www.pwc.com

Vers une nouvelle approche de la cybersécurité et de la protection des données personnelles

A l'ère du digital, les entreprises mettent en place des mesures innovantes pour gérer les menaces et gagner en compétitivité

CIO
BUSINESS TECHNOLOGY LEADERSHIP
CSO
BUSINESS RISK LEADERSHIP

Résultats de l'enquête : The Global State of Information Security® Survey 2017

pwc

Agenda

1. Méthodologie de l'enquête
2. Introduction : Des risques de cybersécurité désormais bien identifiés mais dont les impacts potentiels encore peu connus
3. Implication grandissante des comités exécutifs
4. Collaboration à tous les niveaux
5. Cloud, Externalisation des services de sécurité, Big Data : l'innovation au service de la Cybersécurité
6. La protection de données personnelles un enjeu de sécurité poussé par la réglementation
7. Evolution, causes et impact des incidents
8. Conclusion : La confiance au cœur des enjeux numériques

Méthodologie de l'enquête

1

Méthodologie

The **Global State of Information Security®** Survey 2017 est une étude mondiale réalisée par PwC, *CIO* et *CSO magazine*, en ligne entre le 4 Avril et le 3 Juin 2016 :

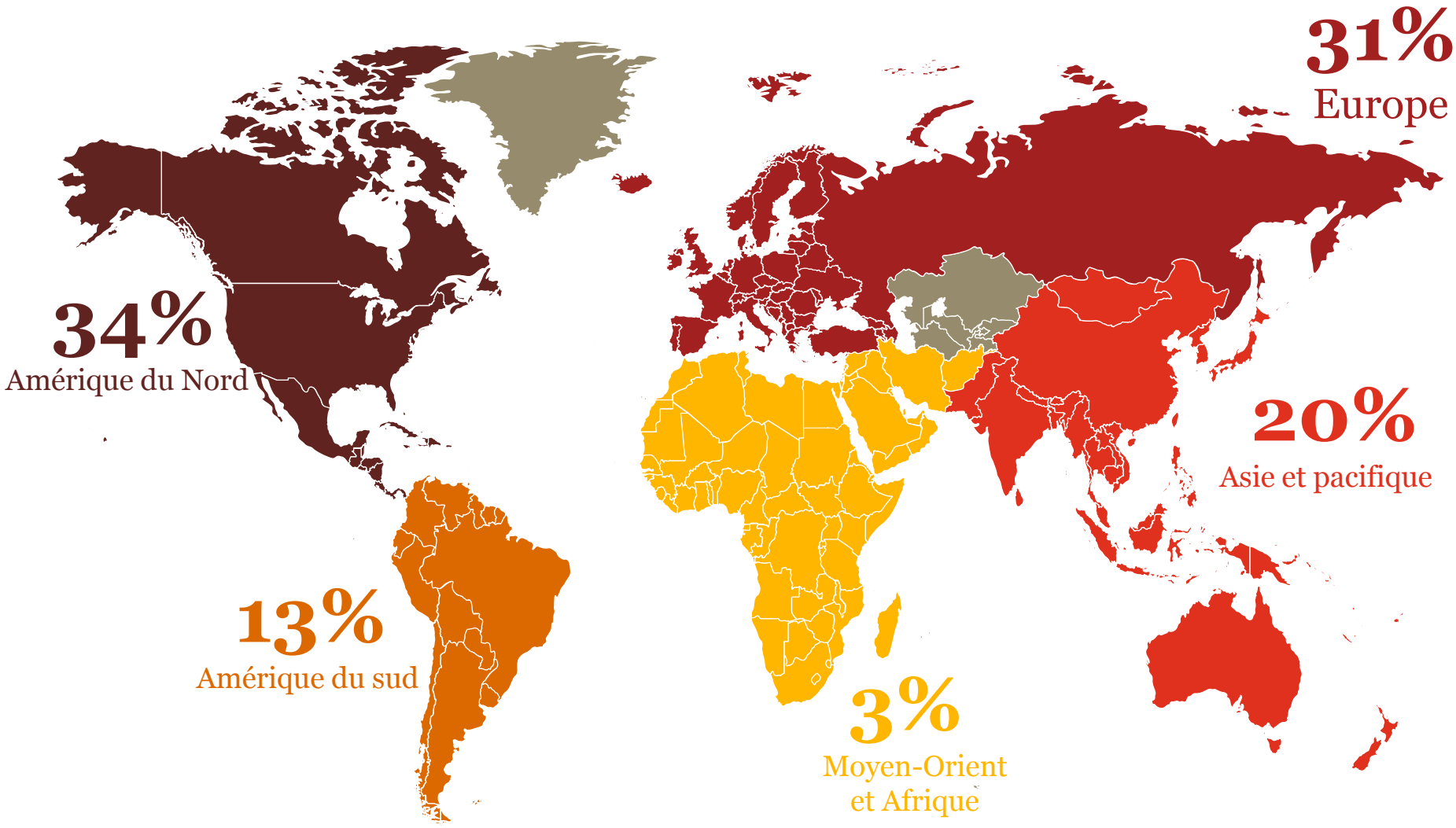
- Menée depuis **19** ans par PwC et depuis **14** ans en partenariat avec *CIO et CSO magazine*

- Des réponses apportées par les **lecteurs** et les **clients** de PwC, répartis dans **133** pays

- Un sondage contenant plus de **40** questions relatives à la **confidentialité**, à la **sécurité** de l'information et à l'implémentation par les entreprises de nouveaux **dispositifs de protection**

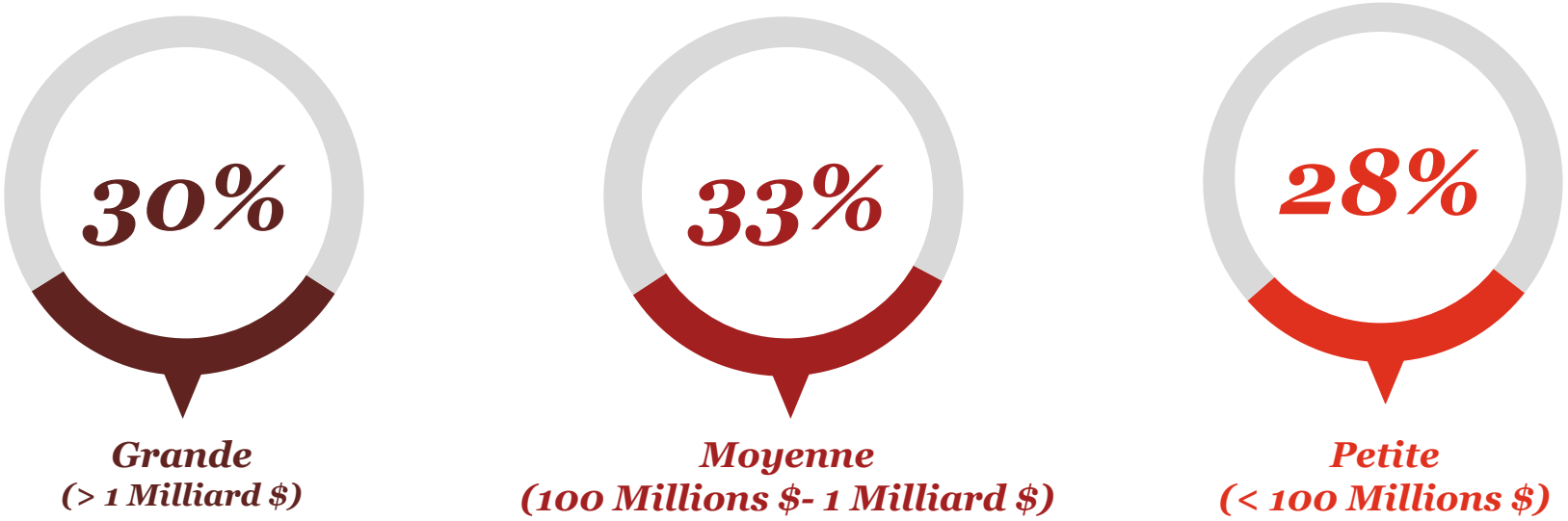
- Une marge d'erreur inférieure à **1%**

Plus de 10.000 personnes sondées dans 133 pays



Un échantillon constitués de dirigeants d'entreprise et responsables Cybersécurité…

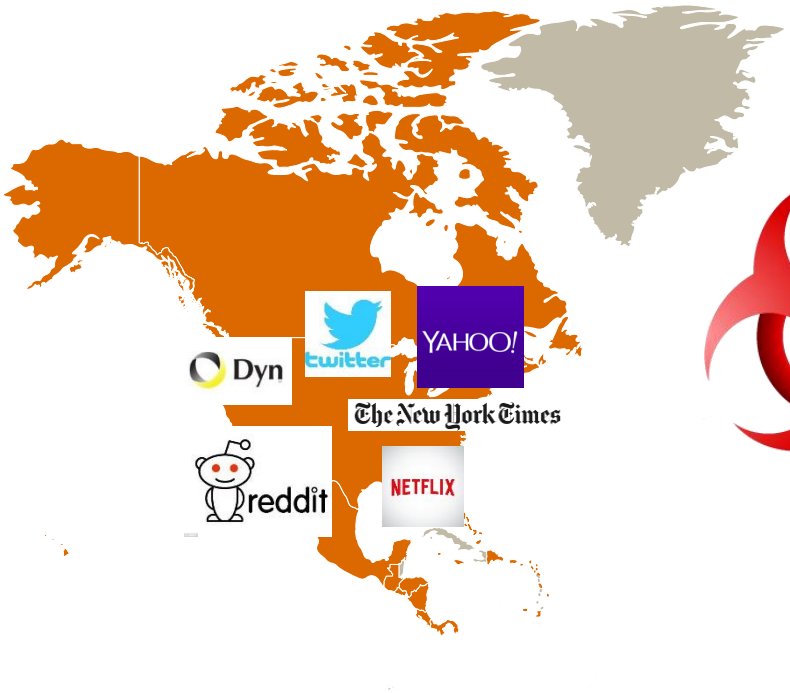
… et d'un large éventail d'entreprises



Introduction : Des risques de cybersécurité désormais bien identifiés mais dont les impacts potentiels encore peu connus

2

Les risques sont clairement identifiés, cependant les impacts qu'elles induisent restent difficilement estimables



Le Vendredi 21 octobre, la société Dyn qui gère les noms de domaine des géants de l'internet est victime d'une cyberattaque massive.

Nature de l'attaque

- Attaque par Déni de service l'interconnexion de plusieurs appareils infectés par un virus, ont été utilisés par les pirates pour rendre indisponible les serveurs des sites visités.

Impact

- Ralentissement voir indisponibilité des sites pendant plusieurs heures

La médiatisation a poussé les directions générales à prendre davantage conscience des problématiques de cybersécurité, avec comme conséquence, une implication plus forte de leur part, une plus grande pression sur les responsables informatiques et une augmentation du budget alloué à la cybersécurité.

