Analyse de risque quantitative en Sécurité

Franck Jeannot, *Montreal, Octobre 2016, H222, v1.1*

L' approche classique financière de mesure de ROI (Return On Investment) n'est pas particulièrement appropriée en sécurité [1] pour mesurer les initiatives de sécurité. La sécurité n'est généralement pas un investissement qui résulte en un profit mais plutôt la prévention d'une perte. La méthode ROSI (Return On Security Investment) va permettre de calculer quelle perte est éliminée grâce à l'investissement.

ROSI

Les objectifs sont de **déterminer la valeur de la protection** et de **prioriser les investissements** sur les mesures de protection qui ont la plus grande valeur.
On considère six éléments de calcul :

- Valeur de l'actif
- Facteur d'exposition
- Expectative de perte individuelle
- Taux d'occurrence annuelle
- Expectative de perte annualisée
- Coût de la mesure de protection

ROSI : définitions

Valeur de l'actif [VA] ($) : La valeur estimée ou son coût de remplacement.
Facteur d'exposition [FE] (%) : Pourcentage de la valeur de l'actif qui serait détruit advenant la matérialisation d'une menace spécifique.
Expectative de perte individuelle [EPI] ($) : Montant en dollars assigné à un événement donné qui représente la perte potentielle d'une organisation si une menace spécifique se matérialisait.

$$\mathbf{E}PI = VA * FE$$

Taux d'occurrence annuelle [TOA] : Fréquence estimée de matérialisation d'une menace spécifique au cours d'une période d'un an.
Expectative de perte annualisée [EPA] : Montant de la perte financière annuelle estimée relatif à un actif donné, résultant d'une menace spécifique.
Coût de la mesure de protection [CM] : Montant en dollars représentant l'investissement requis pour la mise en place et le maintien de la mesure.

$$\mathbf{E}PA = EPI * TOA$$

La **valeur d'une mesure [VM]** de protection est son économie potentielle.
[VM] = Expectative de perte annualisée avant l'implantation de cette mesure
- (expectative de perte annualisée après l'implantation de cette mesure)
- (coût de la mesure)

$$\mathbf{V}M = EPA_{avant} - EPA_{apres} - CM$$

[English]
Single Loss Expectancy (SLE) = Asset Value (AV) X Exposure Factor (EF)
Annual Loss expectancy (ALE) = SLE X Annualized Rate of Occurrence (ARO)

Références

[1] ENISA. Gestion des ressources informationnelles. https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport. 2012.

[2] S. Harris. *CISSP All-in-One Exam Guide, 6th Edition*. All-in-One. McGraw-Hill Education, 2012. ISBN : 9780071781732. URL : https://books.google.ca/books?id=vBK2RE_h0EUC.

[3] HEC. 30-715-12 - Gouvernance et gestion des risques. 2016.