



accenturesecurity

# SÉCURISER L'ÉCONOMIE DIGITALE

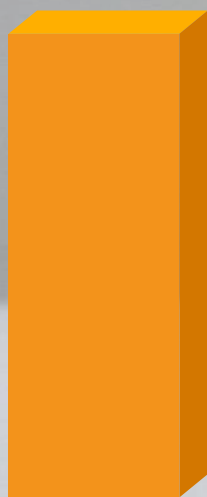
Repenser Internet pour renforcer la confiance

 ZOOM SUR  
DEMAIN



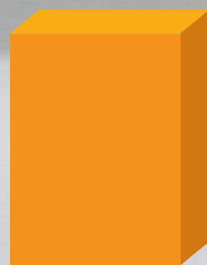
# Internet ne peut pas suivre

Les entreprises dépendent de plus en plus d'Internet pour leur croissance



**90%**

classent dans leurs trois principales priorités stratégiques, la croissance de leurs activités via les initiatives basées sur Internet.



**76%**

sont devenus largement dépendants d'Internet au cours des 10 dernières années.



**18% à 35%**

L'objectif de croissance pour les entreprises dépendantes d'Internet devrait doubler au cours des cinq prochaines années.



## ... Mais la confiance diminue dans les mesures de sécurité sur Internet

---

**68%**

déclarent que la dépendance à Internet augmente et que les risques de cybersécurité augmentent également.

---

**59%**

considèrent qu'Internet devient de plus en plus instable du point de vue de la cybersécurité, sans savoir précisément quelle réponse apporter à ce défi.

---

**50%**

prévoient une croissance future freinée car nous ne pouvons pas nous développer en toute sécurité dans l'économie digitale.

---

**Seul 30%**

sont très confiants dans les mesures de sécurité sur Internet pour leur entreprise, tombant à **25%** au cours des cinq prochaines années.

## Les risques sont élevés pour les entreprises, l'économie et la société

---

# 90%

des cadres supérieurs estiment qu'une économie digitale fiable est essentielle au développement futur de leur entreprise.

---

# 84%

des entreprises pensent que le potentiel économique d'Internet et de l'IoT serait libéré si nous pouvions créer une économie digitale plus fiable.

Accenture estime que les opportunités de revenus à risque sont de

# 2.8%

par an pour les grandes organisations au cours des cinq prochaines années.

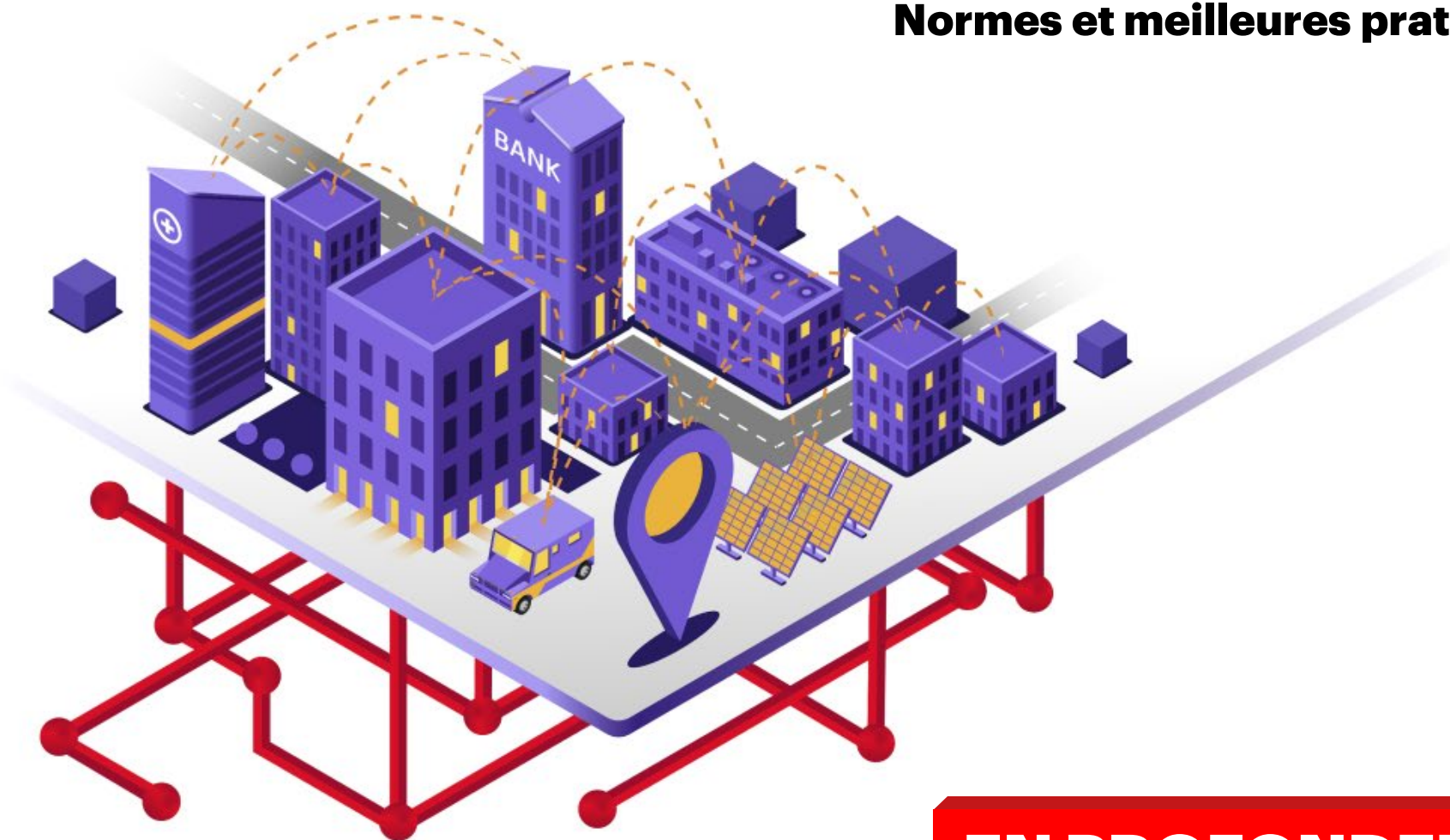
En d'autres termes, la cybercriminalité pourrait coûter aux entreprises