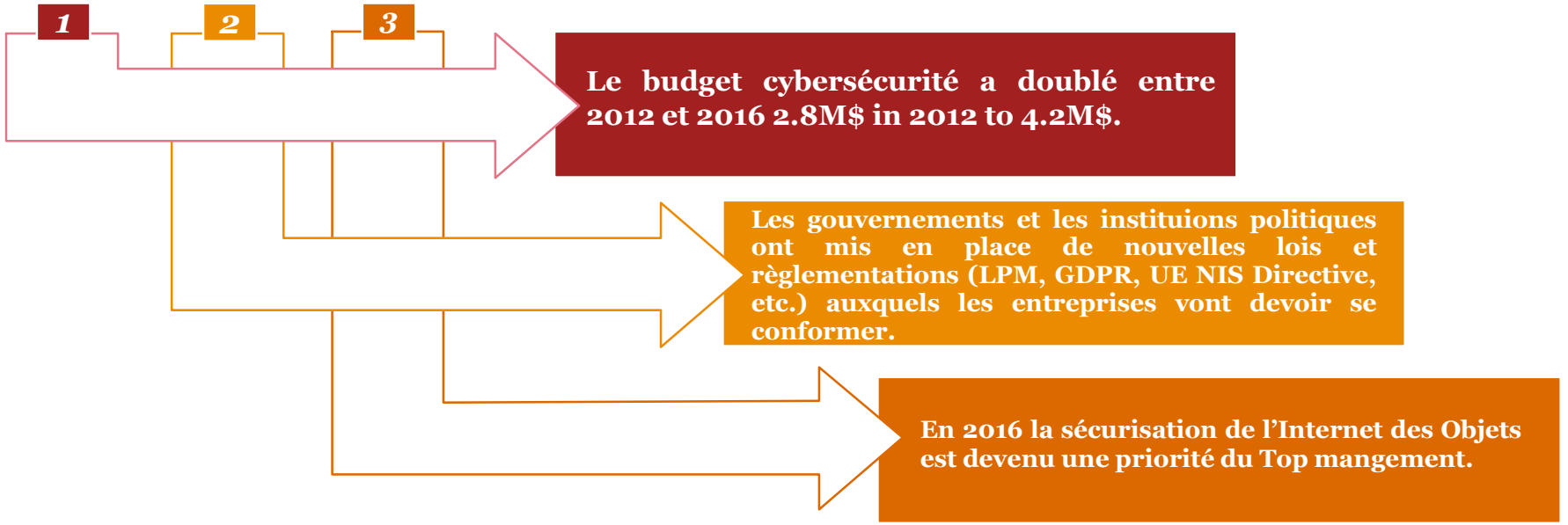
Se protéger sans arrêter d'innover

La révolution digitale est en marche et elle a totalement changé la donne!

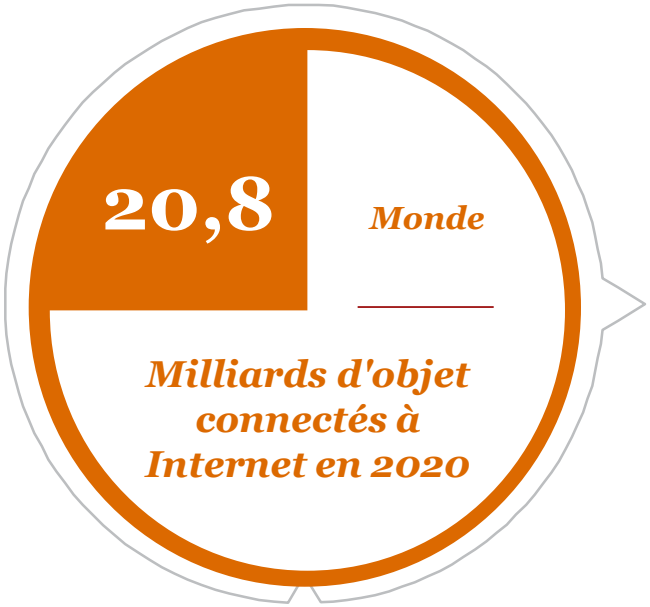
L'expansion de l'Internet et la digitalisation croissante des organisations impliquent une exposition significative à des impacts économiques, légales et touchant à l'image de marque de l'organisation.

PwC's 20th CEO Survey

Notre dernier étude "*CEO Survey*" reconnait que la digitalisation est devenue une priorité du top management



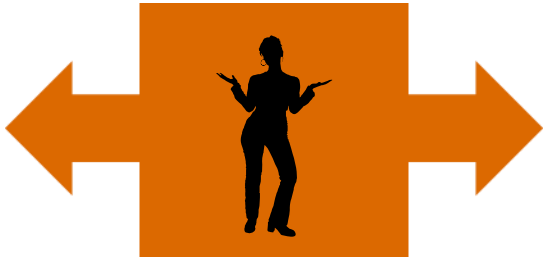
A ton suffisamment conscience des impacts d'une cyberattaque d' envergure ?



Source: Gartner
(http://www.gartner.com/newsroom/id/3165317)

Qu'arriverait-il si un attaquant mettait en place une attaque similaire pour paralyser une partie du web, l'accès à Internet d'un pays ?

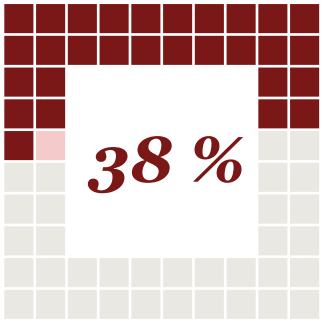
Quelles seraient les impacts d'une telle attaques sur les entreprises ? Sur les états ?



Quels moyens mettre en œuvre pour se protéger contre ce type d'attaques ?

Face à l'ampleur des cyberattaques, le partage…

Citation de Barack Obama: "*There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.*"



Seulement des répondants affirment faire de la collaboration un pilier de leur programme de cybersécurité

ISAO

IOCTA

Pour anticiper, faire face à des attaques massives, les états, les entreprises et les populations doivent partager, collaborer, innover ensemble et être proactif.

