Que retenir du schéma ?

Comment l’exploiter ?

1. Définir sa stratégie

- Répondre aux questions:
  - Que veut-on faire ?
  - Quels sont les grands objectifs ?
  - Quels moyens peut-on y consacrer ?
- Durée de vie typique: 4-5 ans (pas toujours adaptée au numérique…).
- Fortement influencée par le niveau actuel de maturité cyber de l’entreprise.

Deux cas possibles (de façon un peu caricaturale)

<u>Société pas mature en cybersec</u>

→ stratégie = sortir la tête de l'eau / sortir de la zone d'humiliation,

= priorité à la mise en œuvre des mesures de securité de base.

<u>Société déjà mature en cybersec</u>

→ stratégie = pérenniser la sécurité acquise,

= généralement en formalisant (via des écrits) les processus (ce que l'on fait).

2. Définir sa politique

- Répondre aux questions:
  - Comment fait-on ? Concrètement… pour atteindre les objectifs de la stratégie.
  - Des actions donc mais qui seront idéalement documentées… (*).
- Durée de vie typique // durée de vie de la stratégie.
- Ici aussi, deux cas sont possibles selon la maturité.

(*) Le terme politique de sécurité désigne à la fois les actions menées et le (ou les) document(s) décrivant ces actions.

Société pas mature en cybersec

→ politique = mettre en œuvre rapidement des mesures de sécurité de base en se basant sur ce que préconisent des référentiels bien établis dans le domaine (p.ex. guide d'hygiène informatique ANSSI en 42 mesures, CIS controls,…)
https://ccb.belgium.be/fr/cyberfundamentals-framework

Société déjà mature en cybersec

→ politique = pérenniser la sécurité acquise en formalisant les processus au travers du monde des normes et des certifications (p.ex. ISO 27001).
La « philosophie » généralement utilisée est de type « modèle PDCA »: Plan – Do – Check – Act.

3. Procédures et documents techniques

- Viennent compléter la politique et répondent à des questions plus pointues:
  - Qui fait quoi ?
  - Quand ?
  - Avec quel(s) moyen technique(s) ?
  - Selon quelle(s) méthode(s) ?
  - …

Au cœur de la démarche: la gestion du risque

- La gestion du risque devrait toujours servir de boussole pour définir les actions prioritaires (quelque soit le niveau de maturité).
- Elle est même au cœur des pratiques « avancées » de type ISO27000.
- Elle se concrétise typiquement par une matrice des risques et un plan d’actions associé.

Gestion des risques

Démarche simplifiée

1. Identifier les biens, les actifs,…les « trucs » à protéger

- Peu importe le vocabulaire, il faut identifier ce qui a de la valeur pour votre métier: ressources, services, information,…
- Cela devrait être facilité par une bonne cartographie du SI:

https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation

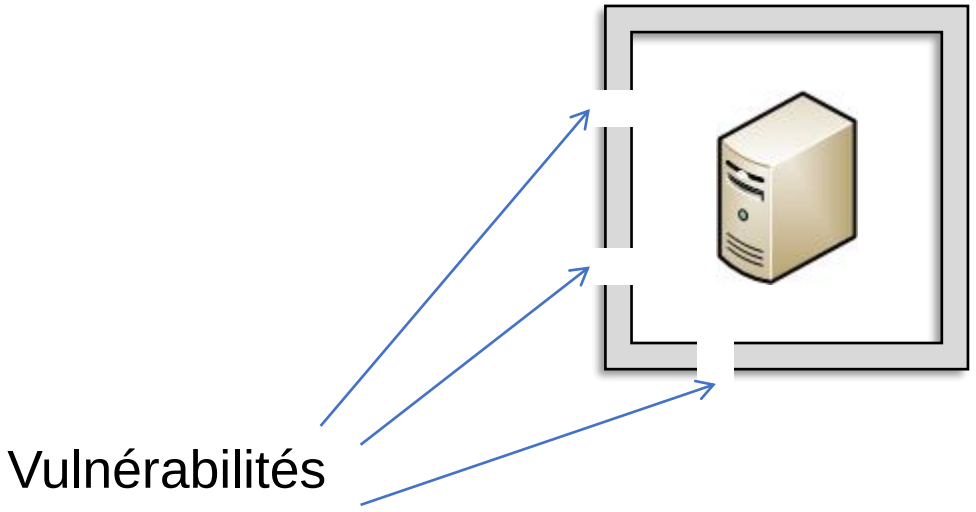
- Dans la pratique, peu d'organisation dispose de cette documentation… ☹

2. Définir les risques

- Le **risque** provient de la rencontre d'une **vulnérabilité** et d'une **menace**. Nous devons donc nous y intéresser.

