, se privant ainsi d'un puissant outil offensif.

Et cela peut être un obstacle à la sécurité dans le monde interconnecté d'aujourd'hui. Avec la 5ème Enquête Annuelle du QI numérique[4], nous avons remarqué que les entreprises avec des équipes de directions collaboratives entremêlent stratégie métier et stratégie SI, et que cela permet souvent d'améliorer la performance et d'offrir une meilleure agilité face aux changements du marché.

Raisons invoquées pour justifier l'absence de collaboration sur la sécurité de l'information

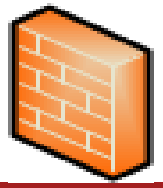


[4] PwC, *PwC's 5th Annual Digital IQ Survey*, 2013
Question 41 : "Votre organisation collabore-t-elle formellement avec d'autres acteurs de votre industrie, y compris des concurrents, pour améliorer la sécurité et réduire le potentiel des risques futurs ?" Question 41A : "Pourquoi votre organisation ne collabore-t-elle pas avec d'autres acteurs de votre industrie pour améliorer la sécurité et réduire le potentiel des risques futurs ?" (Seule une partie des facteurs sont présentés ici.)

Comment faire face aux menaces de demain ?

5

« Defending yesterday » : des protections statiques face à des menaces dynamiques.



Moyens statiques

Composants actuels

- Protection périmétrique
  - Pare-feu réseau
- Détection à base de signatures
  - Antivirus
  - Sondes de détection d'intrusion
  - Pare-feu applicatif
- Approche uniforme
  - Même niveau de confiance pour tous les utilisateurs
  - Faible isolation entre les différentes couches techniques

Décalage

Risques non couverts

Menaces dynamiques

Paysage actuel et futur

- APT : NY Times, NetTraveler

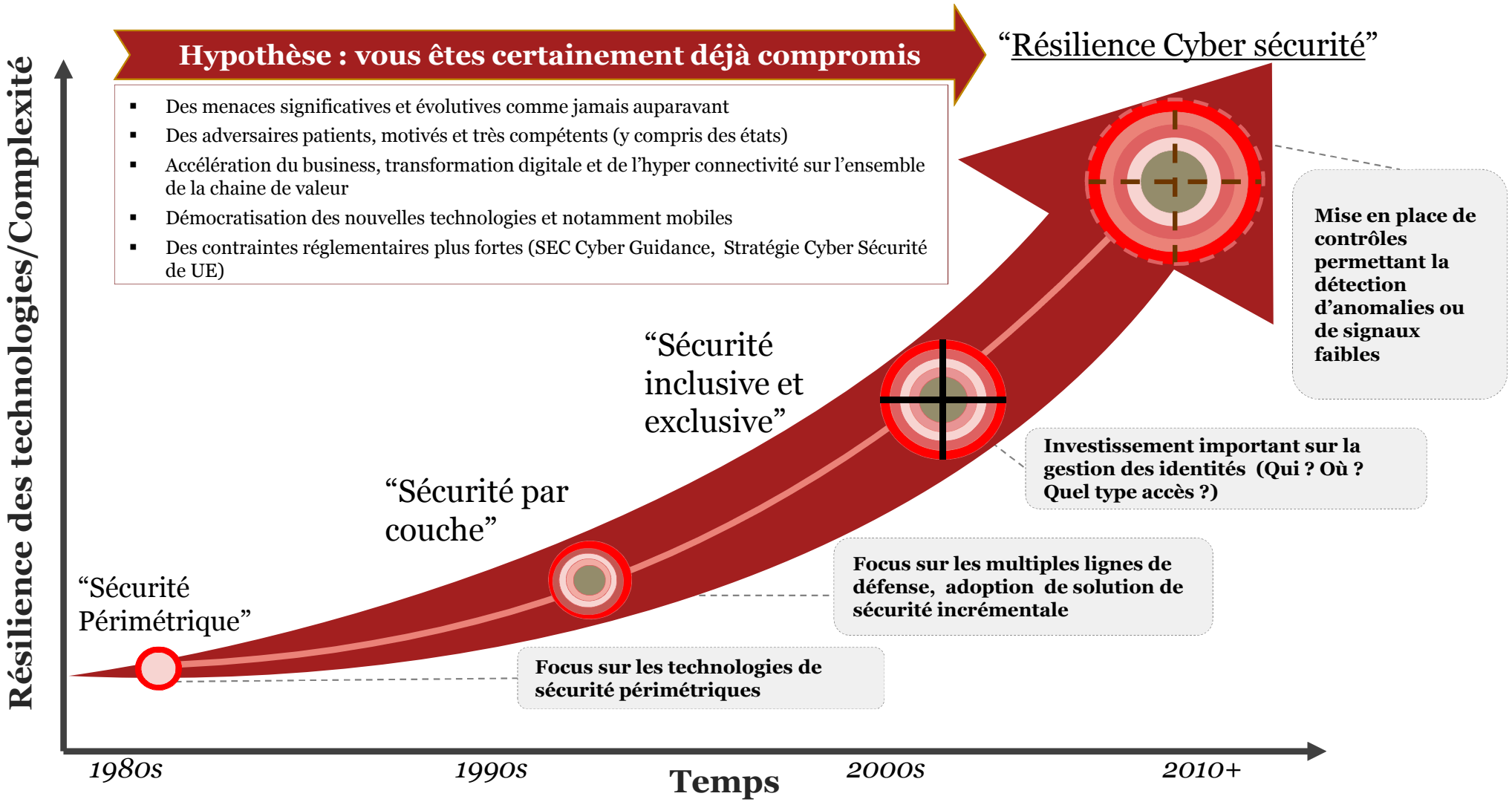
  Ciblent des utilisateurs de confiance, sont développés sur mesure pour échapper à la détection.
- Systèmes industriels : Aramco