Approche planifiée, humaine et collectives

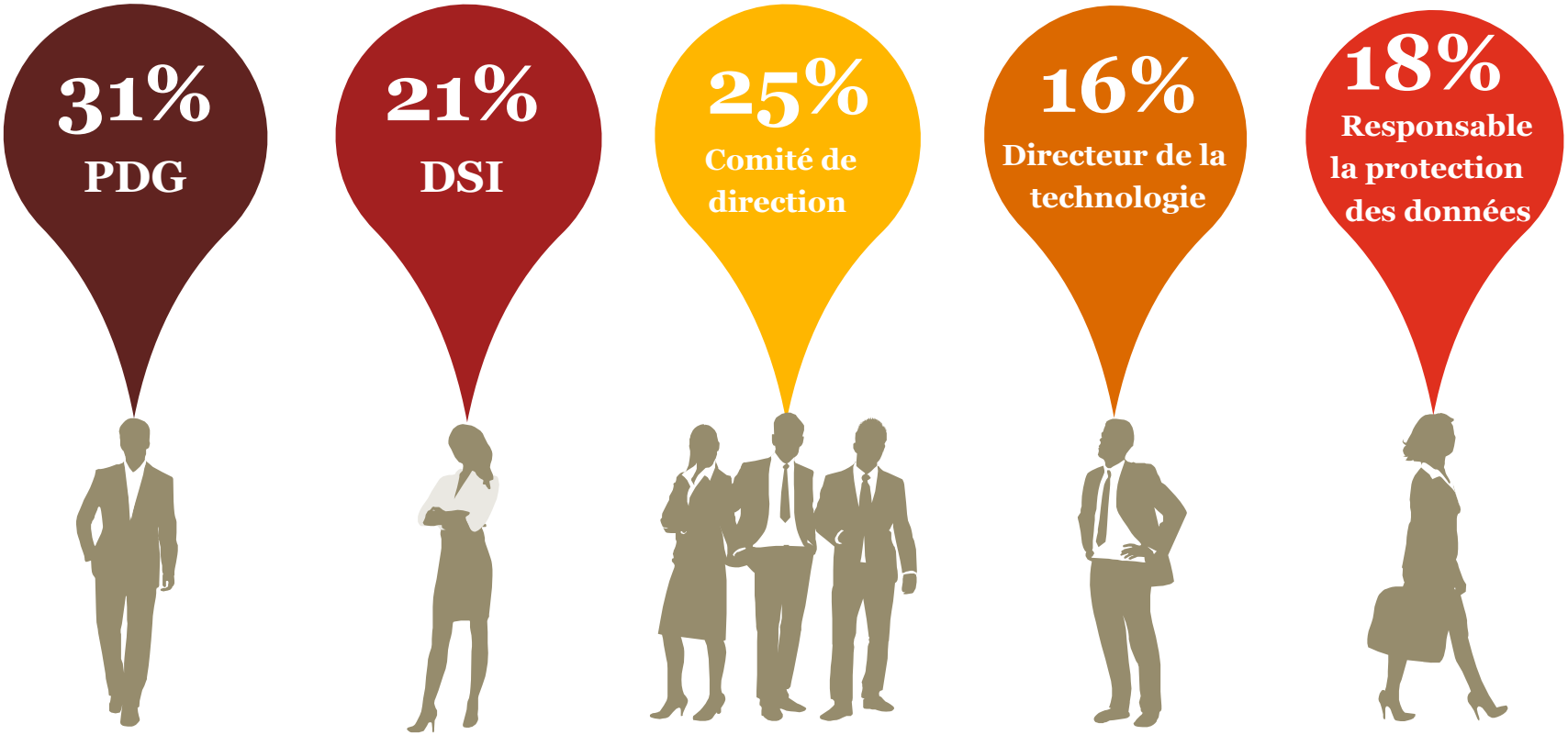
Postes ouverts en cybersécurité

Implication grandissante des comités exécutifs

3

De nombreux responsables de la sécurité reportent directement au PDG

Rattachement hiérarchique direct du RSSI/RSI

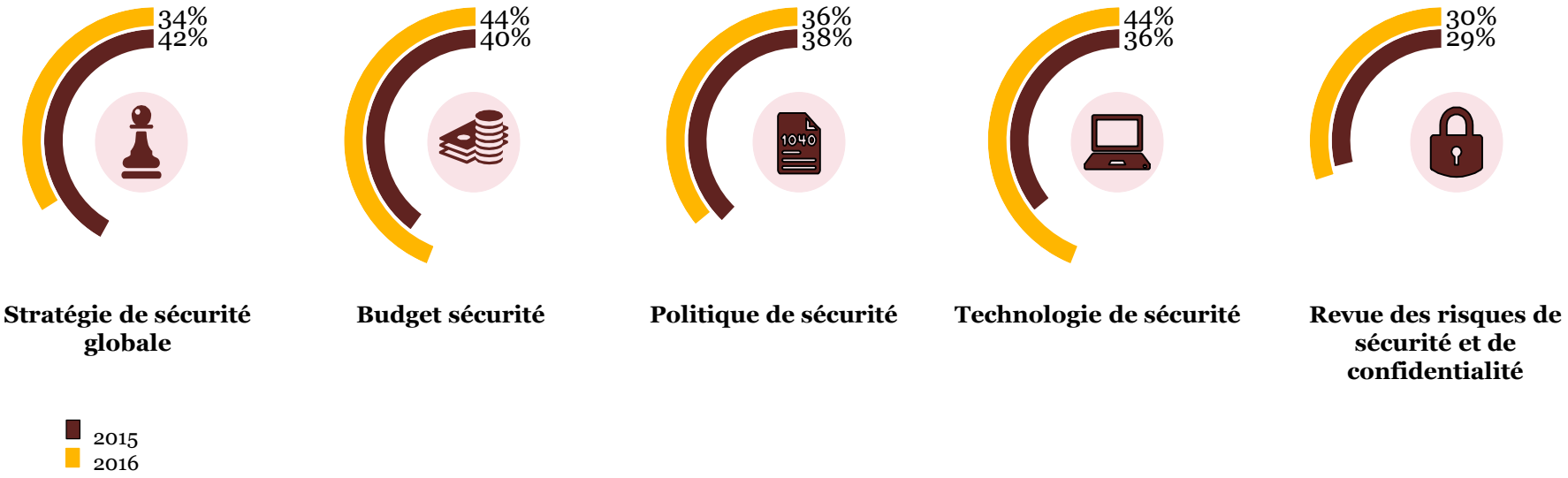


49 % des entreprises interrogées comptent une fonction RSSI

Le comité exécutif s'implique davantage dans les problématiques de cybersécurité

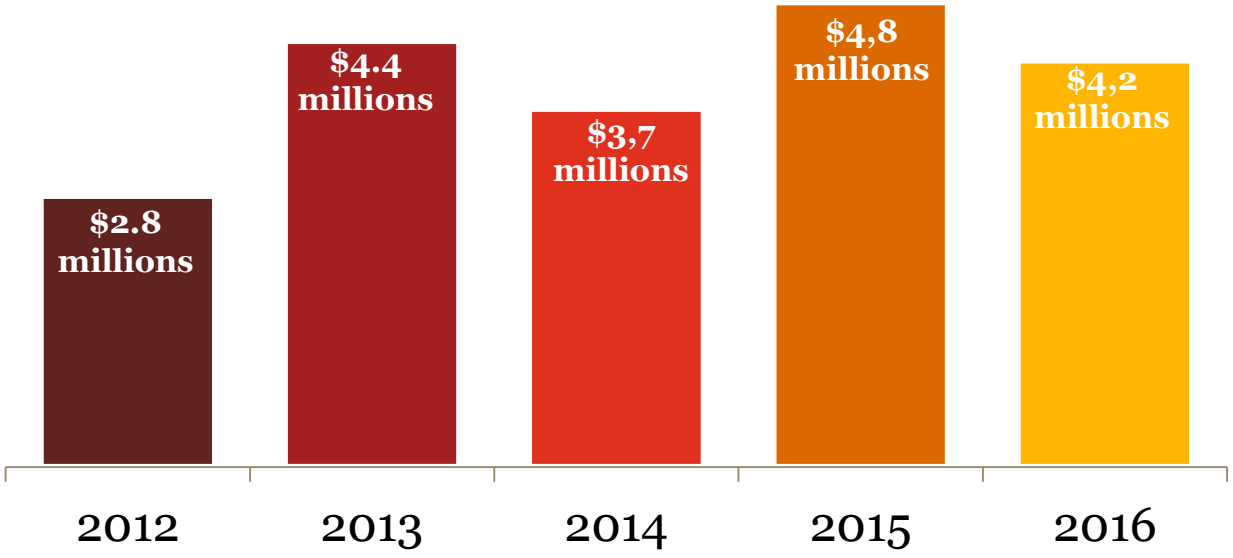
Les répondants ont affirmé que l'implication de plus en plus poussée du comité exécutif a permis d'améliorer les pratiques de cybersécurité.

Les principaux sujets d'implication



Un budget sécurité globalement stable depuis 2013

Un budget sécurité informatique qui augmente chez **7 industries sur 12**, mais une **moyenne** qui reste **stable** depuis 2013



Budget sécurité informatique par années

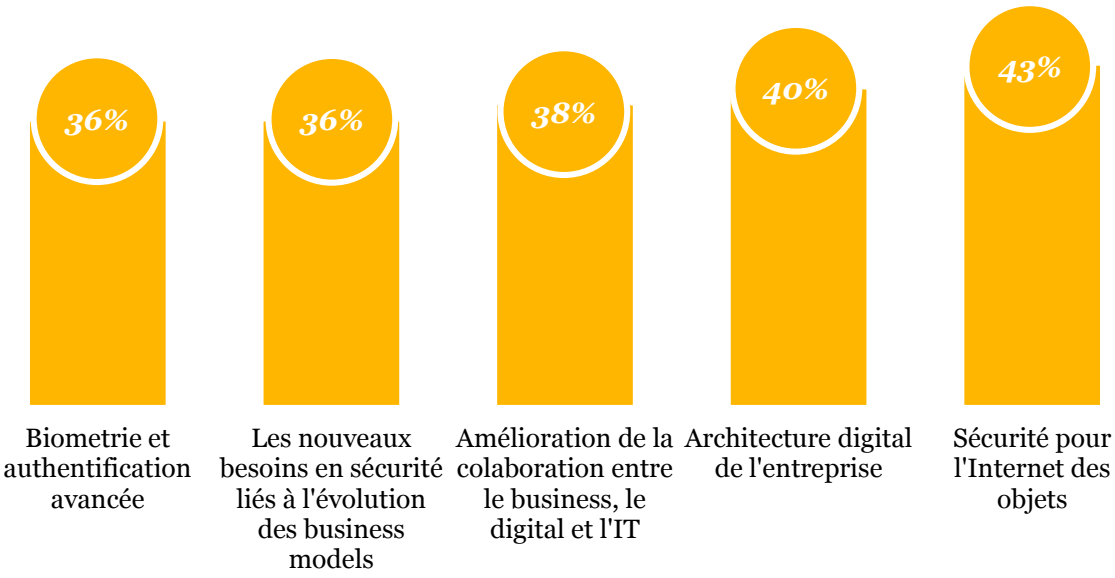
D'augmentation de budget reporté par les services financiers, l'industrie santé et l'automobile

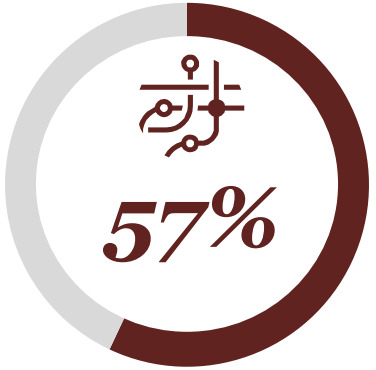
Un renforcement des investissements visant à protéger l'écosystème numérique

Les **priorités** de sécurité en 2016 sont :

- la collaboration interne
- l'architecture digitale
- la sécurité de l'IoT

Le **digital** et la **Cybersécurité** sont devenus des piliers pour les entreprises, liés aux nouveaux besoins clients





Disent que la digitalisation a impacté les dépenses en Cybersécurité

Dépenses prioritaires pour la sécurité informatique en 2016

Collaboration à tous les niveaux

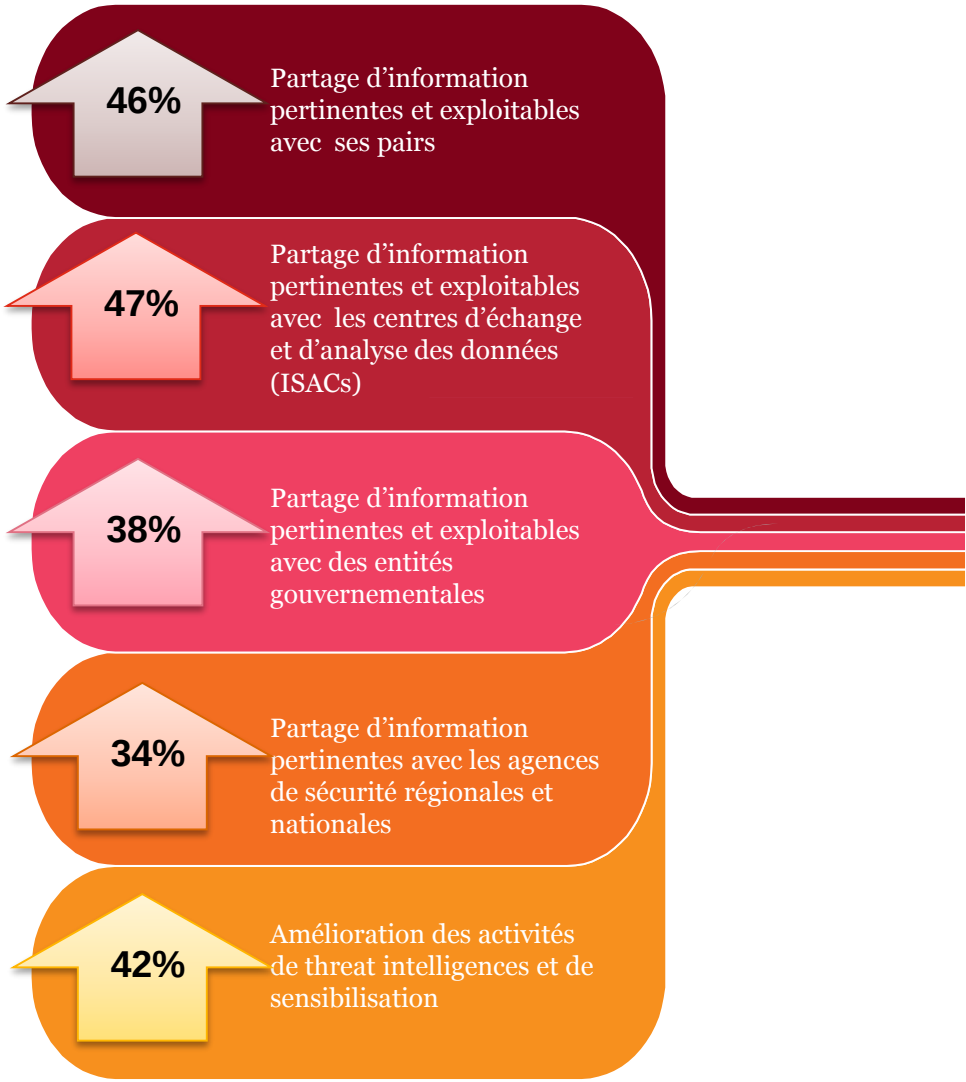
4

Collaboration à tous les niveaux

Au cours des trois dernières années, le nombre d'organisations qui adoptent une démarche collaborative avec des entités externes augmente de façon régulière.

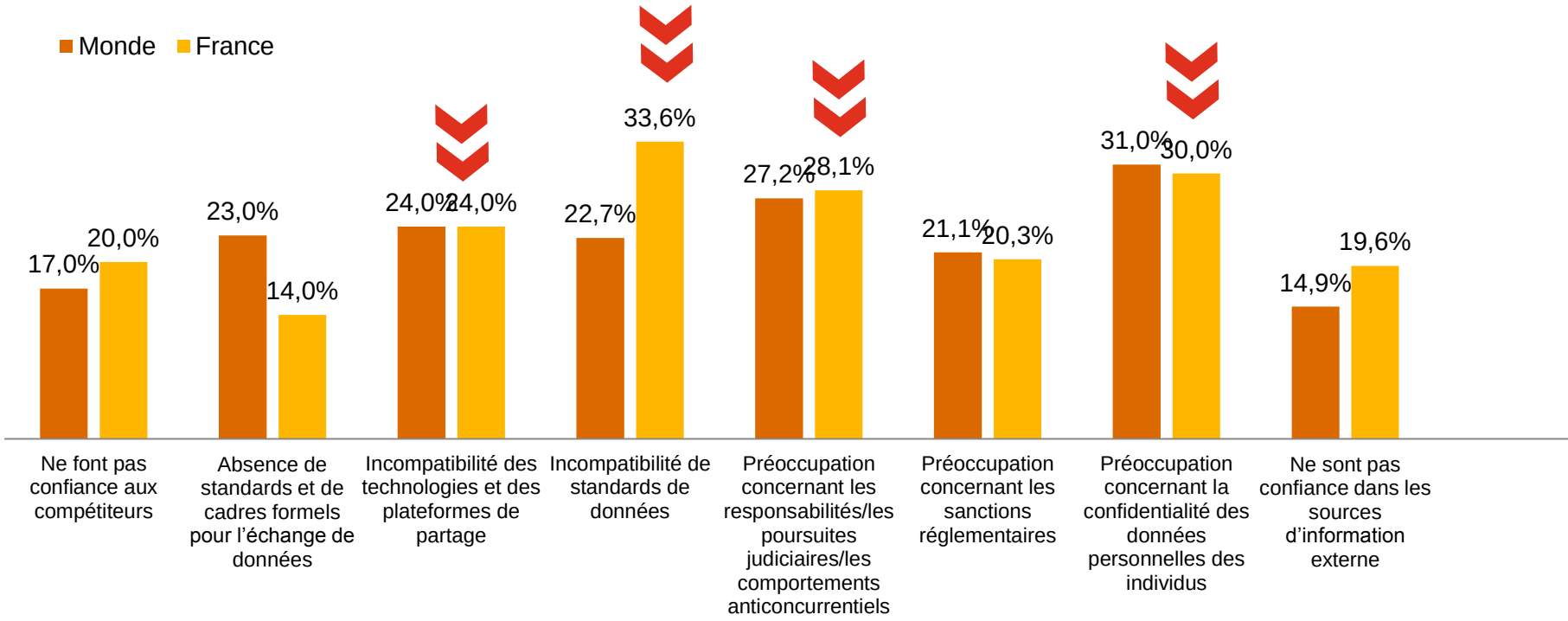
Plus de la moitié des organisations questionnées ont affirmé tirer de réels bénéfices d'une collaboration avec d'autres acteurs du même secteur d'activité et avec les centres d'échange et d'analyse des données.