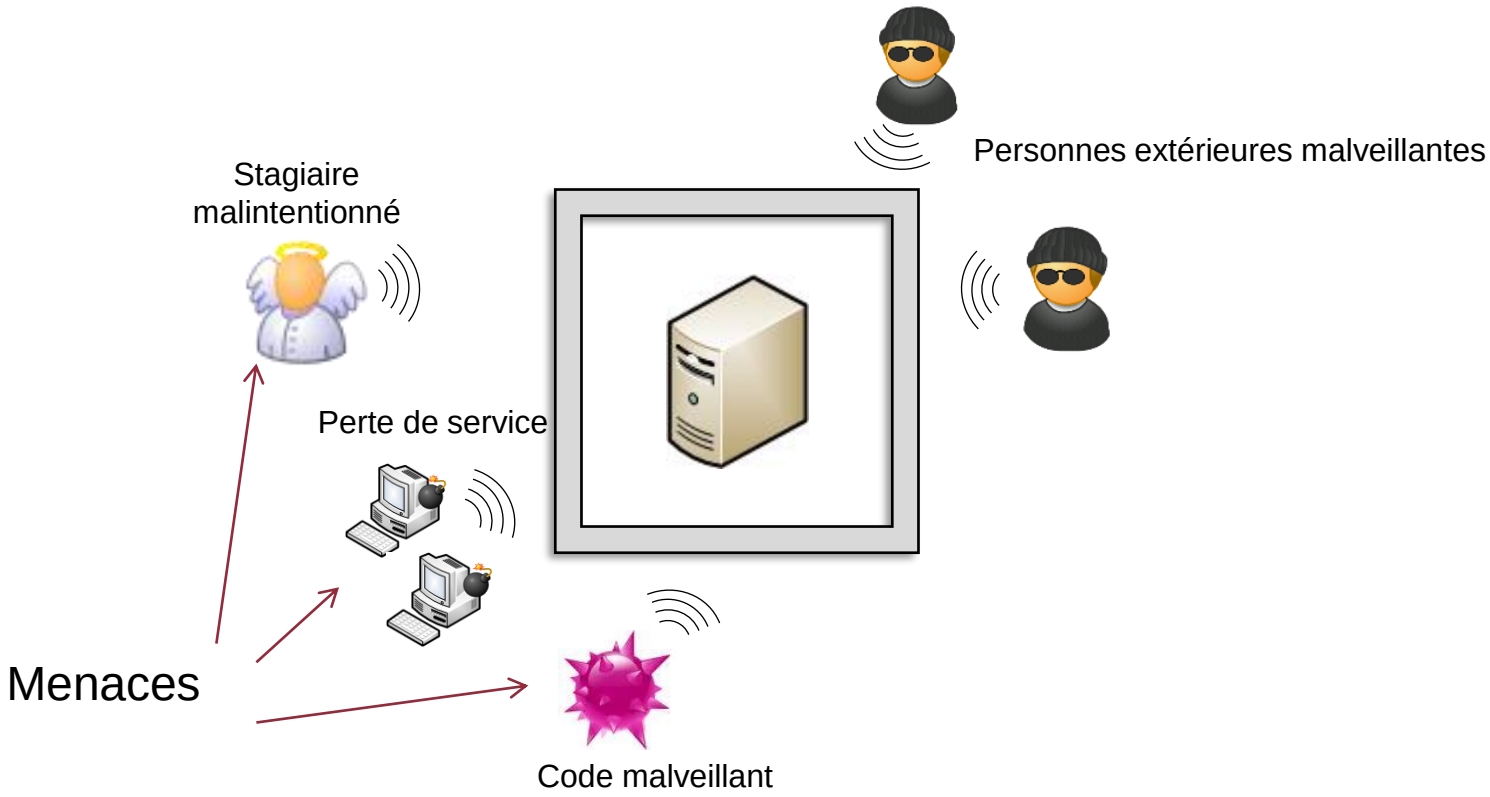
Notion de « Vulnérabilité »

- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



Notion de « Menace »

- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



Notion de « risque »

RISQUE = MENACE x VULNERABILITE

→ beaucoup de menaces mais peu de vulnérabilités = un risque modéré.