  Démontrent le manque d'isolation entre les systèmes, en utilisant de nouveaux canaux.
- BYOD / COPE

  Les différents moyens d'accès nécessitent des considérations de sécurité propres.
- Cloud / SaaS
- Internet des objets (futur)

L'évolution vers une résilience cyber sécurité

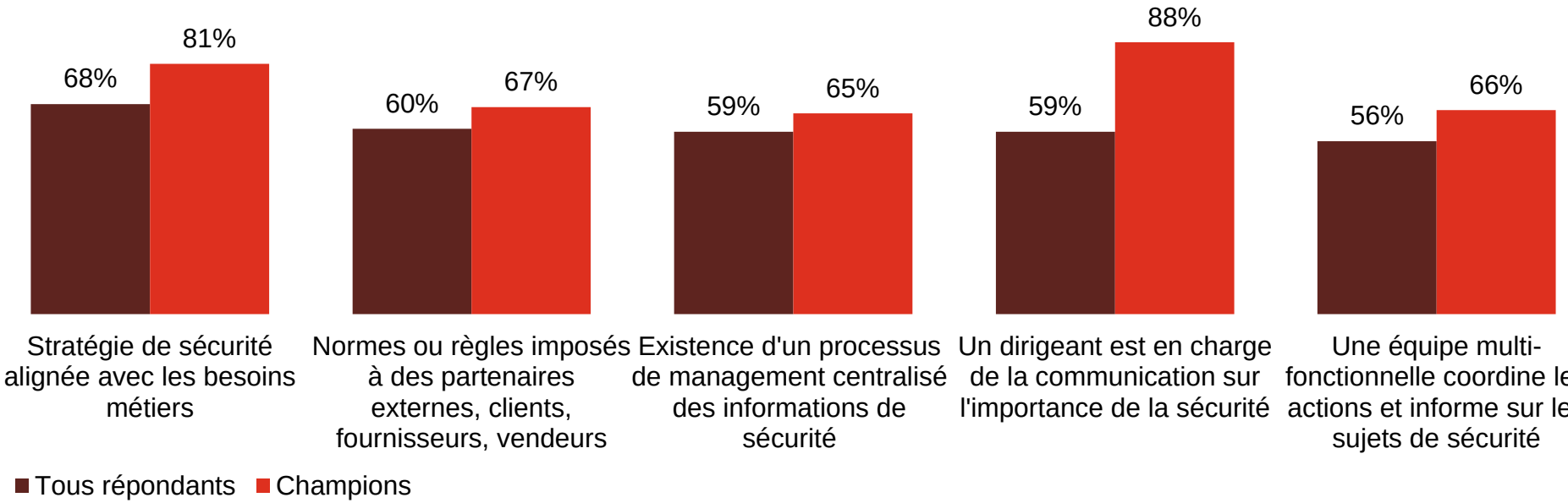
Transition du paradigme sécurité



Les champions montent en compétence et démontrent que la sécurité est maintenant un impératif métier, pas juste un défi uniquement IT.

Aligner sécurité et besoins métiers, normaliser les exigences imposées aux partenaires externes, améliorer sa communication… Voici autant de démarches qui montrent que les champions, plus que tout autre, repensent les bases de la sécurité. Les écarts constatés à l'échelle mondiale sont encore plus marqués en France.

Politiques de sécurité et mesures actuellement en vigueur : Tous répondants vs. Champions



Question 14 : "Quelles mesures de sécurité de l'information liées aux processus sont actuellement en place dans votre organisation ?" (Seule une partie des facteurs sont présentés ici.) Question 29 : "Y a-t-il, dans votre organisation, un dirigeant (PDG, Directeur financier, Directeur des opérations, etc.) qui communique de façon proactive sur l'importance de la sécurité de l'information à l'intérieur de l'organisation ?"

