La méthode EBIOS appliquée au risque de sécurité physique

Club EBIOS – séance du 19 Janvier 2010
Denis MANGIN & François ZAMORA– Groupe France Telecom-Orange
Sylvain CONCHON – Conix Security

Agenda

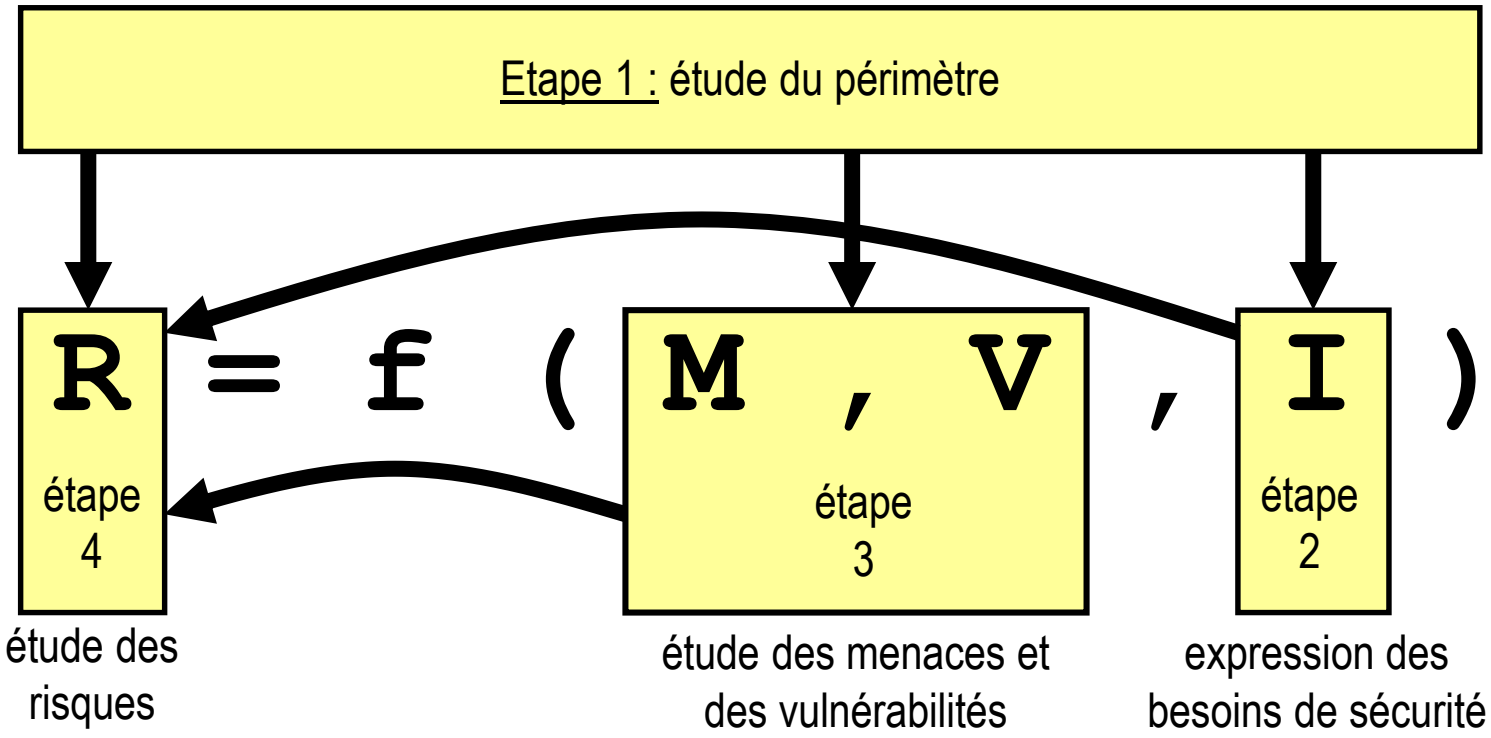
- Objectifs
- Rappels et travaux préalables
- Phase 1 : étude du périmètre
- Phase 2 : expression des besoins de sécurité
- Phase 3 : étude des menaces et des vulnérabilités
- Etude de cas
- Conclusion

Objectifs

- L'utilisation d'un cadre de référence analytique (EBIOS) vise :
  - > à tendre vers l'exhaustivité dans l'identification des risques / des impacts
  - > à faciliter le travail de l'auditeur
  - > à faciliter la restitution par le risque (vs. par le constat d'audit)
  - > à contribuer à la mise en œuvre d'un système de management de la sécurité physique

- Moyens :
  - > un savoir-faire méthodologique EBIOS
  - > une expertise de sécurité physique

Définition générale du risque et méthodologie EBIOS



Un préalable indispensable : expliciter les vocabulaires et les notions associées au risque 1/2