# 4.6Mrd€

sur les cinq prochaines années.

**EN SURFACE**

**Normes et meilleures pratiques**



**EN PROFONDEUR**

**Investissements technologiques**

## EN SURFACE

Là où les décisions d'affaires sont prises au sujet des normes et des meilleures pratiques dans les entreprises et les écosystèmes.

### Gouvernance

75%

des répondants estiment que la résolution des problèmes de cybersécurité nécessitera un effort collectif et réfléchi.

### Architecture d'entreprise

80%

estiment qu'il est de plus en plus difficile de protéger leur organisation des faiblesses dont souffrent leurs partenaires tiers, compte tenu de la complexité et du caractère tentaculaire des écosystèmes connectés modernes.

## EN PROFONDEUR

Là où les nouvelles technologies et les innovations pour sécuriser Internet peuvent faire progresser les entreprises et renforcer la sécurité digitale.

### Technologie

79%

reconnaissent que leur organisation adopte les technologies émergentes plus rapidement qu'elle ne parvient à résoudre les problèmes de cybersécurité qui en découlent et de garantir une économie digitale résiliente.

# IMPULSER D'IMPORTANT CHANGEMENT

Découvrez comment les dirigeants peuvent aider à établir un climat de confiance pour l'économie digitale de demain.

## 1

---

### **GOVERNANCE :**

**Joignez vos forces à celles d'autres entreprises et mettez en place une gouvernance mondiale**

- Créer un code d'éthique pour chaque secteur et des principes guidant les normes de sécurité sur Internet.
- Promouvoir un contrôle des identités en ligne par les consommateurs.
- Aider à réduire la stigmatisation liée aux cyberattaques en s'engageant à partager des informations dessus.

## 2

---

### **ARCHITECTURE D'ENTREPRISE :**

**Assurez votre connectivité et votre protection en adoptant un modèle fondé sur la confiance numérique**

- Prioriser la sécurité "by design".
- Responsabiliser les dirigeants à propos de la sécurité.
- Embarquer un RSSI au comité de direction.
- Protéger l'ensemble de la chaîne de valeur.

## 3

---

### **TECHNOLOGIE :**

**Renforcez la sophistication technologique et la sécurité de votre activité**

- Mener des campagnes pour résoudre les vulnérabilités dans le Protocole Internet (IP) de base.
- Renforcer la sécurité jusqu'au "bout".
- Adoptez les avantages du "Software-Defined Networking" (SDN).
- S'attaquer à la question du quantum.

## À propos de l'étude

Accenture Research a interrogé 1 711 cadres dirigeants travaillant pour des entreprises dont le chiffre d'affaires annuel est supérieur ou égal à un milliard de dollars, cela en octobre et novembre 2018 et dans 13 pays : Allemagne, Australie, Brésil, Canada, Chine, Espagne, États-Unis, France, Inde, Italie, Japon, Royaume-Uni et Suisse. Des entretiens approfondis ont été menés avec des PDG (61 %), des directeurs opérationnels (20 %), des directeurs de l'innovation (9 %) et des directeurs de la stratégie (9 %). Le coût moyen de la cybercriminalité a été calculé en pourcentage des revenus pour chaque secteur, en incluant le coût engendré par une cyber-attaque de grande ampleur. Ces pourcentages sectoriels ont ensuite été appliqués aux revenus mondiaux de chaque secteur pour générer un modèle d'évaluation des risques sur cinq ans et pour chaque industrie.

---

### En savoir plus

[www.accenture.com/ReinventTheInternet](http://www.accenture.com/ReinventTheInternet)