Ces organisations affirment que la collaboration permet l'amélioration des activités de threat intelligences et de sensibilisation.



Collaboration à tous les niveaux

D'après les organisations questionnées, le principal frein au partage de données avec les tiers est **l'absence de standards, de cadre formel d'échange** et **la confidentialité des données personnelles**. En France, l'absence d'échange est guidée par le **manque de confiance envers les compétiteurs et l'incompatibilité des technologies et des plateformes.**



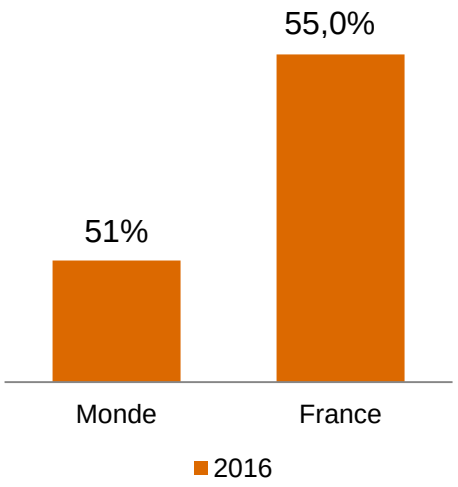
Cloud, Externalisation des services de sécurité, Big Data : l'innovation au service de la Cybersécurité

5

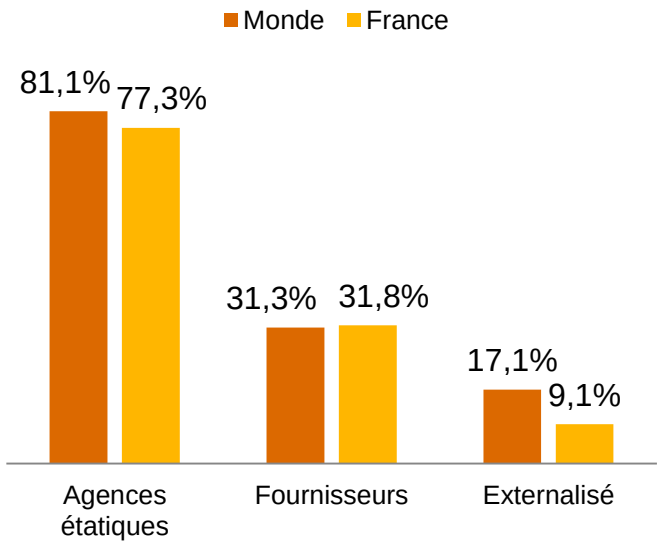
Le SOC, cœur névralgique du système de cyberdéfense (1/2)

En matière de détection et de réponse aux menaces, le SOC (Security Operations Center) est présenté comme **incontournable** pour les grandes entreprises.

Répondants disposant d'un SOC

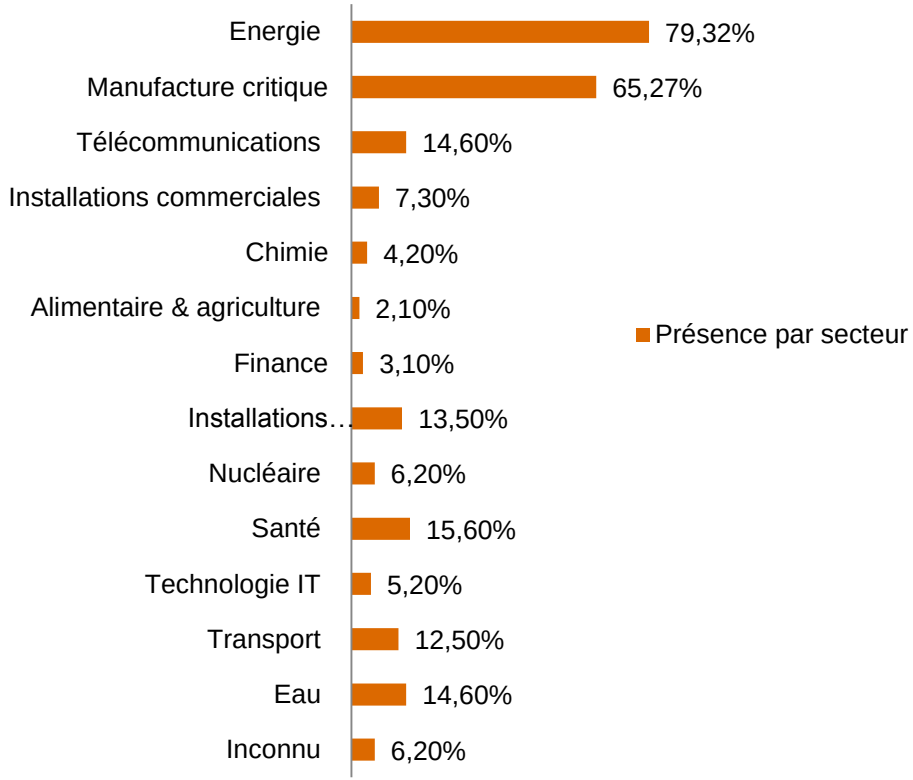


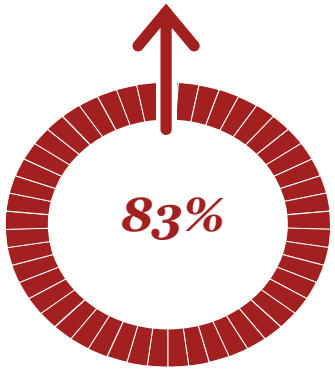
Exploitation du SOC



Un décalage croissant entre la sécurité des systèmes industriels et le paysage des cybermenaces

De nombreux secteurs d'activités (services publics, le transport, la logistique, l'industrie ou la santé) sont concernés par la sécurité de leur systèmes industriels qui peut se résumer aujourd'hui à **l'isolation du réseau informatique traditionnel par rapport au réseau des systèmes industriels.**



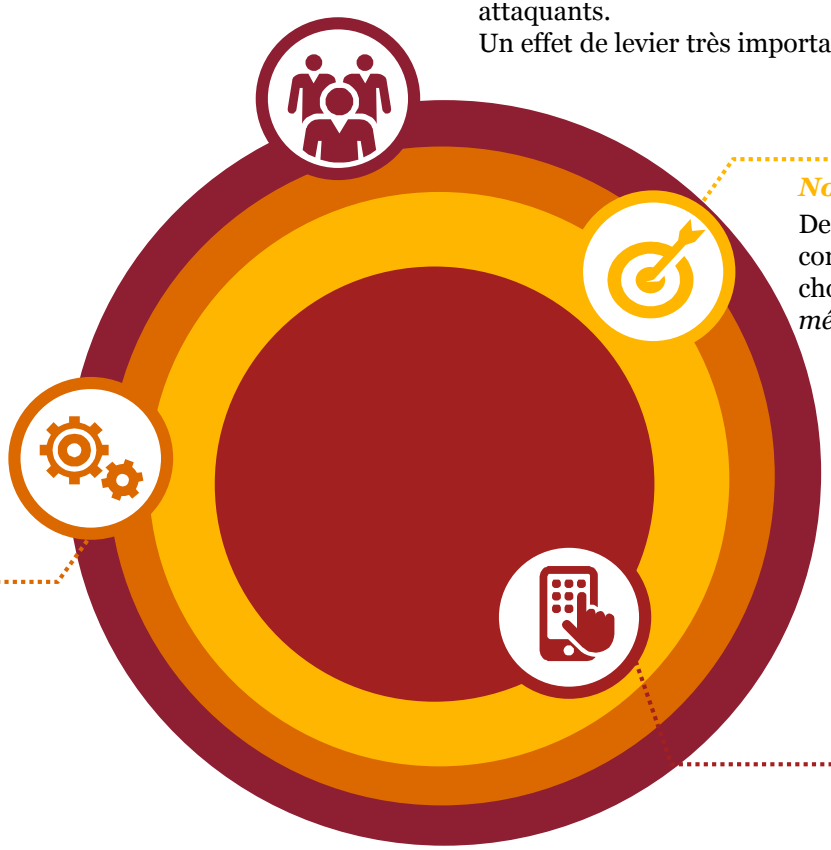


d'augmentation des attaques visant les systèmes industriels en France en 2016

Un décalage croissant entre la sécurité des systèmes industriels et le paysage des cybermenaces

Les principales causes des incidents sur les systèmes industriels

L'apparition de nouveaux attaquants
Une position dominante des Etats dans le spectre des attaquants.
Un effet de levier très important pour les attaquants isolés.



Nouvelles cibles
Des secteurs historiquement non concernés qui deviennent des victimes de choix (*transport, télécom, électricité, médical, etc.*)

Obsolescence des infrastructure SCADA-legacy
Des infrastructures vitales opérés grâce à des technologies vieillissantes

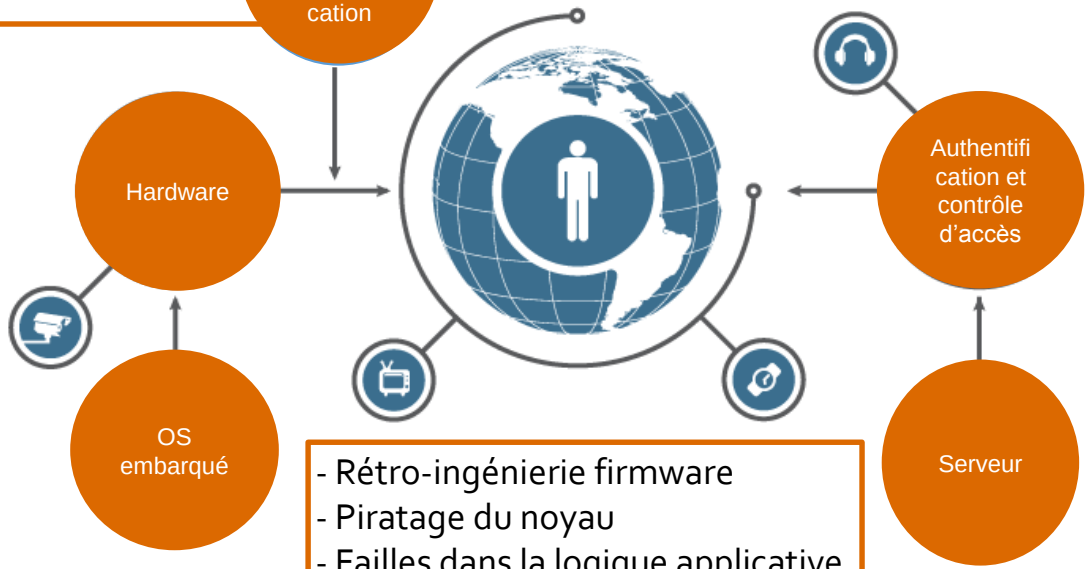
Une forte évolution des composants et un déploiement élargi des technologies SCADA
Une croissance continue de la portée de ces technologies, bien au-delà des frontières industrielles.
Des équipements et des sondes autrefois analogiques qui deviennent des objets connectés (Internet des Objets).