De nombreuses organisations ont investi dans des mesures technologiques pour protéger leur écosystème contre les menaces d'aujourd'hui.

Les Champions sont ceux qui implémentent le plus ces technologies. Mais étant donné le paysage des menaces actuelles, *toutes* les organisation devraient sérieusement penser à implémenter ces mesures.

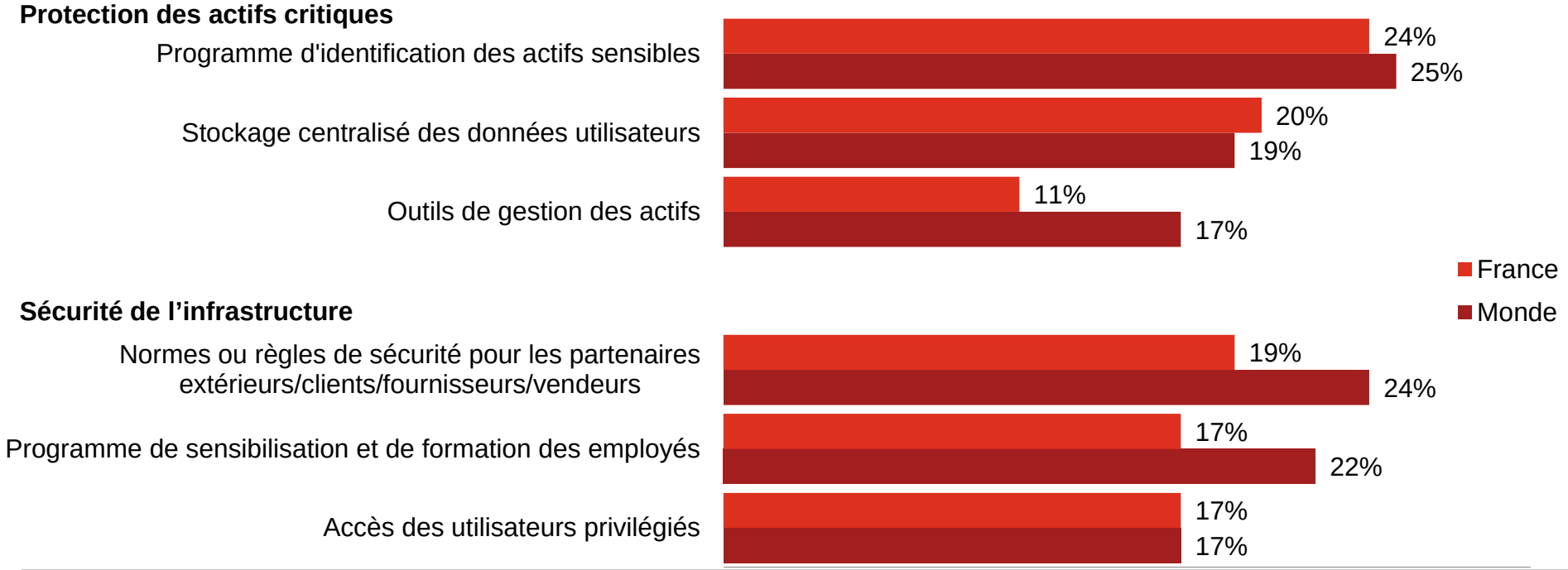
Mesures technologiques actuellement en place	Tous répondants	Champions Monde	Champions France
Outils de détection de code malveillant	74%	88%	79%
Outils de recherche de vulnérabilités	62%	71%	58%
Outils de prévention de perte de données (*Data Loss Prevention*)	58%	67%	79%
Détection de maliciels sur périphériques mobiles	57%	67%	66%
Outils de corrélation d'événements de sécurité	57%	66%	68%
Interface bureau virtualisé	55%	65%	68%
Outils d'analyse de code	54%	64%	77%
Solution de gestion de la détection et protection contre les APT	54%	66%	81%
Technologies de gestion des événements et informations de sécurité	54%	66%	76%

