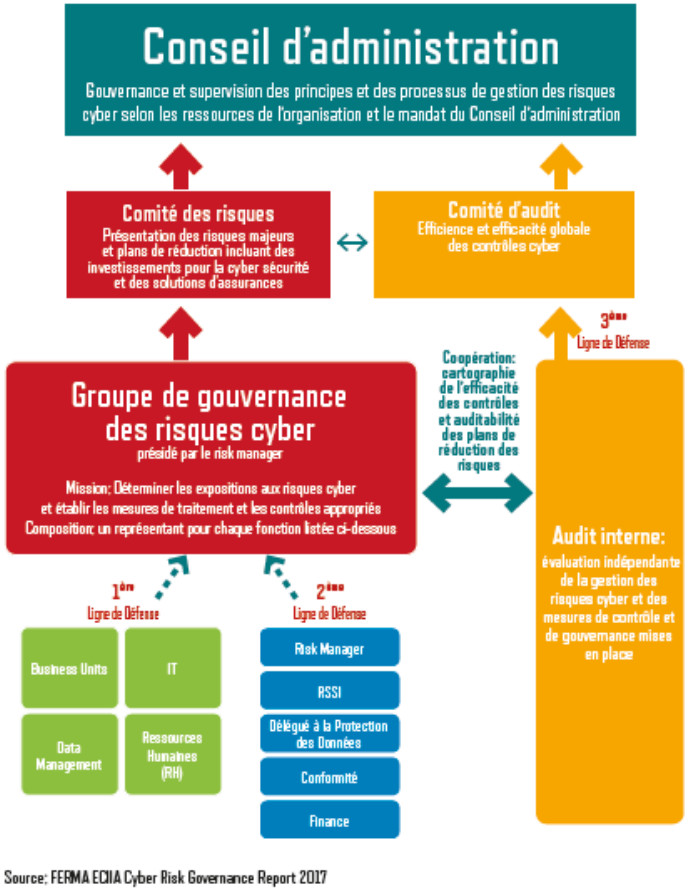
Comment organiser la gouvernance des risques cyber ?

26èmes Rencontres du Risk Management | AMRAE 2018

POUR UNE GOUVERNANCE D'ENTREPRISE DU RISQUE CYBER

Des propositions de standard européen



Source: FERMA ECIIA Cyber Risk Governance Report 2017

Point clé: la creation d'un groupe de gouvernance cyber risk

- **Une équipe multifonctionnelle coordonnée par le risk manager**

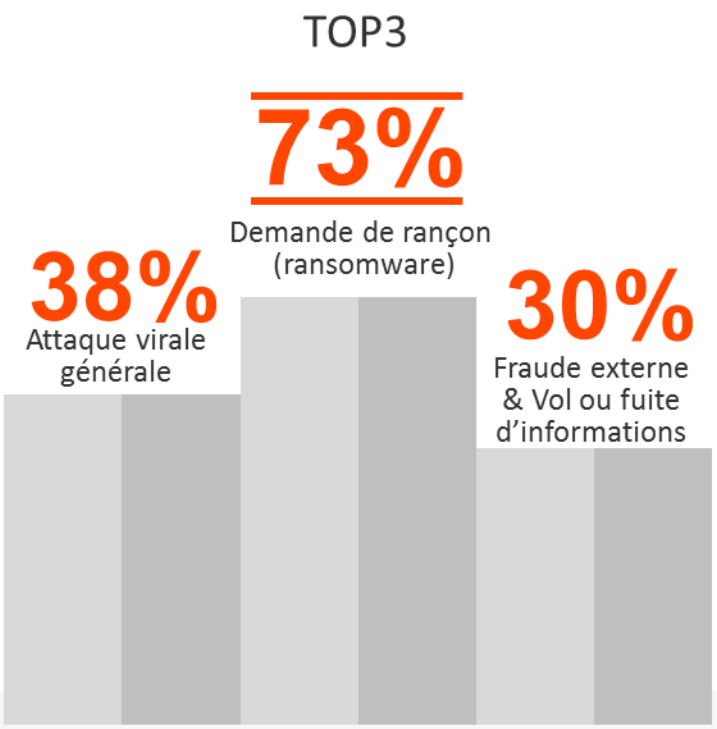
  Composée de fonctions opérationnelles de la 1ere ligne de defense et fonctions clés de la 2eme ligne de defense afin de **determiner l'exposition au risque cyber** en termes financiers et **designer les possibles plans de mitigation**

- **Pourquoi multifonctionelle?**

  La confrontation de la connaissance Business avec l'expertise en sécurité permet de développer un **consensus** sur l'identification des scenarios critiques pour l'entreprise et lister les options de reponses demandant un **arbitrage** managerial.