Un décalage croissant entre la sécurité des systèmes industriels et le paysage des cybermenaces

Les vecteurs d'intrusion

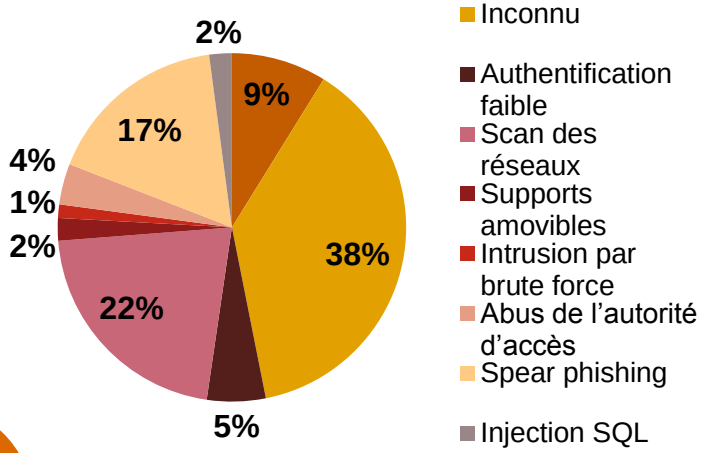
- Désassemblage d'appareils
  - Identification des composants
- Analyse entropique
  - Analyse des signaux
- Espionnage des canaux
  - Découverte du canal de Fréquences utilisées

- Test de signal radio
  - Vérification de fonctionnement
- Cryptographie
  - (Dé)chiffrement des données
- Rétro-ingénierie de protocoles
  - Extraction du protocole employé



- Rétro-ingénierie firmware
- Piratage du noyau
- Failles dans la logique applicative
- Injection de malware

Répartition des vecteurs d'intrusion



- Elévation de privilèges
  - Prise du rôle administrateur
- Compromission de session
  - Vol de session

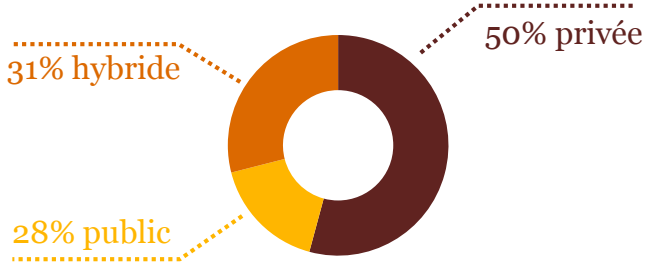
Le Cloud…

Le Cloud offre :

- Une capacité de **ressources** illimitée
- Une architecture et une puissance de calcul permettant d'effectuer des **analyses Big Data** à moindre coût. Ces analyses Big Data sont la clé de voute qui permettra de détecter les signaux faibles des attaques de cybersécurité.

Les bénéfices de l'utilisation du Cloud:

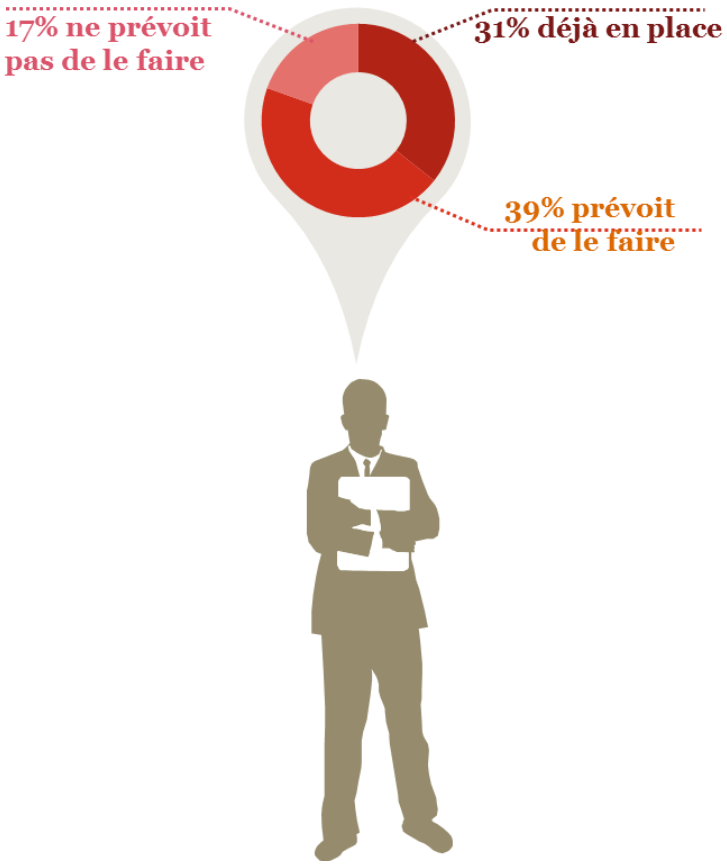
- **Réduire les coûts**
- **Identifier et répondre plus rapidement aux menaces**
- **Mieux connaitre le comportement du consommateur**
- **Améliorer la Cybersécurité grâce au machine learning et à l'intelligence artificielle**



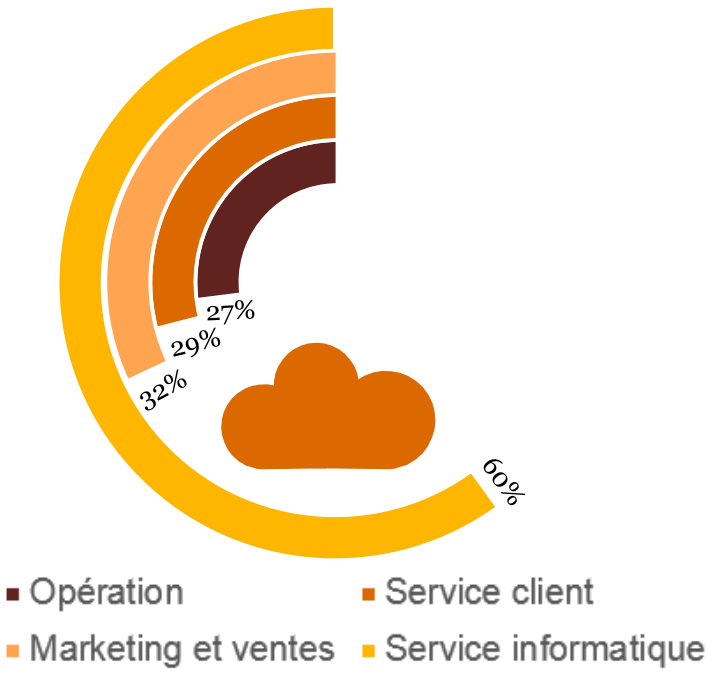
Types de cloud utilisés

Le Cloud… sans limite ?

Les entreprises stockent de plus en plus de **données sensibles** sur le Cloud, ce qui les rend **dépendantes** de leurs fournisseurs et menace la **confidentialité**, **l'intégrité** et la **disponibilité** de leurs **données**



Fonctions déployées sur le cloud

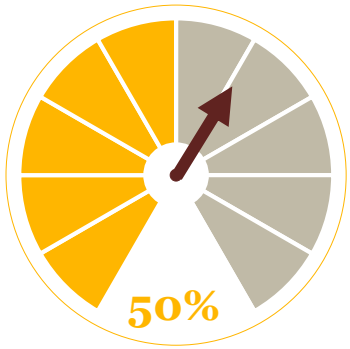


Le Big Data entre en jeu…

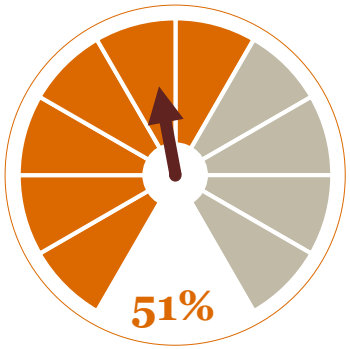
Le Big Data permet de détecter les signaux faibles laissés par les cyberattaques et donc de repérer une attaque persistante avancée.

En France, **32%** des répondants considèrent l'analyse des données comme un levier d'amélioration de la sécurité car elle permet aux organisations **d'utiliser les informations en temps réel** de façon à pouvoir **prédire les incidents de sécurité**.

Les bénéfices du Big Data

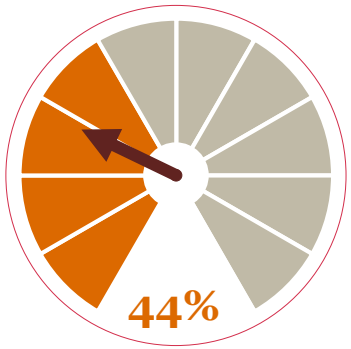


Une meilleure compréhension des menaces externes

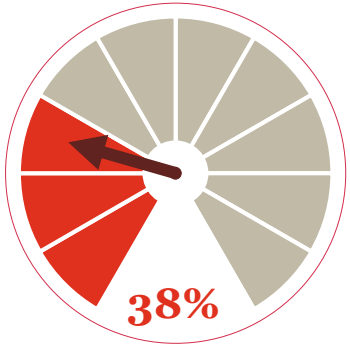


Une meilleure compréhension des menaces internes

Une meilleure compréhension du comportement des utilisateurs



Une meilleure visibilité sur les activités anormales sur le réseau

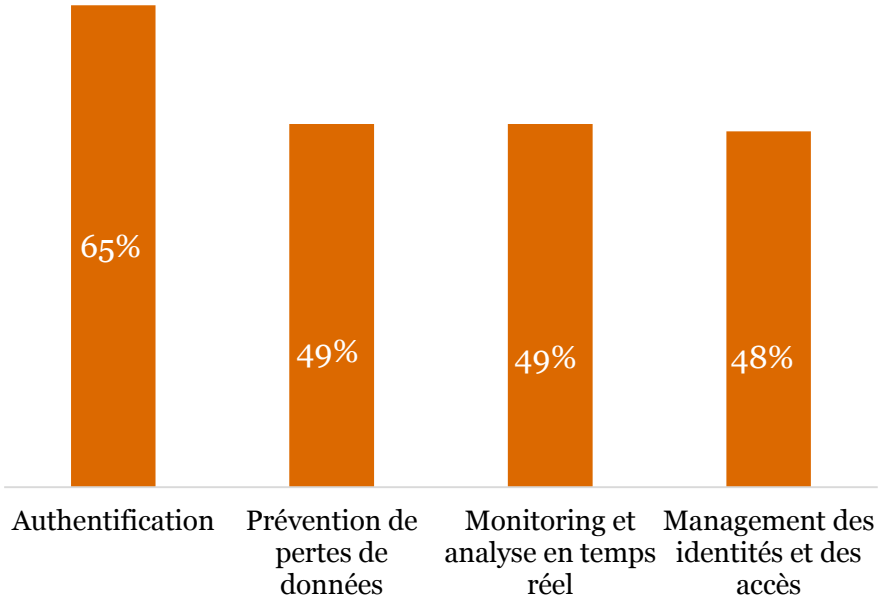


Une meilleure réactivité face aux incidents de sécurité

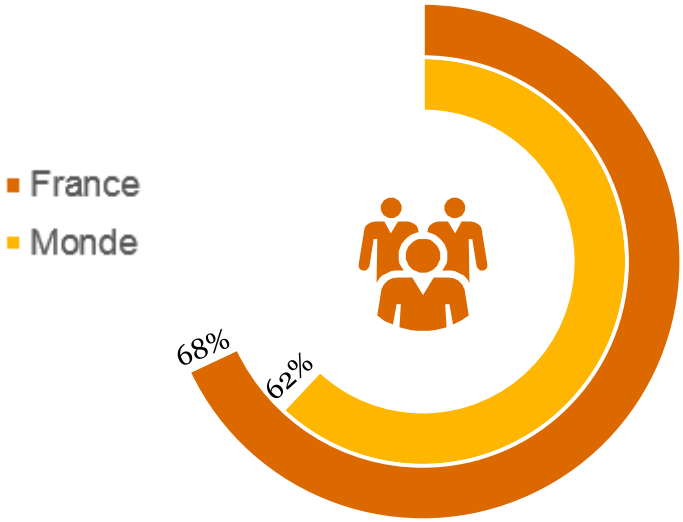
L'externalisation, une solution?