Question 15 : "Quelles mesures technologiques de sécurité de l'information sont actuellement en place dans votre organisation ?" (Seule une partie des facteurs sont présentés ici.)

Dans quels impératifs métiers et processus les répondants vont-ils investir ?

Quelques-unes des principales priorités incluent les technologies pouvant aider l'organisation à protéger ses actifs les plus précieux et à développer des avantages stratégiques.

Mesures n'étant pas actuellement en place mais qui constituent une priorité pour les 12 prochains mois

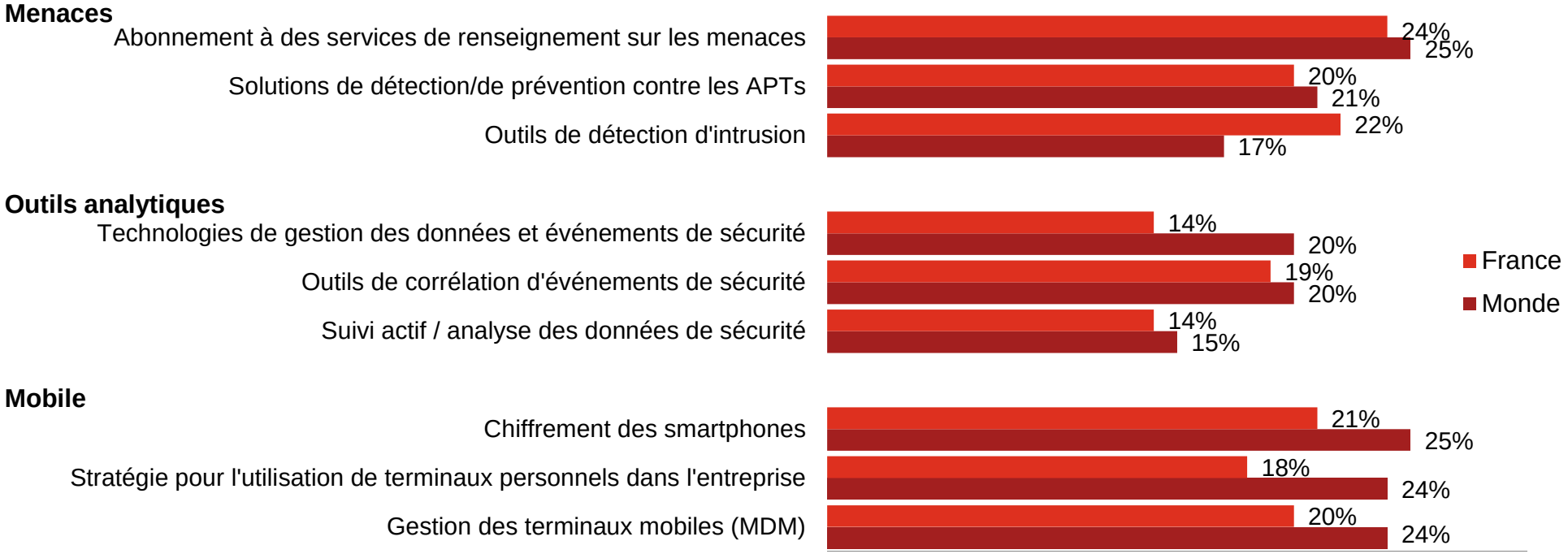


Question 14 : "Quels processus de préservation de la sécurité de l'information ne sont actuellement pas en place mais constituent une priorité pour l'année à venir ?" Question 15 : "Quelles technologies de préservation de la sécurité de l'information ne sont actuellement pas en place mais constituent une priorité pour l'année à venir ?" (Seule une partie des facteurs sont présentés ici.)

Les autres priorités sont la détection et la réponse aux menaces.

La connaissance est une force. Les organisations interrogées l'ont compris et s'orientent en priorité vers des technologies qui peuvent les aider à mieux comprendre les menaces tout en améliorant la sécurité liée aux terminaux mobiles.