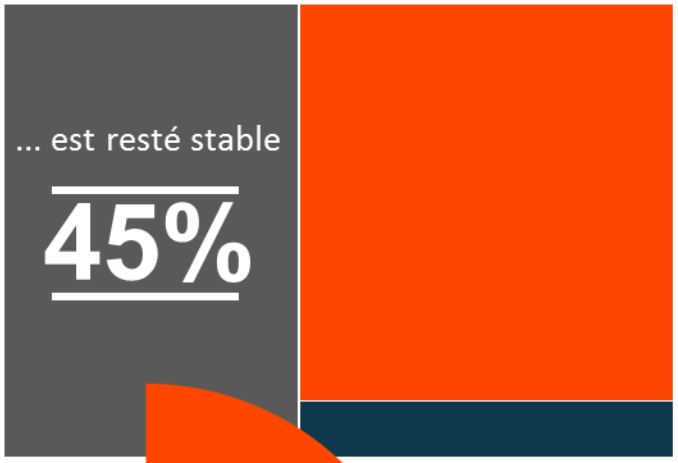
LE RÔLE DU RSSI SE LIMITE-T'IL À LA FOURNITURE DES MOYENS DE SÉCURISATION DU SYSTÈME D'INFORMATION ?

Baromètre 2018 du CESIN



Baromètre 2018 du CESIN

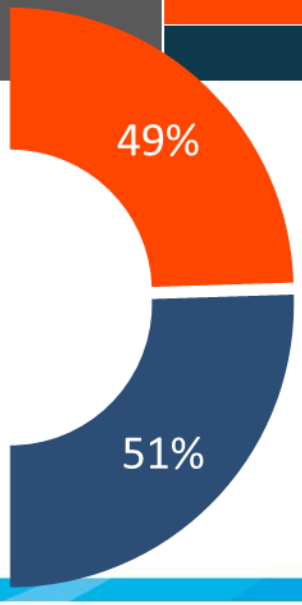
En un an, le nombre d'attaques...