De plus en plus d'entreprises utilisent des **fournisseurs de services** pour améliorer et gérer leurs programmes de **Cybersécurité**

Services externalisés utilisés par les personnes sondées en France



Personnes sondées utilisant l'externalisation des systèmes de sécurité

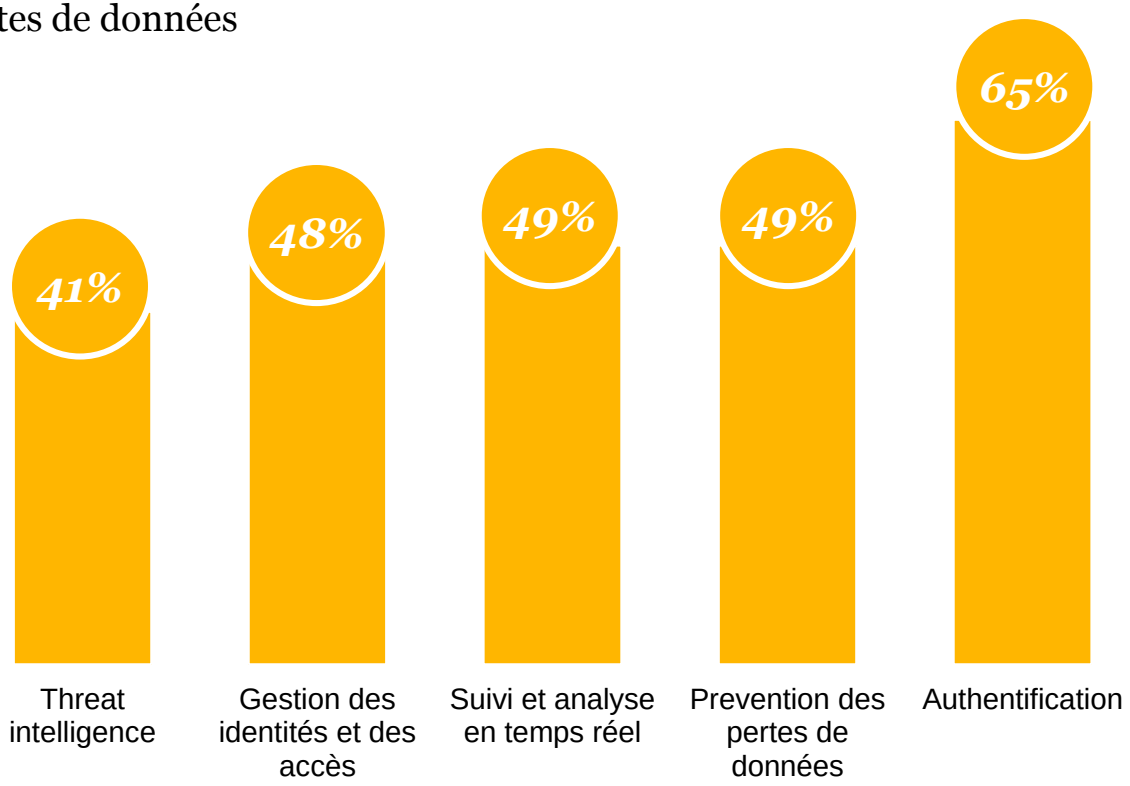


Une croissance de l'utilisation des services de sécurité managé

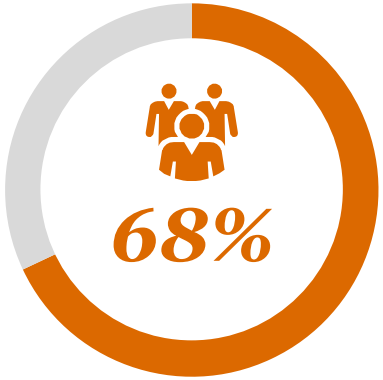
Les entreprises utilisent de plus en plus les **services managés de sécurité** car :

- Un **manque de spécialistes** dans le domaine de la sécurité est constaté
- Leurs **prix** est avantageux

L'externalisation cible les **initiatives techniques** comme l'authentification et la prévention des pertes de données



Types des services de sécurité managé utilisés



Utilisent des services externalisés pour la Cybersécurité

L'externalisation, une solution?

La **Cybersécurité** et la **protection de données** est un vrai challenge pour les entreprises, car on observe :

- Un manque de **personnes compétentes** dans le domaine
- Un manque de **moyens financiers** nécessaires pour engager une équipe à temps plein en interne

Par conséquent, les entreprises se tournent vers des fournisseurs de services, qui proposent :

- Des personnes hautement **qualifiées**
- Des outils **sophistiqués**
- Une détection et une réponse rapide aux **menaces**
- Une **aide** pour améliorer les investissements et les processus de Cybersécurité

Les services proposés sont disponibles 24/7

1,9 millions de nouveaux emplois dans la Cybersécurité d'ici 2019

La protection de données personnelles un enjeu de sécurité poussé par la réglementation

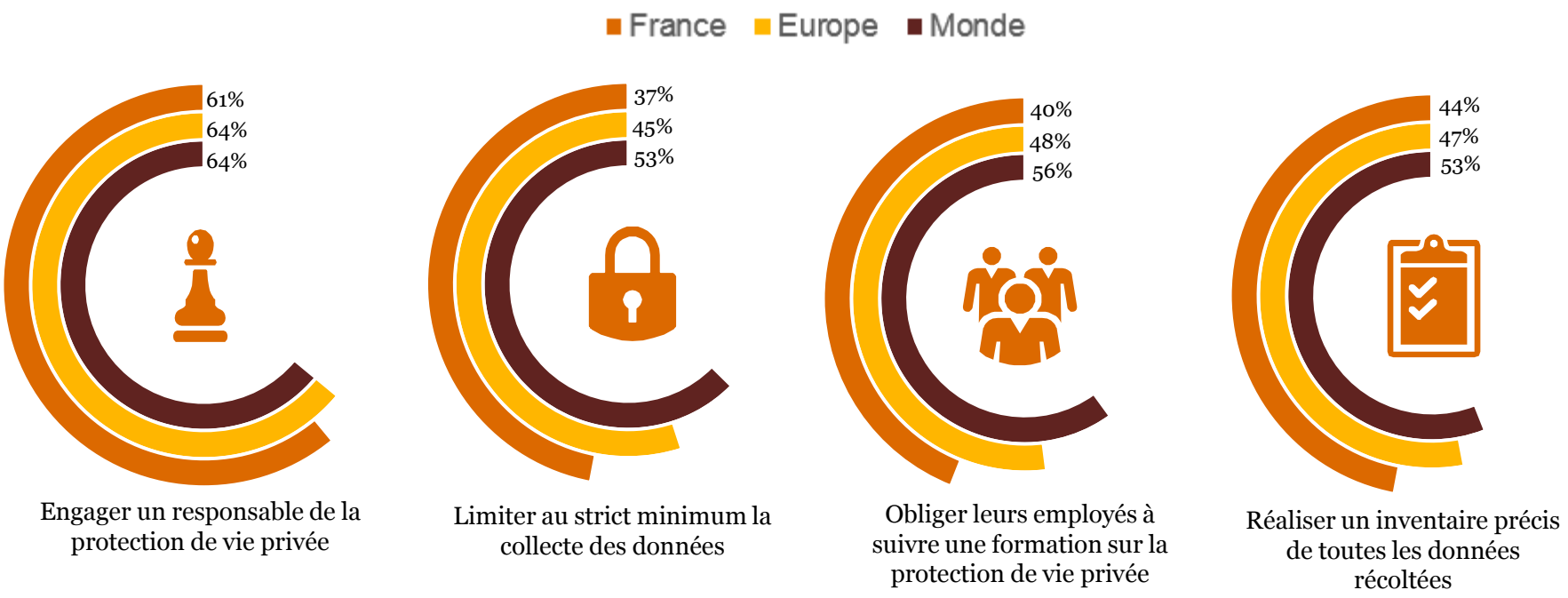
6

Les nouvelles contraintes sur les données privées

La GDPR est la **réglementation** qui exige un niveau de contrôle interne élevé en terme de confidentialité

Actuellement, la France et l'Europe en général ont un léger **retard** sur la **protection des données**

Dispositifs de protection mis en place par les personnes sondées



Les nouvelles contraintes sur les données privées

La protection des données privées est devenue un **besoin critique** pour les entreprises, afin de gagner la **confiance des consommateurs** et de se **mettre en conformité** avec de nouvelles réglementations (GDPR)

Dans le cadre de la mise en application de la GDPR, les entreprises devront:

- Disposer d'un **inventaire** de toutes les données collectées
- Obtenir le **consentement explicite** pour la collecte de données personnelles
- Permettre le **droit à l'oubli**
- Prévenir l'utilisateur en cas de **compromission** de ses données
- Evaluer la sécurité de la **routine des données**, y compris chez les prestataires

Mise en application de la GDPR le 25 mai 2018

Des sanctions jusqu'à 4% du chiffre d'affaires dans la limite de 20 millions euros

La confiance par l'authentification forte

Les utilisateurs sont souvent **peu réceptifs** à la sécurité et utilisent des mots de passe **trop faibles**

L'authentification **forte** permet d'améliorer :

- La protection de données grâce à une nouvelle couche de sécurité
- La confiance grâce aux différents partenaires et utilisateurs
- L'expérience utilisateur

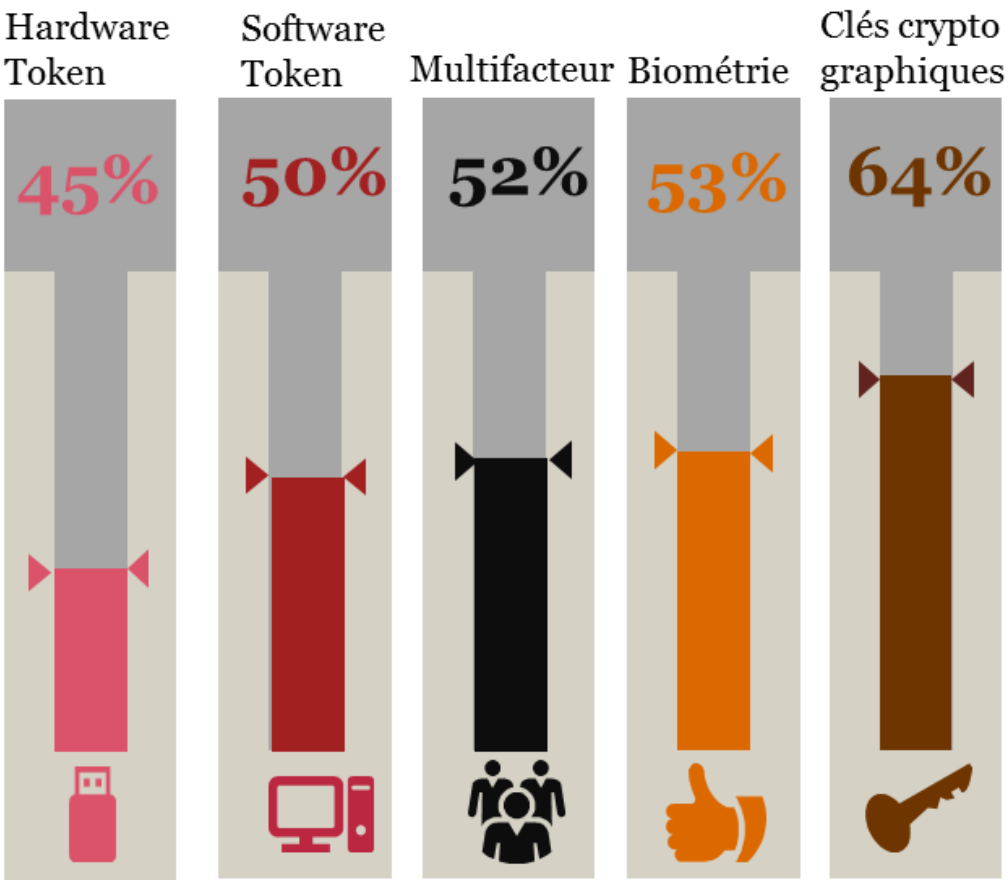
40% des personnes sondées pensent que cela augmente la confiance des partenaires et utilisateurs