Mesures n'étant pas en place actuellement mais constituant une priorité pour les 12 prochains mois

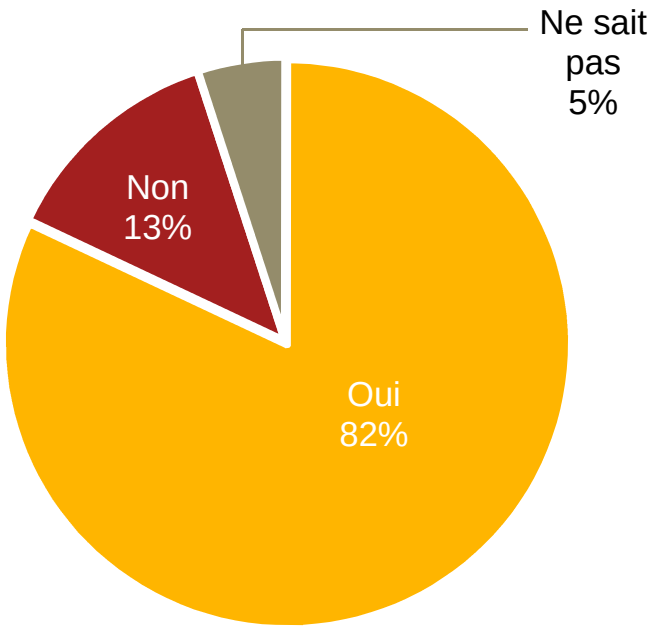


Question 14 : "Quels processus de préservation de la sécurité de l'information ne sont actuellement pas en place mais constituent une priorité pour l'année à venir ?" Question 15 : "Quelles technologies de préservation de la sécurité de l'information ne sont actuellement pas en place mais constituent une priorité pour l'année à venir ?" (Seule une partie des facteurs sont présentés ici.)

Les champions internationaux voient les bénéfices que peuvent leur apporter collaboration et partage d'information.

Beaucoup de champions se rendent compte que des collaborations entre la sphère publique et la sphère privée peuvent être un moyen efficace d'obtenir des renseignements sur des menaces qui ne cessent de changer.

Collaborent formellement avec d'autres acteurs de leur industrie sur les sujets de sécurité de l'information (Champions seuls)



82% des **champions** collaborent

Question 41 : "Votre organisation collabore-t-elle formellement avec d'autres acteurs de votre industrie, y compris des concurrents, pour améliorer la sécurité et réduire le potentiel des risques futurs ?"

L'alignement de la sécurité de l'information avec la stratégie et les objectifs métiers est nécessaire pour une sécurité efficace.