... a augmenté
48%

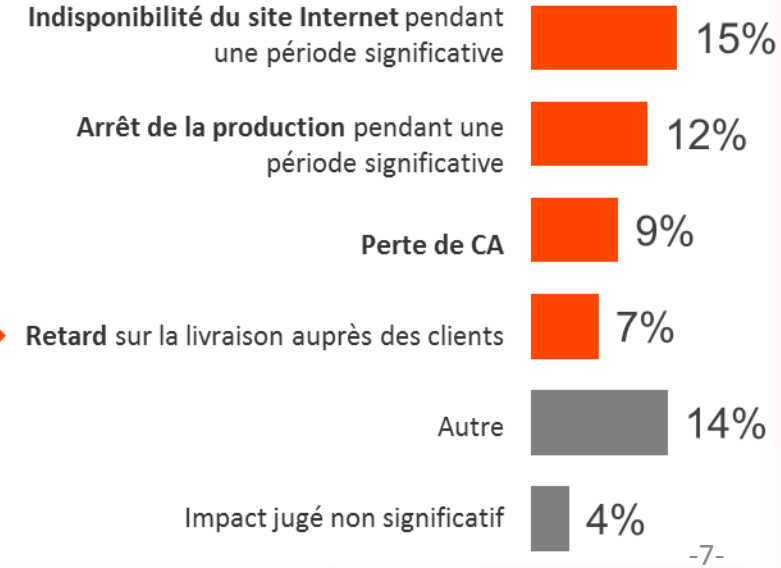
... a diminué
7%

79%
des entreprises ont constaté au moins une cyber-attaque



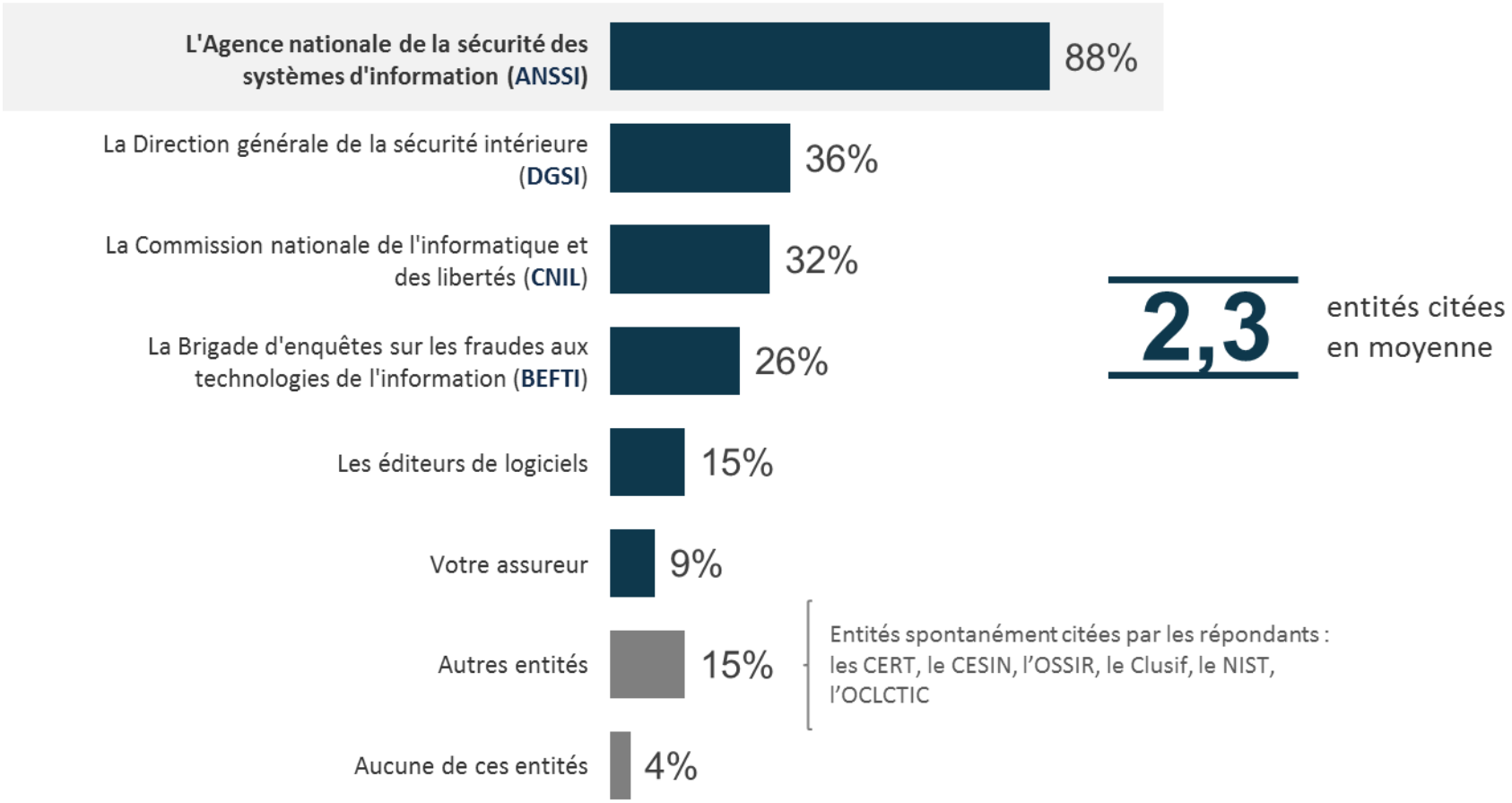
Impacts sur le business

Aucun impact sur le business



Baromètre 2018 du CESIN

Les RSSI s'informent auprès de tout un écosystème d'acteurs, l'ANSSI leur semblant le plus légitime



Baromètre 2018 du CESIN

Dans ce contexte, de plus en plus d'entreprises souscrivent une cyber-assurance

40% ↗

15%

22%

Baromètre 2018 du CESIN

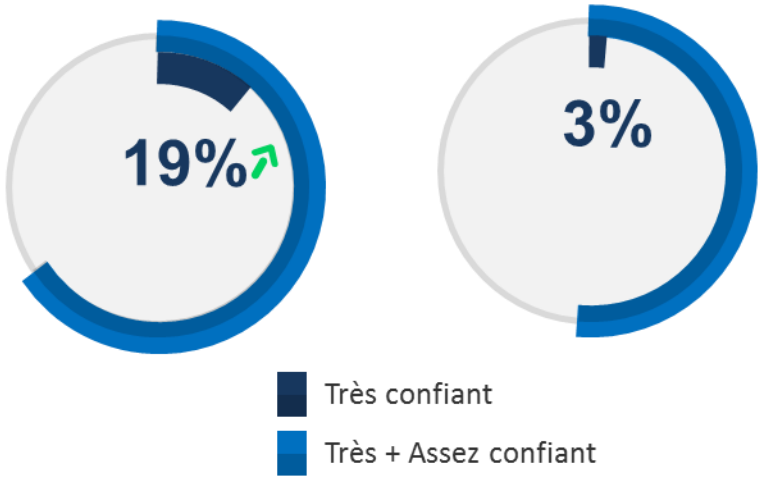
Pour l'avenir, une confiance dans la capacité à faire face aux cyber-risques réelle et en hausse