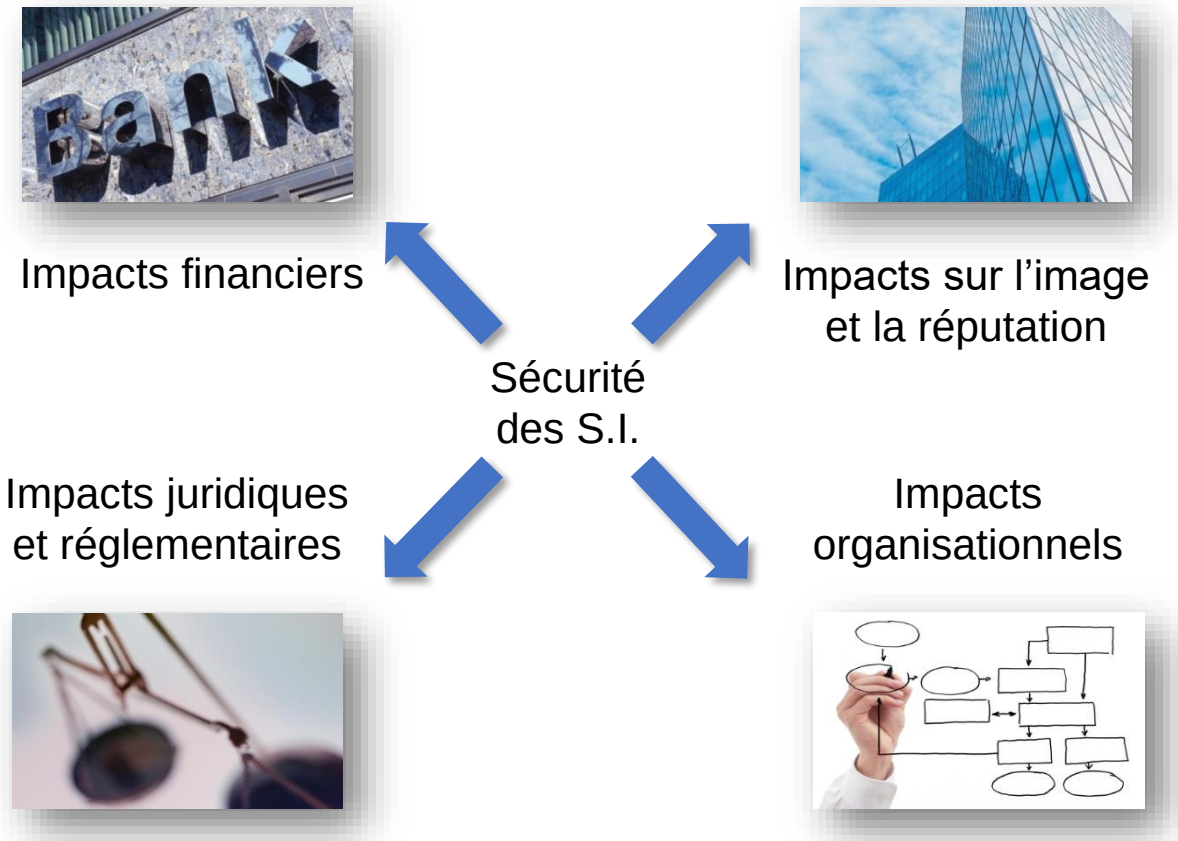
→ beaucoup de vulnérabilités mais peu de menaces = un risque modéré

→ Beaucoup de menaces et beaucoup de vulnérabilités = un risque élevé !!!

Le risque 0 n'existe pas mais c'est vers quoi il faut tendre. Il faut faire des choix et définir des priorités.

3. Identifier impacts

- Identifier les impacts engendrés par la concrétisation du risque.
- Répondre à la question: si l'évènement redouté survient, qu'arrive-t-il ?



4. Catégoriser les risques

- La formule Vulnérabilité(s) x Menace(s) définit plutôt la ***probabilité du risque***.
- Dans un second temps, le risque pourra être qualifié de grand ou petit en fonction des ***impacts***.