Par rapport à l'an dernier, davantage de répondants disent que leurs dépenses en sécurité et leurs politiques sont tout à fait en phase avec leurs objectifs métiers. En d'autre termes, les organisations commencent à comprendre que la sécurité fait partie intégrante de l'agenda métier et peut contribuer, en fin de compte, aux résultats financiers de l'entreprise.

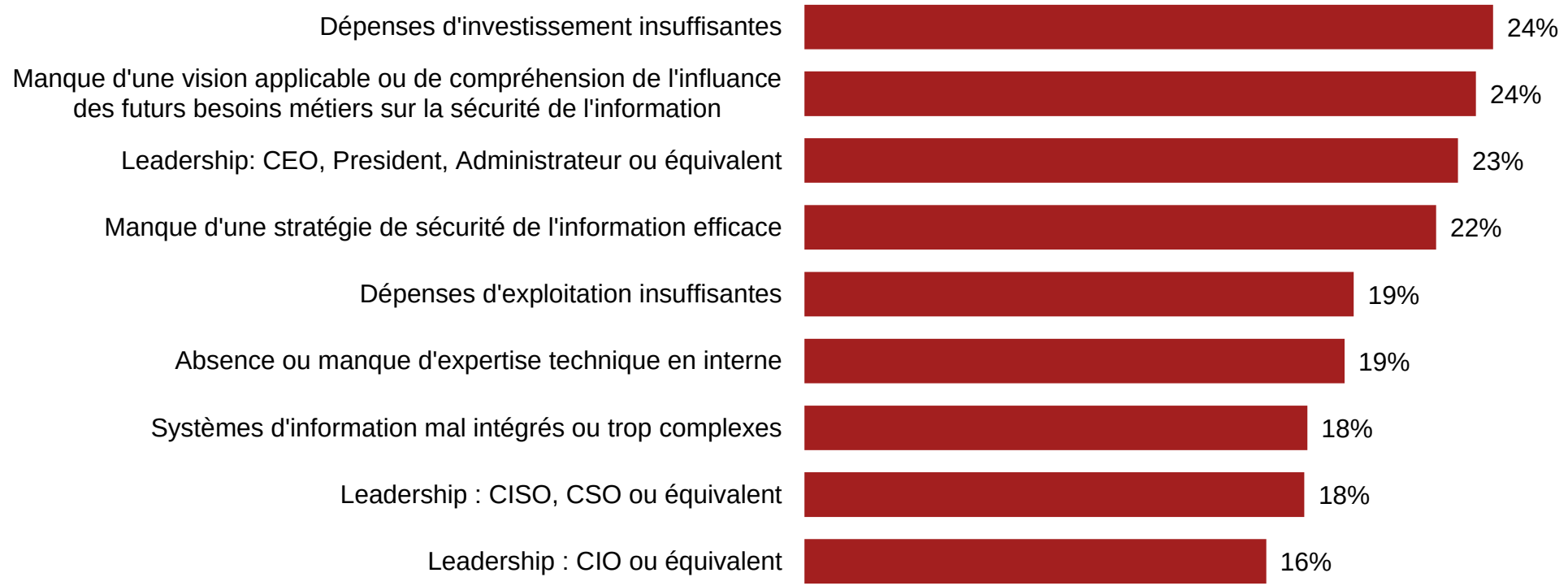
Niveau d'alignement avec les objectifs métiers (plutôt ou très aligné)

Question 33 : "D'après vous, à quel point les politiques de sécurité de votre entreprise sont-elles alignées avec les objectifs métiers ?" Question 34 : "D'après vous, à quel point les dépenses de sécurité de votre entreprise sont-elles alignées avec les objectifs métiers ?"

Il faudra plus de moyens financiers et un leadership engagé pour dépasser les obstacles et aboutir à un meilleur niveau de sécurité.

Ces facteurs sont capitaux parce qu'une approche adaptée de la sécurité nécessite le soutien des dirigeants et un budget adéquat, aligné avec les besoins métiers.