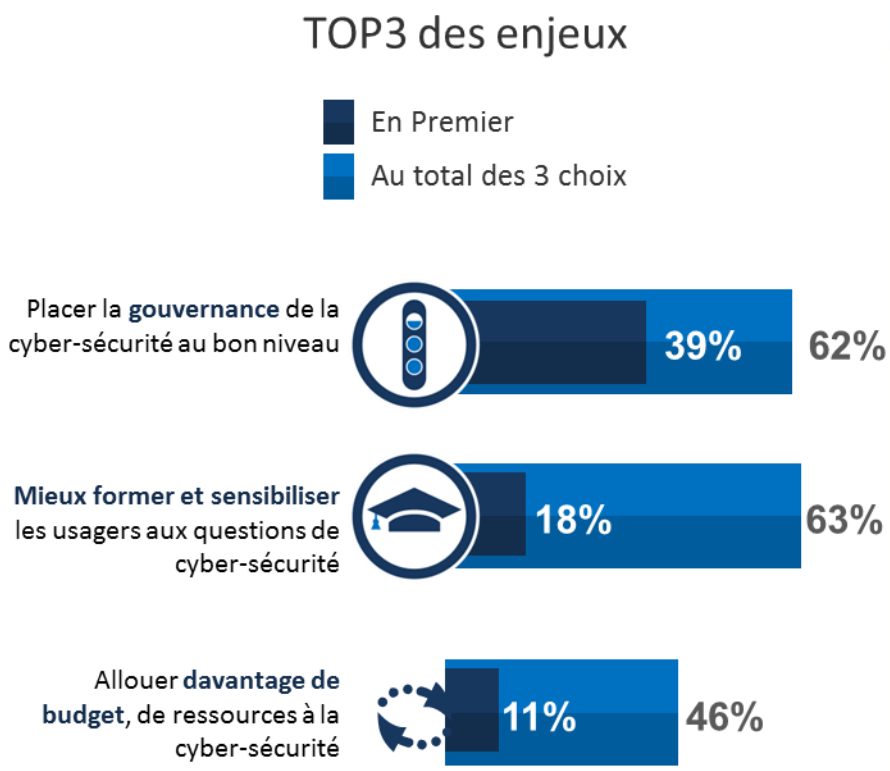
71%

La **prise en compte des enjeux** de la cyber-sécurité au sein du COMEX votre entreprise

63% ↗

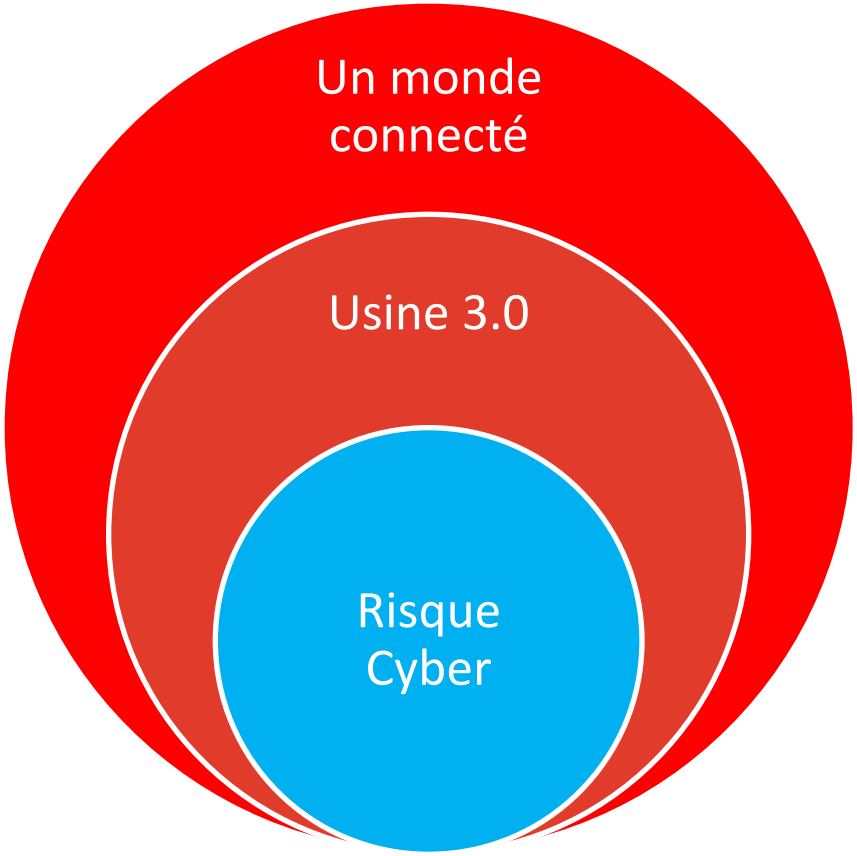
La **capacité** de votre entreprise à faire face aux cyber-risques