- Définition d'un scenario de risque :
  - > Une menace utilise une ou plusieurs vulnérabilité(s) portée par une ou plusieurs entité(s) pour porter atteinte à un ou plusieurs critère(s) de sécurité sur un ou plusieurs élément(s) essentiel(s)
  - > Une menace utilise une ou plusieurs vulnérabilité(s) portée par une ou plusieurs cible(s) pour porter atteinte à un ou plusieurs critère(s) de sécurité sur un ou plusieurs objet(s) de risque

- Points particuliers :
  - > Un élément essentiel est parfois une entité
  - > Un objet de risque est souvent une cible
  - > Les notions de sécurité et de sûreté sont réunies dans la sécurité de l'information

Un préalable indispensable : expliciter les vocabulaires et les notions associées au risque 2/2

Sécurité de l'information	➔	Sécurité physique
Risque brut	➔	Risque
		Risque (net) non pondéré
Risque net	➔	Risque (net) pondéré
Risque résiduel	➔	Risque résiduel
		Risque (net) acceptable

Les concepts de risques bruts et nets sont implicites dans la norme ISO 27001, mais exprimés indirectement à la clause 4.2.1j2

Le « client » des recherches est la sécurité physique : on utilise le vocabulaire de la sécurité physique dans la suite des travaux exposés

Phase 1 : étude du périmètre
Objets de risque

- Pour la sécurité de l'information
  - > informations essentielles
  - > fonctions essentielles

- Pour la sécurité physique
  - > personne
  - > flux
  - > bien matériel
  - > bien immatériel

- Pour mémoire :
  - > personne : l'impact généralement le plus élevé (attention néanmoins au recouvrement avec les risques HST)
  - > flux : 5 types de flux existent (d'énergie, de matière, d'information, financier, humain)
  - > bien matériel : inclut à la fois les notions de biens « meubles » et biens « immeubles »
  - > bien immatériel : inclut la notion d'« information » au sens de la sécurité de l'information

Phase 1 : étude du périmètre
Cibles

- Pour la sécurité de l'information
  - > entités EBIOS

- Pour la sécurité physique
  - > Travaux à effectuer :
    - > Identification de cibles et de catégories de cibles
    - > Mise en correspondance de triplets cible / menace / vulnérabilité
  - > Sources possibles :
    - > Base de connaissance EBIOS
    - > Base de connaissance CNPP
    - > Déduction à partir de vulnérabilités

Phase 2 : expression des besoins de sécurité
Critères

- Pour la sécurité de l'information
  - > disponibilité
  - > intégrité
  - > confidentialité
  - > autres critères possibles (souvent composites) :
    - – imputabilité
    - – conformité
    - – etc.

- Pour la sécurité physique
  - > disponibilité
  - > intégrité
  - > confidentialité
  - > conformité

- Pour mémoire :
  - > intégrité physique de la personne : intégrité au sens propre de son utilisation
  - > intégrité morale de la personne : c'est un critère à part entière
  - > conformité : à des référentiels juridiques (dont code du travail), contractuels, normatifs, internes,...
  - > confidentialité : concerne la notion de localisation des flux, es personnes et des biens matériels

Phase 2 : expression des besoins de sécurité
Echelle de besoins de sécurité

- Pour la sécurité de l'information
  - > Approche par le besoin de sécurité : démarche analytique basée sur le couple critère / élément essentiel
  - > Le besoin de sécurité porte sur l'atteinte à un critère de sécurité appliqué à l'élément essentiel

- Pour la sécurité physique
  - > Approche par le niveau d'impact : démarche analytique basée sur le triplet critère / objet de risque / type d'impact
  - > Le niveau d'impact porte sur le type d'impact de l'atteinte à un critère de sécurité appliqué à un objet de risque

Retour d'expérience de l'expert sécurité physique
Besoin de sécurité vs. Niveau d'impact

- Pour la sécurité de l'information
  - > Echelle de besoin de sécurité pour la confidentialité d'une information
    - – Niveau 4 : diffusion à une personne donnée identifiée
    - – Niveau 3 : diffusion à une groupe de personnes identifié
    - – Niveau 2 : diffusion au sein de la société uniquement
    - – Niveau 1 : diffusion interne ou externe libre

- Pour la sécurité physique
  - > Echelle de besoin de sécurité pour l'intégrité d'une personne
    - – Niveau 4 : la personne doit être à son poste en bonne santé
    - – Niveau 3 : la personne doit être à son poste
    - – Niveau 2 : la personne doit être à son poste un jour sur deux
    - – Niveau 1 : la personne doit être à son poste un jour par semaine

- L'impact du risque portant atteinte à la confidentialité prend la valeur du besoin de sécurité de l'information concernée (et c'est un raccourci, assumé ou non)

- Dans le cas d'un risque avéré causant un décès d'une personne de niveau 2, comment justifier d'un risque avec un impact le plus bas ?