Obstacles les plus importants à l'amélioration de l'efficacité stratégique de la fonction SSI



Question 28 : "Quels sont les plus grands obstacles à l'amélioration de l'efficacité stratégique générale de la fonction sécurité de l'information de votre organisation ?"

La course mondiale à la cyberdéfense

6

L'Amérique du Sud est sur le point de prendre la tête en ce qui concerne les investissements, mesures en place et politiques de sécurité de l'information.

L'Asie Pacifique reste très forte en termes de budgets consacrés à la sécurité et pratiques de pointes, tandis que l'Europe et l'Amérique du Nord sont en retard sur plusieurs points.

	Amérique du Sud	Asie Pacifique	Europe	Amérique du Nord
Vont augmenter leurs dépenses en sécurité au cours des 12 prochains mois	66%	60%	46%	38%
Ont une stratégie générale de sécurité	75%	79%	77%	81%
Emploient un RSSI	75%	74%	68%	65%
Ont un dirigeant qui communique l'importance de la sécurité	68%	69%	51%	55%
Ont mesuré / revu l'efficacité des politiques de sécurité et procédures au cours de l'année passée	70%	69%	53%	49%
Ont une politique de sauvegarde et un plan de continuité/de reprise d'activité	58%	55%	45%	47%
Exigent des tierce-parties qu'elles se conforment aux politiques de protection de la vie privée	55%	58%	55%	62%
Ont un programme de sensibilisation et de formation des employés à la sécurité de l'information	54%	63%	55%	64%
Ont des procédures dédiées à la protection de la propriété intellectuelle	20%	24%	17%	21%
Ont déployé des technologies de détection d'intrusion	64%	67%	63%	67%
Inventorient les endroits où les données personnelles sont collectées, transmises et stockées	53%	60%	52%	64%
Collaborent avec d'autres acteurs pour améliorer la sécurité et réduire les risques	66%	59%	45%	42%

(Seule une partie des facteurs sont présentés ici.)

L'avantage est à la Chine pour l'implémentation de mesures technologiques protégeant contre les menaces dynamiques d'aujourd'hui.

La Russie fait aussi montre de progrès solides dans le déploiement de systèmes de surveillance des données et des actifs, alors que les Etats-Unis restent devant le Brésil et que l'Inde tente de rattraper son retard.

	Chine	Russie	E-U	Brésil	France	Inde
Stockage centralisé des données utilisateurs	73%	68%	65%	64%	61%	61%
Profiling et surveillance comportementale	60%	48%	44%	57%	54%	48%
Chiffrement des smartphones	61%	51%	57%	52%	49%	53%
Outils de détection d'intrusion	65%	76%	67%	64%	63%	68%
Outils de recherche de vulnérabilités	72%	60%	63%	63%	57%	58%
Outils de gestion des actifs	71%	60%	64%	59%	63%	62%
Utilisation de bureaux virtuels	64%	61%	56%	55%	55%	52%
Solution de gestion de la détection et la protection contre les APTs	62%	56%	56%	54%	57%	48%
Technologies de gestion des événements et données de sécurité (SIEM)	66%	59%	57%	54%	59%	48%

Question 15 : "Quelles mesures technologiques de sécurité de l'information sont actuellement en place dans votre organisation ?" (Seule une partie des facteurs sont présentés ici.)

La rencontre du cloud computing, de la mobilité, des équipements personnels et des médias sociaux constitue un défi commun à tous les pays.

Aucun pays n'a entièrement répondu à l'impact potentiel de ces quatre questions interdépendantes, mais la Chine et les Etats-Unis donnent le rythme pour l'implémentation d'une stratégie de sécurité.

	Chine	E-U	France	Russie	Brésil	Inde
Stratégie de sécurité pour le Cloud	51%	52%	49%	45%	49%	47%
Stratégie de sécurité pour les équipements mobiles	64%	57%	57%	51%	49%	50%
Stratégie de sécurité pour les médias sociaux	59%	58%	56%	47%	51%	50%
Stratégie de sécurité pour l'emploi d'équipements personnels en entreprise	71%	64%	59%	56%	53%	54%

Question 14 : "Quelles mesures de sécurité de l'information liées aux processus sont actuellement en place dans votre organisation ?" (Seule une partie des facteurs sont présentés ici.)

