flowlysis.

# CHIFFRER UN RISQUE EN EUROS

On remplace la couleur d'un risque par deux estimations : la chance qu'il arrive dans l'année, et ce qu'il coûterait, en fourchette. La perte évitée par une mesure se compare alors à son prix.

**AUSSI APPELÉ** quantification du risque, courbe de dépassement de perte **PRINCIPE QU'IL APPLIQUE** le risque a un propriétaire métier, fiche P-14

**SE PRÉPARE EN** une demi-journée d'entraînement des estimateurs **SE FAIT EN** une heure par scénario, dans un tableur **LEVIER PRINCIPAL** ROI

| CE QUE ÇA RAPPORTE | |
|---|---|
| Impact sur le TTM | Faible |
| Impact sur la qualité (FTR) | Faible |
| Impact sur l'Opex / Capex | Élevé |

| CE QUE ÇA COÛTE | |
|---|---|
| Coût d'implémentation | Faible |
| Difficulté d'implémentation | Moyen |
| Difficulté de maintien | Moyen |

Faible · Moyen · Élevé · N/A (sans objet)

## 1 Le problème auquel ça s'applique

Et ce qu'il vous coûte chaque année

### CE QUE VOUS VOYEZ DÉJÀ

- « Le CISO dit que c'est rouge. Je ne sais pas quoi arbitrer. »
- Deux risques sont rouges tous les deux. L'un coûterait 50 k€, l'autre 5 M€.
- La mesure passe d'un comité au suivant. Personne ne sait ce qu'elle rapporte.

### OÙ PART L'ARGENT

Une couleur ne se compare pas à un prix. Le budget va au risque le mieux plaidé. Une mesure rentable attend, une autre coûte plus qu'elle n'évite, et personne ne le voit.

### L'ORDRE DE GRANDEUR, À LA LOUCHE

*Comptez-le avec le CISO, sur les mesures du dernier budget.*

| COMBIEN DE FOIS / AN | | CE QUE ÇA COÛTE À CHAQUE FOIS | | PART QU'ON ÉVITE | | GAIN / AN |
|---|---|---|---|---|---|---|
| mesures de sécurité arbitrées en comité | × | budget annuel d'une mesure | × | mesures qui coûtent plus qu'elles n'évitent | = | **budget rendu ou réorienté** |

### QUAND ÇA NE SERT À RIEN

Quand un texte ou un contrat impose la mesure : il n'y a plus d'arbitrage. Ou quand elle coûte si peu qu'on la prend sans débat. Si personne ne sait ce que coûte une journée d'arrêt, commencez par là (fiche O-70).

## 2 Comment ça marche

La mécanique, en clair

### L'IDÉE EN UNE PHRASE

Une probabilité et une fourchette en euros, sans puis avec la mesure, donnent la perte évitée chaque année.

### LES GESTES, DANS L'ORDRE

1. Écrire le risque en une phrase : qui, par où, quelle perte.
2. Entraîner les estimateurs : des séries de dix questions à réponse connue, une fourchette à 90 % chacune. Un estimateur calibré en encadre neuf en moyenne.
3. Estimer la chance que l'événement arrive dans l'année, puis son coût en fourchette à 90 % : une chance sur vingt de chaque côté.
4. Perte annuelle attendue ≈ probabilité × (0,65 × bas + 0,35 × haut) : la perte typique reste près du bas.
5. Refaire l'estimation avec la mesure. La perte évitée se compare à son coût annuel.
6. Avec plusieurs risques, simuler dix mille années (Monte-Carlo) et lire la chance de dépasser le seuil du comité.

### CE QU'IL FAUT AVOIR SOUS LA MAIN

Le CISO, le propriétaire métier, les incidents déjà vécus.

### LE SIGNE QUE ÇA A MARCHÉ

Le comité tranche une mesure en euros, sans citer la couleur du risque.

## 3 Les pièges de l'implémentation

Ce qui fait rater, et ce qu'on fait à la place

**AU LANCEMENT — Un chiffre unique**
« L'impact, c'est 500 k€. » Le chiffre a l'air précis et cache ce qu'on ignore.
→ Une fourchette à 90 %, large si on sait peu.

**AU LANCEMENT — La catastrophe en borne haute**
L'estimateur met le pire imaginable en haut de la fourchette. La perte attendue gonfle.
→ Un haut surprenant, pas impossible : une chance sur vingt au-dessus.

**PENDANT — Des estimateurs jamais testés**
Les fourchettes sont étroites, et rien ne dit qu'elles encadrent le vrai.
→ Des séries de dix questions nouvelles, jusqu'à neuf sur dix en moyenne.

**PENDANT — Chiffrer sans comparer**
Le risque vaut 116 k€ par an. La mesure, elle, n'est pas chiffrée.
→ Deux estimations, sans et avec, plus le coût annuel de la mesure.