Phase 2 : expression des besoins de sécurité
Approche par le niveau d'impact

		type d'impact			
		Financier	Personne	Conformité	Juridique
niveau d'impact	1	Quasi nul Perte financière négligeable	Quasi nul ITT d'un jour ou moins	Quasi nul Ecart de conformité	Quasi nul Arrangement à l'amiable
	2	Sensible Perte financière inférieure à 1 % des revenus	Sensible ITT inférieure à 8 jours	Sensible Non-conformité mineure	Sensible Amende
	3	Critique Perte financière comprise entre 1 et 5 % des revenus	Critique ITT supérieure à 8 jours	Critique Non-conformité majeure	Critique Responsabilité civile ou pénale avec un risque faible de condamnation
	4	Vital Perte financière supérieure à 5 % des revenus	Vital Décès ou invalidité	Vital Sans objet	Vital Responsabilité civile ou pénale avec un risque important de condamnation

Phase 3 : étude des menaces et des vulnérabilités
Base de connaissance de menaces

- Travaux effectués sur la base de connaissance CNPP
- Travaux à mener :
  - > Viser la complétude de la base de connaissance
  - > Identifier les triplets menaces, critères, objets de risque

Phase 3 : étude des menaces et des vulnérabilités
Base de connaissance de vulnérabilités

- Travaux effectués sur la base d'un référentiel interne FT
- Travaux à mener :
  - > Viser la complétude de la base de connaissance
  - > Associer chaque vulnérabilité à une (ou plusieurs) menaces
  - > Associer chaque vulnérabilité à une (ou plusieurs) cibles

Etude de cas (partielle) : synthèse des résultats
Phase d'analyse 1/2

- Cibles identifiées :
  - > Immeuble
  - > Pylône
  - > Paratonnerre
  - > Détecteur incendie
  - > Alimentation énergie
  - > Climatisation
  - > Dossier déclaration ICPE
  - > Déchets

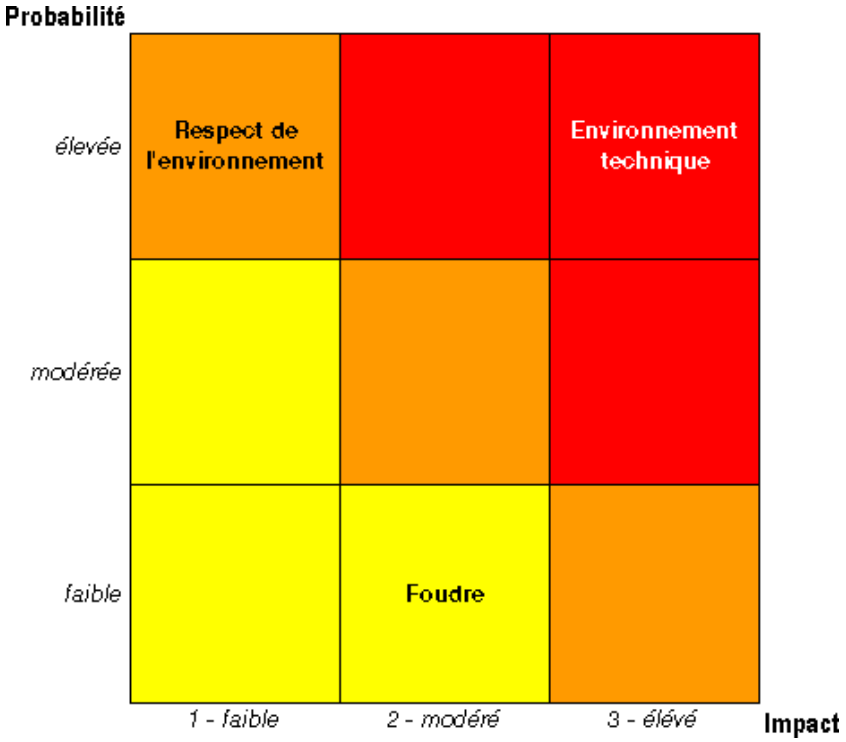
- Liste menaces manquantes (source : base CNPP) :
  - > Perte de service essentiel
  - > Saturation de service essentiel
  - > Non-respect environnement
  - > Pollution
  - > Contamination