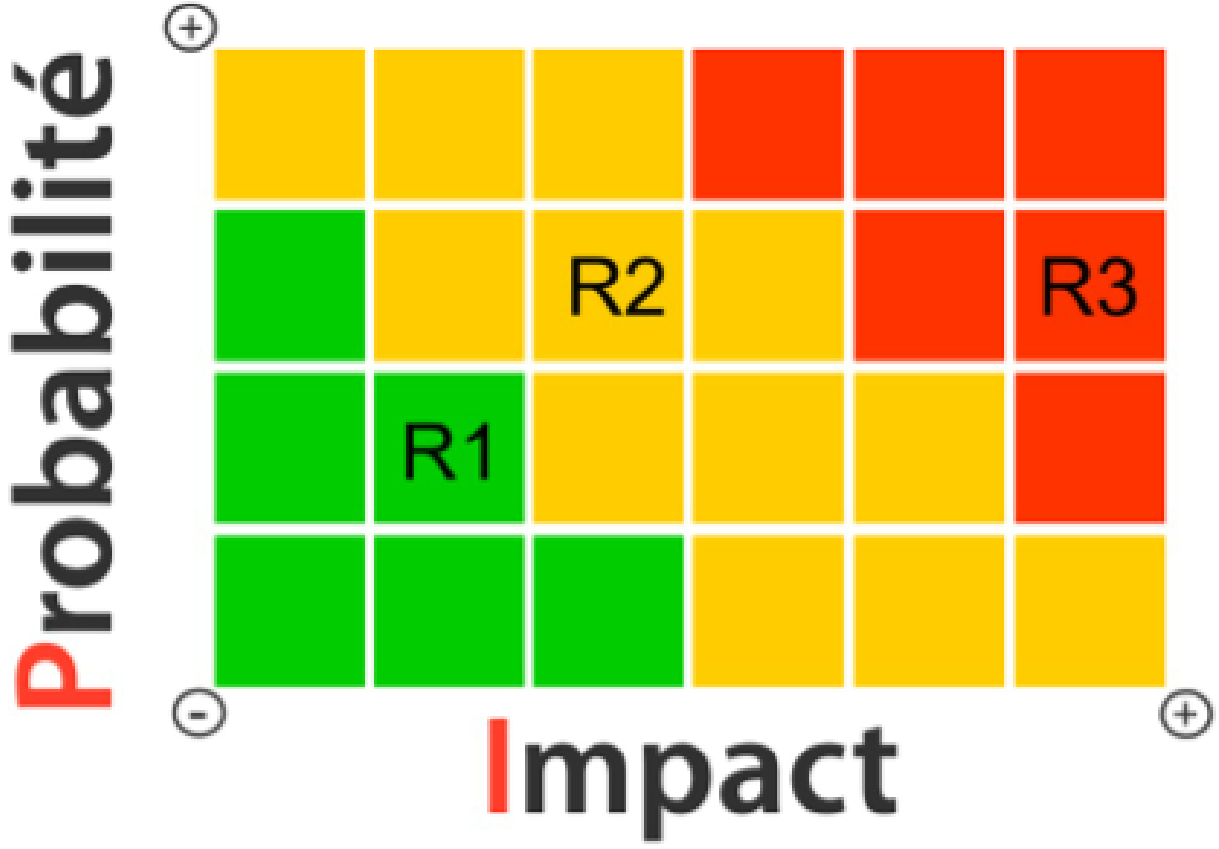
En terme de sécurité, on arrive alors à une nouvelle formule intéressante:

Criticité (ou gravité) du risque = Probabilité du risque x impacts associés au risque

→La priorité sera mise sur les actions/mesures qui réduisent les risques les plus critiques; ç-à-d les plus probables et ceux qui aboutiraient à des impacts majeurs.

→Graphiquement, cela s'illustre dans la **matrice des risques.**

5. Construire la matrice



6. Le plan d’action

- En fonction de la position du risque dans la matrice, on prend les décisions qui s’imposent:
  - On tente de réduire le risque (rouge → orange ou vert) en appliquant des mesures de sécurité.
  - On refuse le risque en ne faisant pas l’action associée (p.ex. refuser d’externaliser une partie de son SI dans certains pays).
  - On accepte le risque (p.ex. ceux dans la zone verte).
  - On partage le risque (via une assurance ou un partenariat).
- <!> PRIORITE AUX TRAITEMENTS DES RISQUES DANS LA ZONE ROUGE <!>