39% disent que cela améliore l'expérience utilisateur

La confiance par l'authentification forte

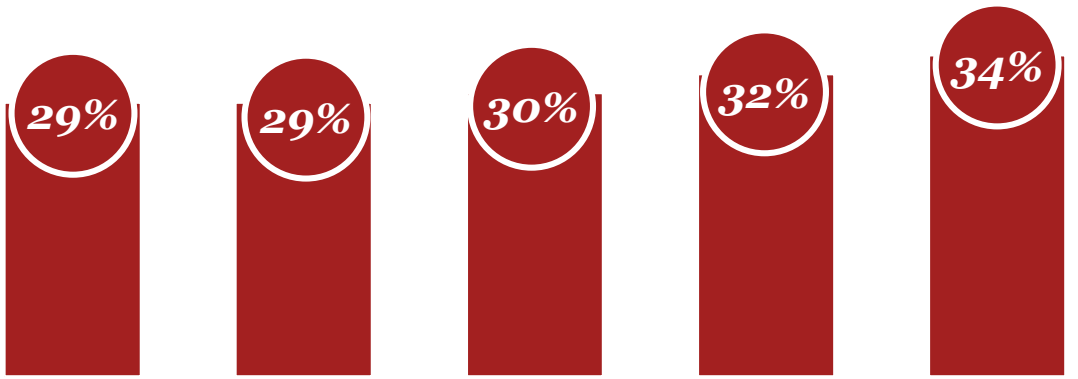
L'authentification forte requiert l'association de **plusieurs éléments** dans le but de prouver de manière irrévocable **l'identité** d'une personne

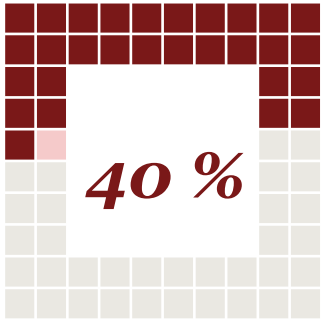
Systèmes d'authentification forte les plus utilisés



La formation des employés, priorité pour répondre à l'enjeu de la protection des données

Les nouvelles **réglementations** sur la protection de données (GDPR) obligent les entreprises à **améliorer leurs protections**



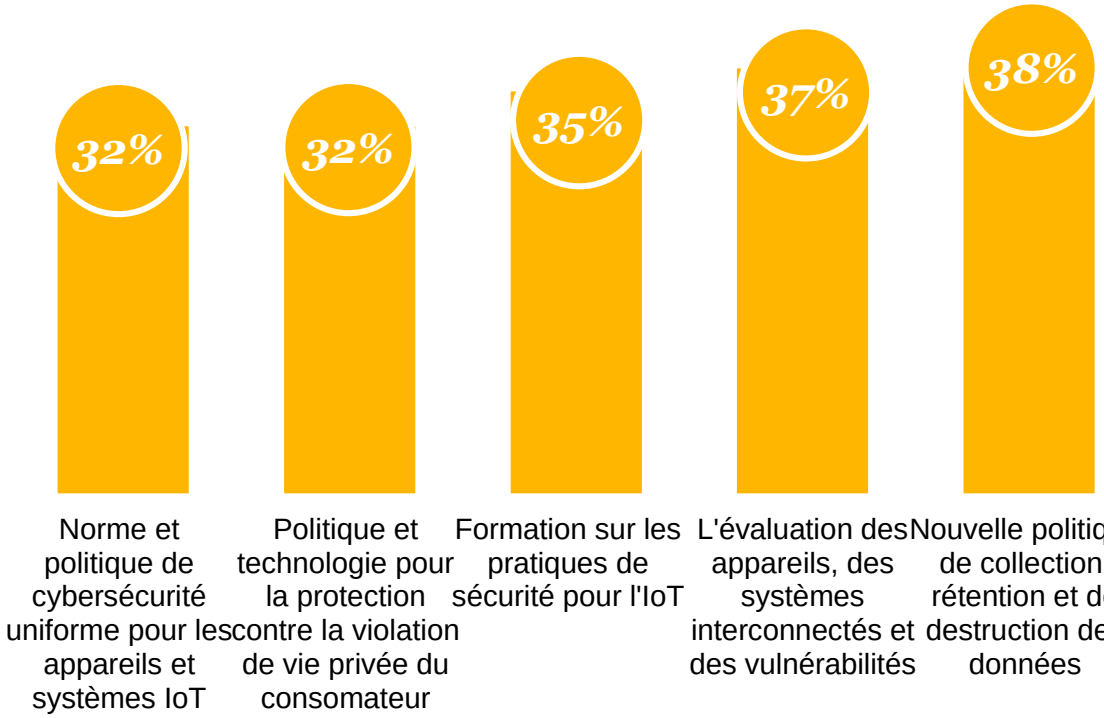


Des répondants obligent leurs employés à suivre une formation sur la protection de données

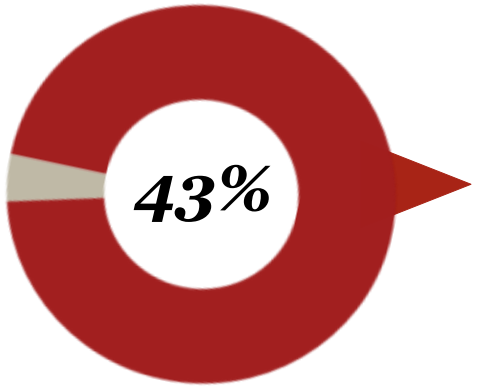
Principales initiatives planifiées sur la protection de données en 2016

Une croissance rapide de l'IoT qui pousse les entreprises à améliorer la Cybersécurité et à mieux protéger la vie privée

Les **objets connectés** génèrent une grande quantité d'information et des portes d'entrée pour des personnes malicieuses, ce qui pousse les entreprises à changer leur **politique de Cybersécurité** et à améliorer la **protection de la vie privée**



Politiques, compétences techniques et humaines utilisées pour l'Internet des objets

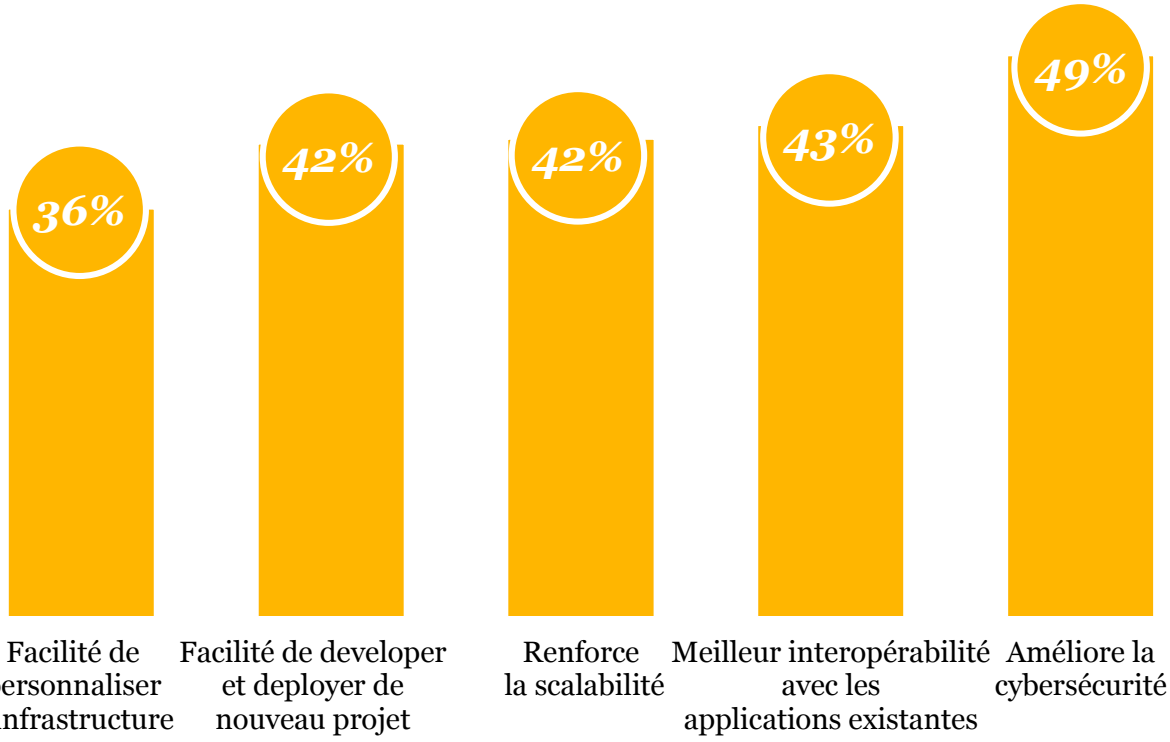


Investissent dans une stratégie de sécurité pour l'IoT

Une utilisation des logiciels open-source qui améliore la Cybersécurité

Les logiciels **open-source** sont de plus en plus utilisés car ils permettent :

- Une amélioration de **l'interopérabilité**
- Une disponibilité à **bas coût** ou **gratuits**



Impact des logiciels open-source

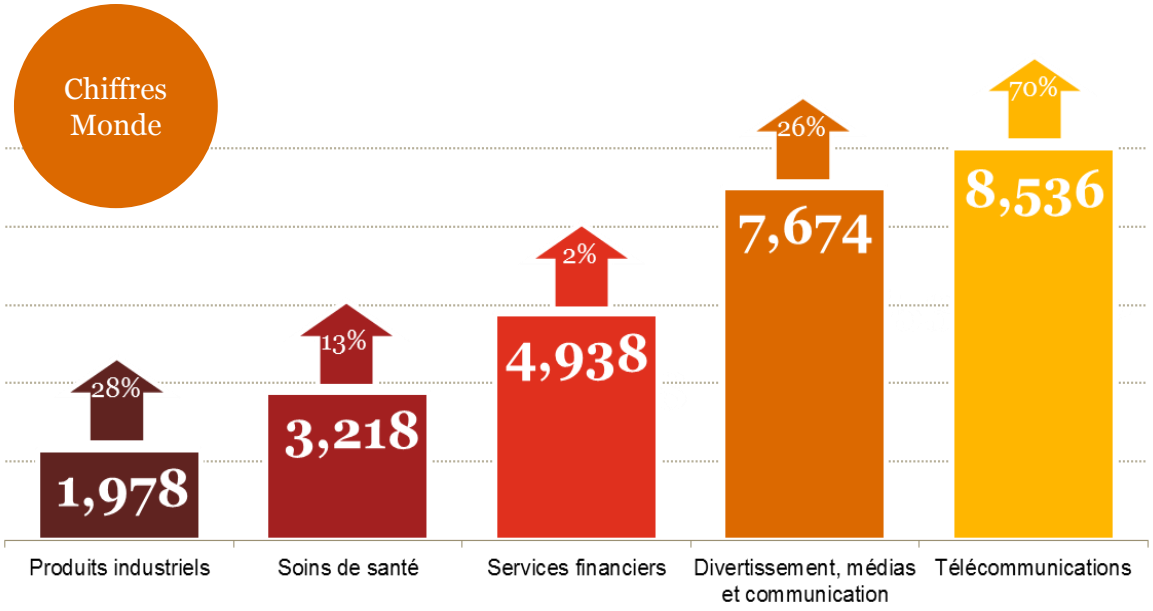
des répondants utilisent des logiciels open-source

Evolution, causes et impact des incidents

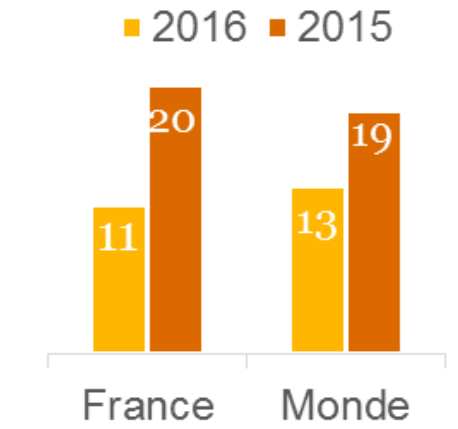
7

Des incidents de sécurité en baisse…

Une **diminution** d'environ **50%** du nombre d'incidents par jour en **France** mais une **augmentation** des incidents dans le monde sur **5** secteurs d'activités