**DANS LA DURÉE — Des fourchettes figées**
Un incident est arrivé. L'estimation de l'an dernier reste au registre.
→ Revoir à la date de révision et après chaque incident (fiche P-14).

## 4 Exemple

Cas type du tertiaire, du constat au résultat

### LA SITUATION DE DÉPART

**L'OBJET**
L'accès à distance de 40 prestataires de maintenance au progiciel de gestion locative d'un bailleur social, par identifiant et mot de passe.

**CE QUI CLOCHE**
L'authentification forte des prestataires est reportée depuis deux budgets.

**CE QU'ILS REGARDAIENT AVANT**
Une matrice cinq sur cinq où ce risque partage la case rouge avec six autres.

**LES CHIFFRES DE DÉPART, HYPOTHÈSES DU CAS**

| | |
|---|---|
| **12 %** | de chances par an d'une intrusion par un compte de prestataire |
| **200 k€ à 2,4 M€** | son coût, fourchette à 90 % |
| **4 %** | de chances par an avec l'authentification forte, même coût s'il arrive |
| **30 k€** | coût annuel de la mesure, mise en place comprise |

### CE QU'ILS ONT FAIT

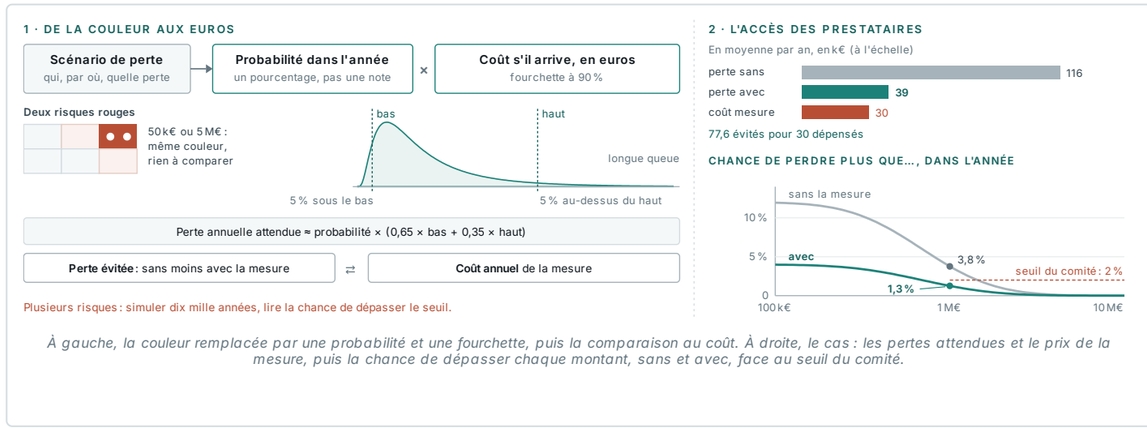
*Après le test de calibrage, le CISO a estimé la probabilité, la directrice de la gestion locative le coût total. Le comité a comparé la perte évitée au prix.*

| LE DÉCLENCHEUR | LE GESTE | CE QU'ILS ONT VU | LA DÉCISION |
|---|---|---|---|
| Troisième report en comité : « C'est rouge, mais tout est rouge. » | Deux estimations en fourchette, sans puis avec la mesure, dans un tableur. | Une perte attendue de 116 k€ par an sans la mesure, de 39 k€ avec. | Financer la mesure. Seuil du comité : au plus 2 % de chances par an de perdre plus de 1 M€. |

### CE QUE ÇA A DONNÉ

| | |
|---|---|
| **116 → 39 k€** | Coût moyen s'il arrive ≈ 0,65 × 200 + 0,35 × 2 400 = 970 k€ ; par an, 12 % × 970 = 116 k€. Avec la mesure, 4 % × 970 = 39 k€. |
| **≈ 78 k€ évités** | En moyenne par an : (12 % − 4 %) × 970 = 77,6 k€, pour 30 k€ de coût. 2,6 € évités par euro dépensé, 47,6 k€ de gain net. |
| **3,8 → 1,3 %** | Ce risque seul, plus de 1 M€ perdus dans l'année : 12 % × 31,4 % = 3,8 %, puis 4 % × 31,4 % = 1,3 %, sous le seuil de 2 %. Le tableur donne les 31,4 % : la chance qu'une intrusion coûte plus de 1 M€. |

Refaites-le avec le risque rouge le plus discuté chez vous : une probabilité et une fourchette, sans puis avec la mesure. Posez la perte évitée à côté du prix, sur l'A3 de décision (fiche O-11).




*À gauche, la couleur remplacée par une probabilité et une fourchette, puis la comparaison au coût. À droite, le cas : les pertes attendues et le prix de la mesure, puis la chance de dépasser chaque montant, sans et avec, face au seuil du comité.*



*L'exemple est un cas type, reconstruit à partir de situations courantes du tertiaire. Aucune situation client n'y est identifiable.*