LA GOUVERNANCE DU RISQUE CYBER EST IL UN CRITÈRE DE SÉLECTION DES RISQUES ?

Une gouvernance Indispensable



« Tout sera Numérique »

RM = CEO

Une gouvernance Indispensable

- Effective
- Adaptée
- Pas suffisante

Une gouvernance
Co construite

Etats

Entreprises

Assureurs

Une gouvernance dans un cadre

- Législatif et règlementaire
- Certifications / Normes
- Connaissance du risque / Données

Une gouvernance marquée par la

CONFIANCE

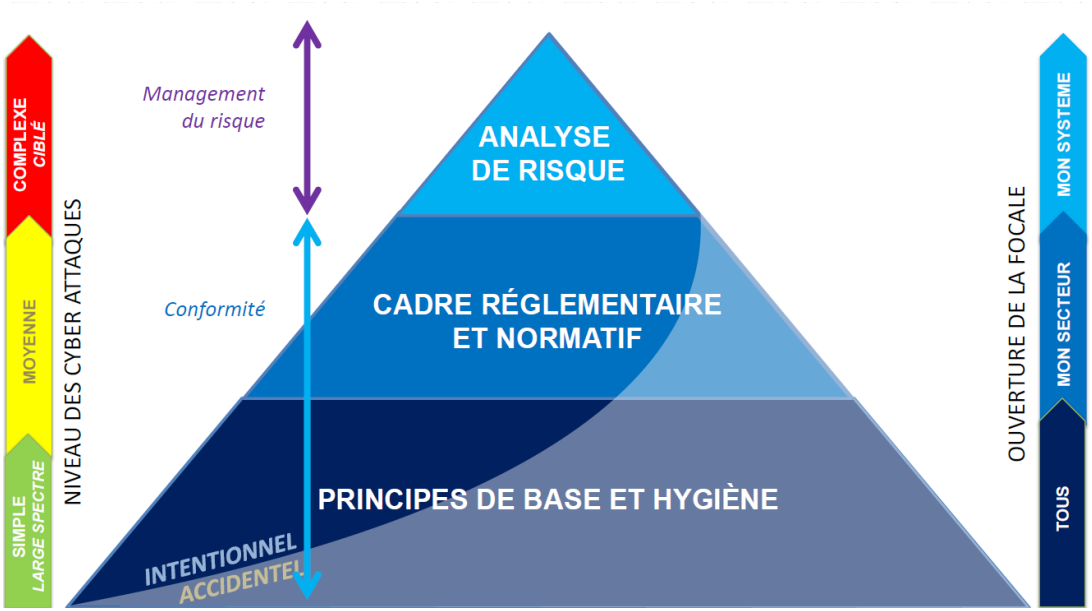
Une gouvernance co construite

DEMANDE  OFFRE

Au-delà de la gouvernance

LA COLONNE VERTÉBRALE DE LA DOCTRINE DE MANAGEMENT DES RISQUES CYBER DE L'ANSSI

La pyramide du management du risque cyber



Le corpus doctrinal de l'ANSSI est basé sur le concept de la pyramide : le management du risque est la résultante d'une approche visant à définir,

- en premier lieu, un socle de sécurité basé sur la **conformité à des bonnes pratiques générales** et des **règlementations particulières**, puis,
- en second lieu, à tester, renforcer et orienter ce socle de sécurité grâce à une **analyse de risque ciblée sur les risques intentionnels de haut niveau** qui menacent l'organisation.

Organisation pour une sécurité en profondeur