Moyenne du nombre d'incident de sécurité dans le 12 derniers mois

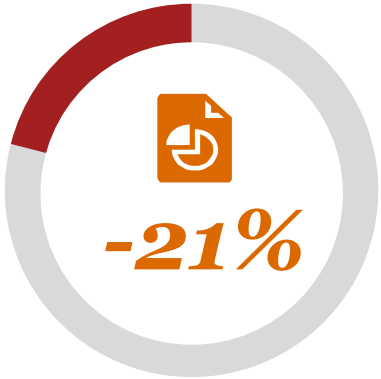


Nombre moyen d'incident par jour

* Un incident de sécurité est défini comme tout incident indésirable qui menace un aspect de la sécurité informatique

… entrainant la diminution des pertes financières

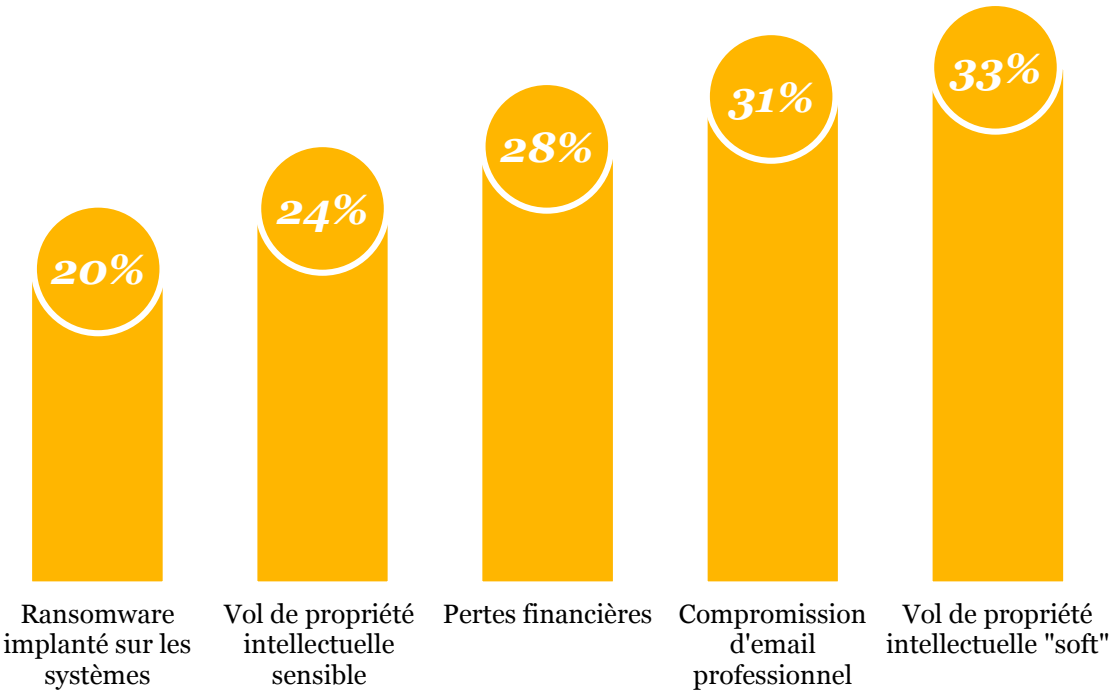
Une diminution moyenne de **21%** des **pertes financières** parmi les grandes entreprises et de **20%** à **90%** suivant les secteurs d'activités dans le **monde**



De pertes financières moyenne parmi les grandes entreprises

Le phishing en tête des vecteurs d'attaque

La **propriété intellectuelle** est la première cible, dépassant la compromission d'e-mail et les pertes financières avec un vecteur d'attaque privilégié, le **phishing**

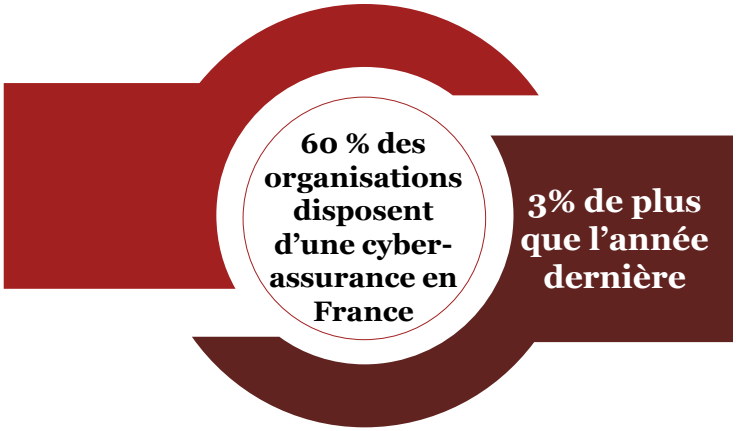


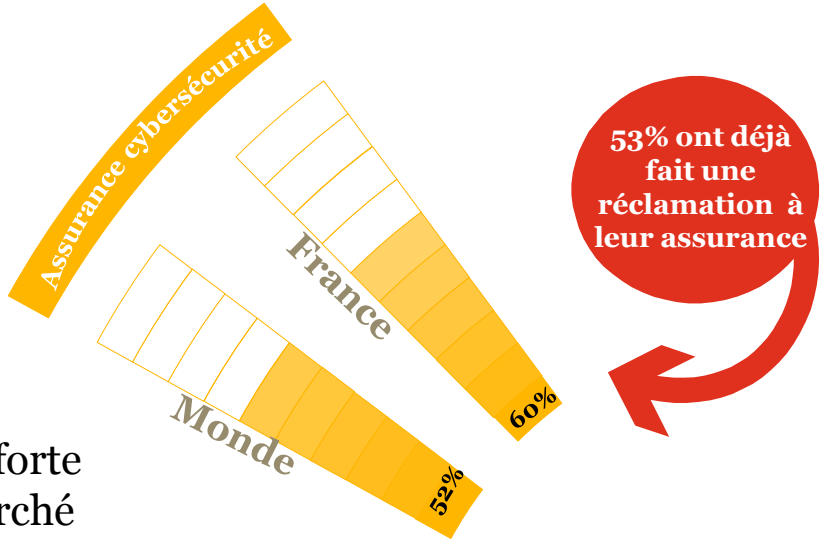
Impact des incidents de sécurité sur le business

« Ce qui ne peut être parfaitement protégé peut être assuré » (1/2)

Le partage d'informations avec les tiers et les technologies de cybersécurité innovantes ne peuvent pas stopper toutes les cyberattaques. Les assaillants, techniquement avancés, sont en mesure de contourner les barrières de sécurité.

De plus en plus d'organisations souscrivent à des **assurances cybersécurité** dans le but de limiter les pertes financières en cas d'incidents de sécurité avérés.





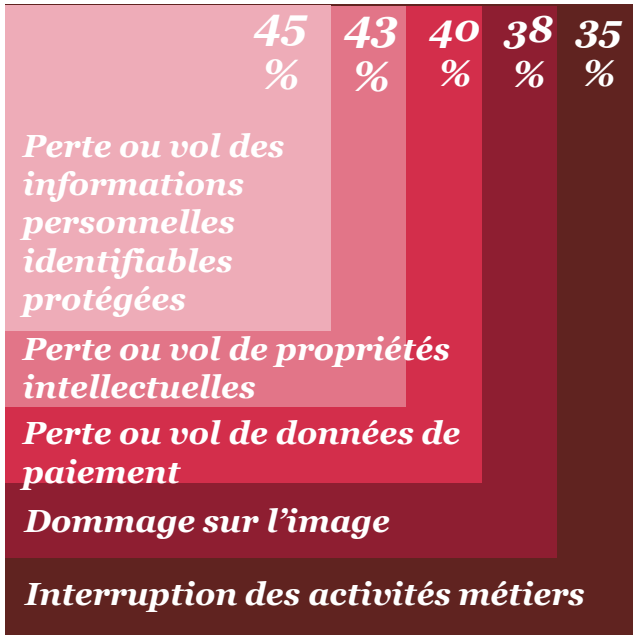
La cyber assurance est l'un des secteurs à plus forte croissance sur le marché de l'assurance. Le marché mondial de la cyber assurance devrait atteindre les **7,5 milliards de dollars** de chiffre d'affaires en 2020*.

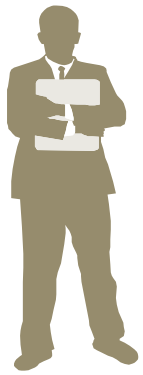
* Source: PwC, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience,* September 2015

« Ce qui ne peut être parfaitement protégé peut être assuré » (2/2)

En plus de **limiter les risques financiers** associés aux cyber attaques, les organisations qui souscrivent à une assurance cybersécurité commencent à gagner une **meilleure compréhension de leur niveau de maturité pour faire face aux cyber menaces**.

En France, les répondants déclarent que leur cyber assurance couvre les pertes suivantes:





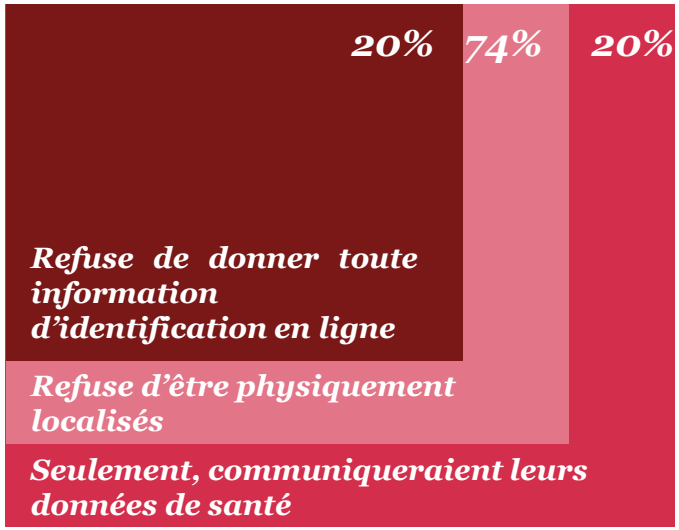
Les assureurs exigent une évaluation approfondie des capacités de protection de l'organisation contre les risques actuels comme condition préalable à une politique d'achat.

Conclusion : La confiance au cœur des enjeux numériques

8

Un monde en plein processus de digitalisation mais qui soulève des inquiétudes

Plusieurs études montrent qu'Internet échouent à offrir aux utilisateur un niveau de confiance adéquat.



Baromètre annuel sur la confiance numérique produit par l'ACSEL

(Source: http://www.acsel.asso.fr/resultats-du-barometre-2015-acsel-cdc-de-la-confiance-des-francais-dans-le-numerique/)

La tendance dévoile clairement une baisse de la confiance des utilisateurs en Internet.

Paradoxalement, chaque jour nous sommes de plus en plus à utiliser les medias sociaux, les solutions digitales, les sites de e-business, les applications collaborative, etc.

La confiance est et sera le principal facteur de réussite de la digitalisation

Les attaques à des fins de déstabilisation nuisent directement à l'image de marque de l'entreprise. Sa défaillance en matière de sécurisation des données est mise à nue. Si les organisation et les institutions ne sont pas en mesure d'offrir suffisamment de garanties pour se protéger et protéger leurs clients contre les cybermenaces, la confiance est rompue.

L'utilisation du e-commerce a baissé de

6%

La Redoute a augmenté ses ventes de 28%, sa base client de 10% et à baissée le coût de 18% en utilisant une stratégie basée sur l'analyse des données Facebook.

(Source: http://www.criteo.com/media/4960/criteo-laredoute-case-study-fr.pdf)

Plus de 25% des répondants de l'enquête 2015 "US to Privacy Index" de TRUSTe ont indiqué avoir des inquiétudes concernant la sécurité et la confidentialité des données collectées par les tiers à des fins de personnalisation de l'expérience utilisateur.

Ceci est une illustration directe de l'importance de la confiance dans la construction de nouveau « business models » supportés par Internet.

Merci pour votre attention !