Le futur de la sécurité : de la prise de conscience à la concrétisation, « Awareness to Action »

7

Les mesures fondamentales à mettre en place pour un programme de sécurité efficace.

Une sécurité efficace requiert l'implémentation de nombreuses mesures aux niveaux technique, organisationnel et humain. À l'aide d'une analyse par régression sur les résultats du sondage et de l'expérience de PwC des pratiques mondiales en sécurité, nous avons identifié les 10 clefs suivantes.

Mesures essentielles pour une sécurité de l'information efficace	
1	Une politique écrite de sécurité de l'information
2	Des plans de sauvegarde, de reprise et de continuité d'activité
3	Une collecte et une rétention minimales d'informations personnelles, combinée à des restrictions d'accès physique aux systèmes conservant les données personnelles
4	Des mesures technologiques fortes de prévention et détection des attaques, et de chiffrement
5	Un inventaire précis des lieux et systèmes où les données personnelles des employés et clients sont collectées, transmises et stockées, incluant les tierces parties amenées à manipuler ces données
6	Une évaluation interne et externe des risques couvrant les aspects : respect de la vie privée, sécurité, confidentialité et intégrité des enregistrements électroniques ou papier
7	Un suivi continu des politiques de confidentialité des données et du respect de la vie privée
8	Des vérifications d'antécédents sur le personnel
9	Un programme de sensibilisation et de formation des employés à la sécurité de l'information
10	L'exigence que les employés et tiers se conforment aux politiques de respect de la vie privée

Aller plus loin : une nouvelle approche de la sécurité pour un monde nouveau.

Les mesures de sécurité traditionnelles restent limitées. Une nouvelle approche est nécessaire pour faire face au niveau de risque élevé du paysage. Une approche axée sur la connaissance des menaces, des actifs et des adversaires. Nous appelons ce modèle « *Awareness to Action* ».

La sécurité est un impératif métier

- Il faut comprendre l'exposition et l'impact métier potentiel associés au contexte d'un écosystème mondial et interconnecté.
- Une stratégie de sécurité intégrée doit être un élément clef de votre business model. La sécurité n'est plus uniquement un défi SI.

Les menaces sont aussi des risques métier

- Les directeurs généraux, membres du conseil d'administration, et autres dirigeants doivent comprendre que les risques de sécurité sont des menaces pour l'organisation.
- Vous devez anticiper ces menaces, connaître vos vulnérabilités et être capable d'identifier et de contrôler les risques correspondants.
- Assurez-vous que vos fournisseurs, partenaires, et autres tiers connaissent et suivent vos pratiques de sécurité.

Aller plus loin : une nouvelle approche de la sécurité pour un monde nouveau (suite).

Protégez l'information qui compte vraiment

- Comprenez et adaptez-vous aux changements de l'environnement des menaces en identifiant vos informations les plus précieuses.
- Sachez où sont vos « pépites » et qui y a accès.
- Allouez et priorisez vos ressources pour protéger les informations qui ont de la valeur.

Prenez l'avantage grâce à *Awareness to Action*

- Toutes les activités et tous les investissements devraient être conduits en fonction de la meilleure connaissance à disposition sur les actifs informationnels, les écosystèmes de menaces et de vulnérabilités et la surveillance des activités métiers.
- Créez une culture de la sécurité qui commence avec l'engagement de vos dirigeants et descend en cascade vers tous les employés.
- Engagez-vous dans des collaborations public-privé avec d'autres acteurs du marché pour obtenir un maximum d'informations sur les menaces.

Notes

Notes

Des questions ?

Philippe Trouchaud
philippe.trouchaud@fr.pwc.com
Tél. : +33 (0) 1 56 57 82 48

Fabrice Garnier de Labareyre
fabrice.garnier.de.labareyre@fr.pwc.com
Tél. : +33 (0) 1 56 57 58 18

Visitez www.pwc.com/gsiss2014