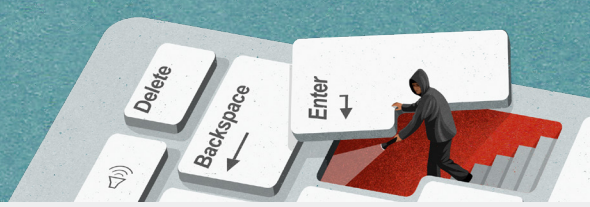


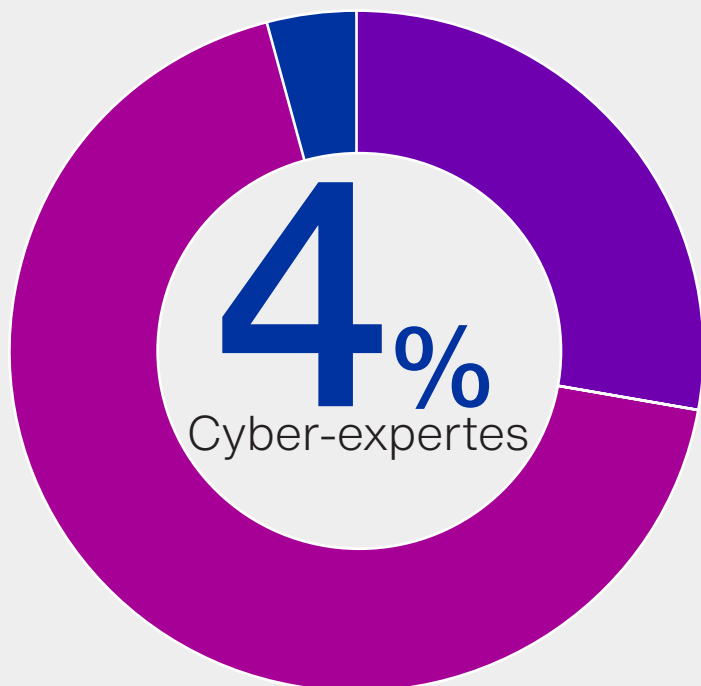
## QUE FONT LES ENTREPRISES EXPERTES?



Dans l'ensemble, les **notes d'évaluation des capacités de gestion des cyber-risques ont décliné de 2,6%**, avec une détérioration marquée de la gouvernance/assurance (fonction processus) et de la présence de salariés convenablement qualifiés et expérimentés (personnes). Des améliorations ont été constatées en matière d'outils et technologies (technologie).

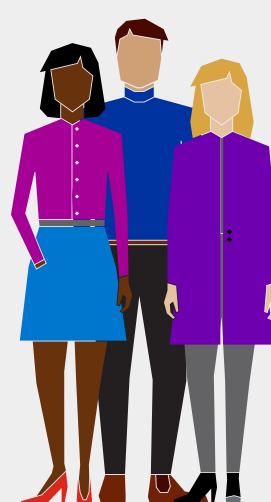


### Maturité



**28%**  
Cyber-novices

**68%**  
Cyber-intermédiaires



### Écart des dépenses



Sur l'ensemble des participants, les dépenses **moyennes** ont **progressé** de **60%** l'an passé pour s'établir à **4.8m€** soit une hausse de **250%** par rapport à 2019.

**5.0m€**  
Administration et organismes à but non lucratif

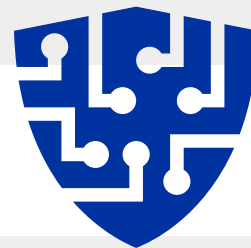
**8.8m€**  
Services financiers

**6.9m€**  
Pharmacie et santé

**30.7m€**  
Services aux entreprises

**6.8m€**  
Fabrication

### Heureusement, tout n'est pas uniquement une question d'argent



Principales mesures peu coûteuses mises en œuvre par les entreprises 'cyber-expertes':

- Élaborer un cadre formel de réponse en matière de cybersécurité. Elles ne l'élaborent pas au gré des attaques.
- Désigner une ou plusieurs personnes en charge de la cybersécurité avec des rôles bien définis.
- Élaborer un plan de réponse aux incidents et simuler régulièrement une cyber-attaque pour tester le plan de réponse aux incidents de l'entreprise – ce sont les mesures qui ont le plus progressé l'an dernier.
- Exiger l'appui du conseil d'administration/de la direction. La grande majorité (87%) font valoir que les hauts dirigeants ont une idée claire de la gestion de la cybersécurité (contre 69% dans l'ensemble du panel).

### Renforcer ses défenses après une attaque



Nous avons demandé aux **experts** comment ils avaient répondu suite à la suite des cyber-attaques subis:

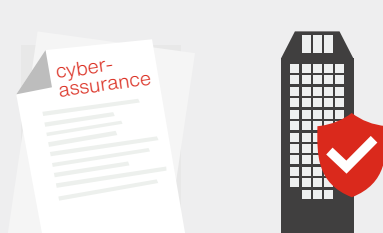
**41%**  
Ajout d'une nouvelle sécurité cyber et audit des systèmes en place;

**39%**  
renforcement des formations auprès des employés;

**39%**  
amélioration des préparations en cas de cyber-attaque;

### Des souscriptions d'assurance toujours en augmentation

**64%** des entreprises ont désormais souscrit une **cyber-assurance**, soit par le biais d'un contrat dédié, soit par le biais de garanties dans le cadre d'une autre police, contre **58%** il y a 2 ans.



| Souscription d'une cyber-assurance (%) |      |      |     |
|--|------|------|-----|
|  | 2021 | 2022 | +/- |
| Belgique                               | 58   | 59   | +1  |
| France                                 | 57   | 61   | +4  |
| Allemagne                              | 64   | 67   | +3  |
| Irlande                                | 64   | 69   | +5  |
| Pays-Bas                               | 55   | 58   | +3  |
| Espagne                                | 63   | 66   | +3  |
| Royaume-Uni                            | 61   | 62   | +1  |
| États-Unis                             | 65   | 65   | -   |

### Pourquoi souscrire une assurance?



Les **grandes entreprises** (1 000 salariés et plus) sont plus **préoccupées** par la **sécurité de leurs données** et craignent les contentieux avec leurs clients. Beaucoup d'entre elles ont également des obligations juridiques. Même si les **petites entreprises** craignent également les contentieux, elles voient en l'**assurance** un moyen de se **doter d'une expertise qu'elles n'ont pas**.

Je suis inquiet de la sécurité de mes données ou celles de mon client/de mon entreprise.

**31%**

Les polices d'assurance Cyber offrent une expertise additionnelle que je n'ai pas (par exemple: management de crise, IT Forensics).

**29%**

Cela m'inquiète car si mon organisation est attaquée, mes clients peuvent faire une réclamation auprès de mon entreprise.

**29%**

Avoir une assurance cyber est une obligation ou une exigence (GRDP, CCPA, ou tout autre obligation réglementaire).

**28%**

Mon organisation a des expériences passées d'incident cyber ou faille de sécurité.

**28%**

**Votre entreprise est-elle experte en matière de cybersécurité?**  
Pour en savoir plus sur l'évaluation de la maturité de votre entreprise par Hiscox ou pour la réaliser vous-même!  
[www.hiscoxgroup.com/cyber-maturity](http://www.hiscoxgroup.com/cyber-maturity)