Parallèle entre l'outil quantificateur du risque cyber et la méthode FAIR

Table des matières

Introduction à la méthode FAIR (Factor Analysis of Information Risk)

Source : Méthode d'analyse FAIR : une révolution pour l'analyse du risque cyber ? (c-risk.com)

Cette méthode propose à la fois une **analyse qualitative** et **quantitative** du risque cyber. Elle analyse le risque de façon probabiliste.

Cette approche de l'analyse du risque cyber propose, dans un premier temps, une taxonomie des facteurs distincts qui constituent le risque. Il s'agit d'un recueil de définitions, qui permet d'utiliser certaines notions sans les confondre : risque, menace, danger, actif, contrôle, audit… La Méthode d'analyse FAIR explique comment ces facteurs sont liées entre eux, pour aboutir à des pistes de réflexions utiles pour l'entreprise.

Le standard FAIR™ propose une méthodologie pour décomposer le risque en facteurs distincts qui peuvent être mesurés puis pour utiliser les statistiques et les probabilités afin d'estimer quantitativement le risque. Objectif : permettre d'analyser des risques complexes, identifier les données nécessaires à la quantification et comprendre les interdépendances entre facteurs constitutifs du risque.

Cette méthode permet donc de répondre à la question du coût du sinistre et d'y ajouter une notion business.

Schématiquement la méthode FAIR :

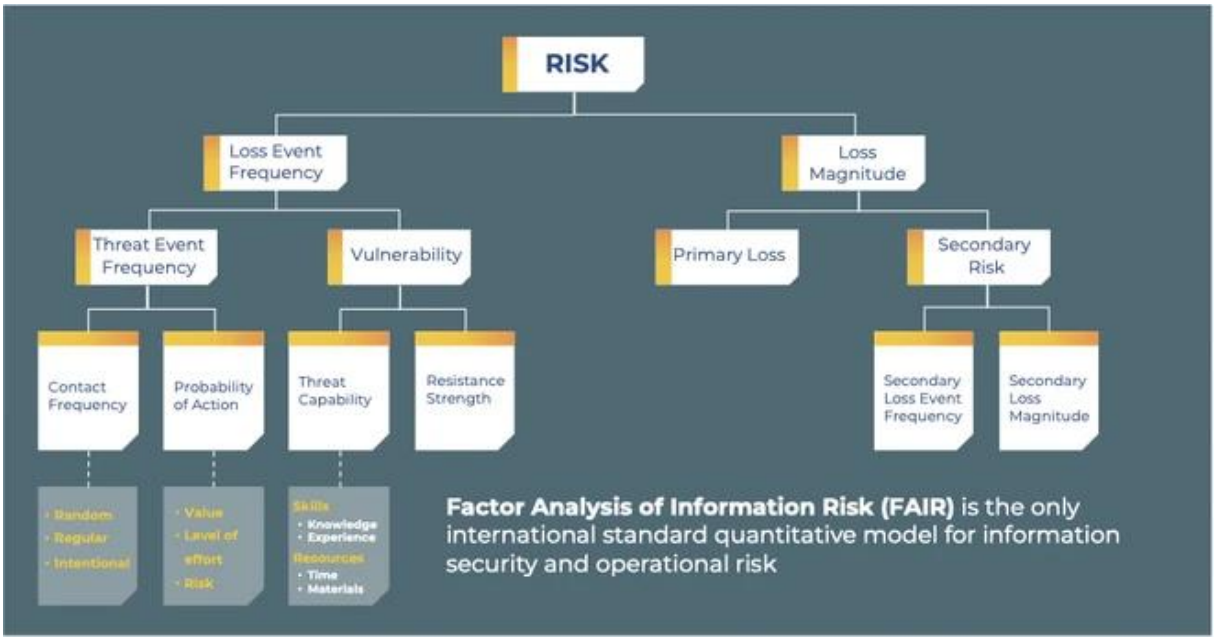

Figure 1 Schéma de la méthode FAIR

La méthode FAIR divise donc le risque en deux sous catégories :

- La fréquence des sinistres
- L'ampleur des sinistres

Plus simplement, RISQUE = COÛTS x FREQUENCE.

Outil modulable de quantification du risque cyber

L'outil créé se structure suivant la méthode FAIR, en 3 gros blocs : fréquence, impact et risque. Voici le schéma global :

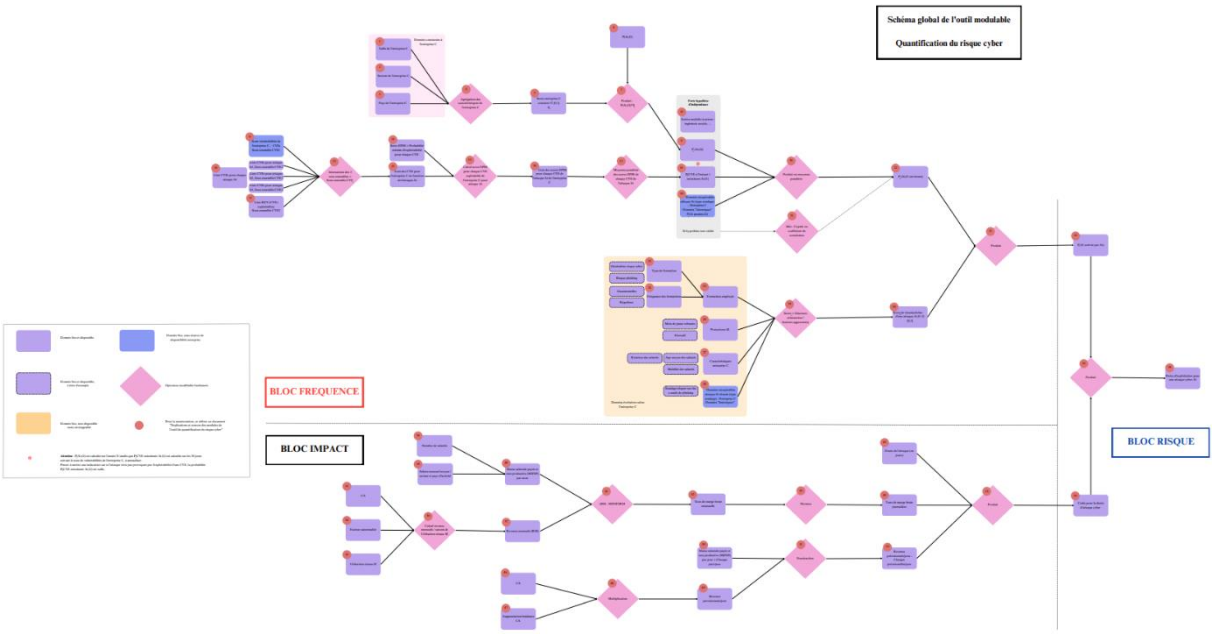

Figure 2 Schéma de l'outil

Le schéma est complexe et illisible sur la Figure du dessus. Pour faciliter sa compréhension, un autre document a été réalisé afin de l'expliquer en détails et d'indiquer l'ensemble des ressources qui ont permis sa réalisation.

Le principal but de ce document réside, en appui avec le document explicatif du schéma de l'outil, à faire le parallèle entre la méthode FAIR et l'outil.

Bloc fréquence

➔ **« Loss Event Frequency » de la méthode FAIR**

Survenance de l'attaque

- **$P(A_i,G)*S_c = P_c(A_i,G)$** :
  - **$P(A_i,G)$:** probabilité « générale » que l'attaque déclenche la garantie pertes d'exploitation.

Cette probabilité correspond à la partie « **Threat Event Frequency** » et la sous partie « **Contact frequency** ». Un module sur des données historiques appartiendrait aussi à cette sous partie.

- S_c : score qui prend en compte les caractéristiques de l'entreprise.
  Ce score correspond à la partie « **Vulnerability** » et la sous partie « **Threat Capability** ».

- **P_c(CVE à l'instant t entraînent A_i, G)** : Cette probabilité prend en compte le nombre de CVE que l'entreprise a à l'instant t sur son scan de réseau, puis correspond à une moyenne du score EPSS de ces CVE. Le score EPSS reflète la criticité de la CVE.
  Cette probabilité correspond à la partie « **Threat Event Frequency** » et la sous partie « **Probability of Action** ».

Réussite de l'attaque

Score de réussite de l'attaque

- **Formation** des employés : correspond à la partie « **Vulnerability** » et la sous partie « **Threat Capability, Skills** ».
- **Protections SI** : correspond à la partie « **Vulnerability** » et la sous partie « **Threat Capability, Ressources** ».

  Caractéristiques entreprise : correspond à la partie « **Vulnerability** » et la sous partie « **Threat Capability, Skills** ». De la même façon, un module sur des données historiques appartiendrait aussi à cette sous partie.

Bloc impact

➔ **« Loss magnitude » de la méthode FAIR**

L'outil créé ne tient compte que des pertes directes (« **Primary loss** ») pour le bloc impact.

Nous ne faisons pas intervenir la partie **Secondary risk** puisque ce sont d'autres garanties qui sont activées dans ce cas.