Etude de cas (partielle) : synthèse des résultats
Phase d'analyse 2/2

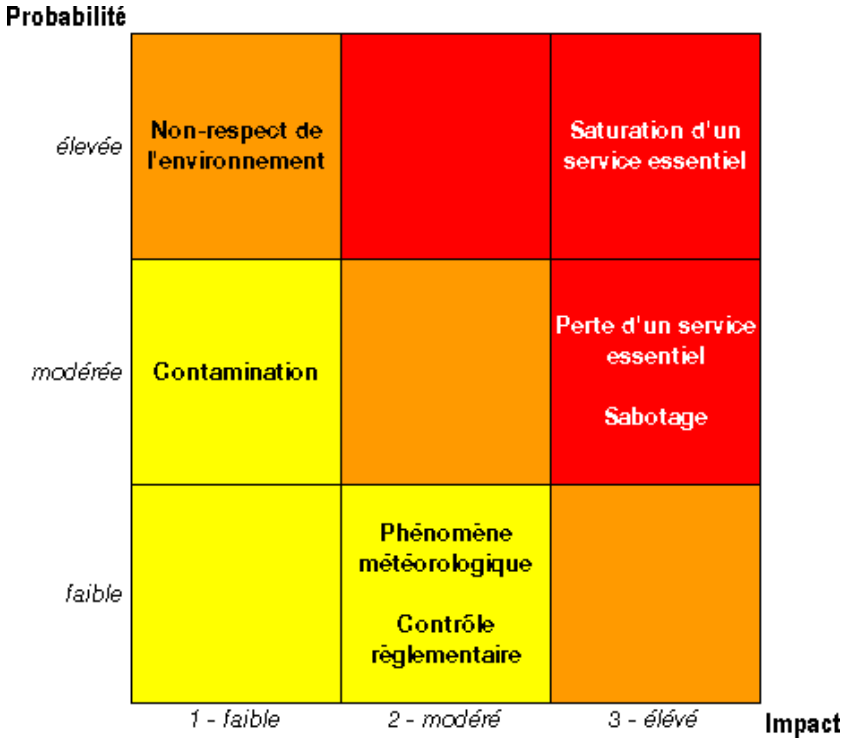
- Réels bénéfices venant du caractère analytique de la méthodologie
  - > Garantie de cohérence de l'appréciation issue de l'audit terrain :
    - – Causes différentes + Effets identiques ➔ Impacts identiques
    - – Exemple de bénéfice : assurance de la cohérence du positionnement des risques sur la matrice
  - > Garantie de complétude de l'appréciation issue de l'audit terrain :
    - – Causes identiques + Effets différents ➔ Impacts différents
    - – Exemple de bénéfice : traitement immédiat des risques associés au non-respect de la règlementation

Etude de cas (partielle) : synthèse des résultats
Phase de restitution 1/2

- Par type de risque (actuel)

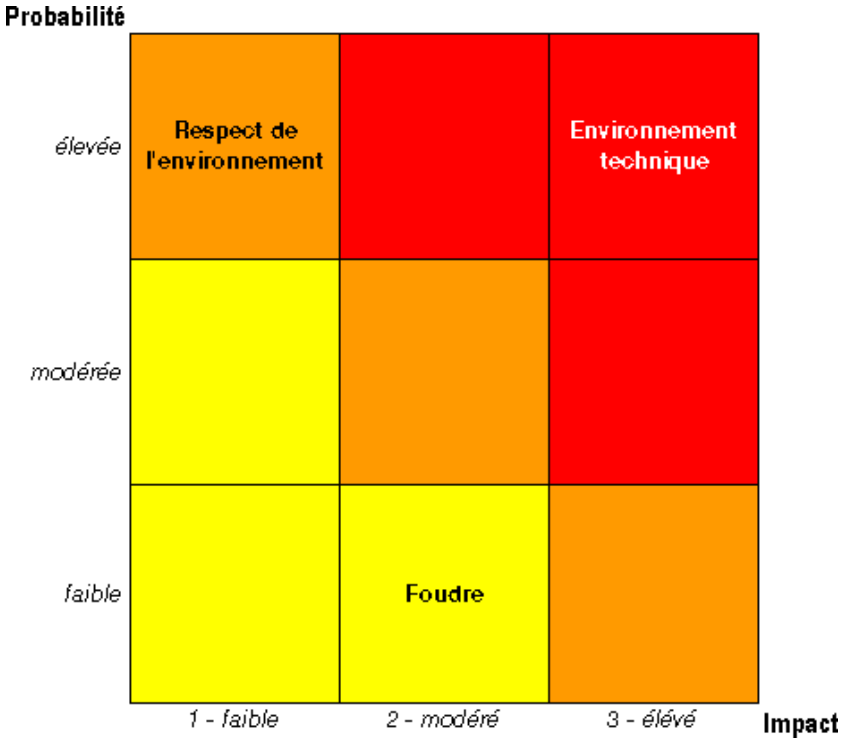


- Par menace générique (CNPP)

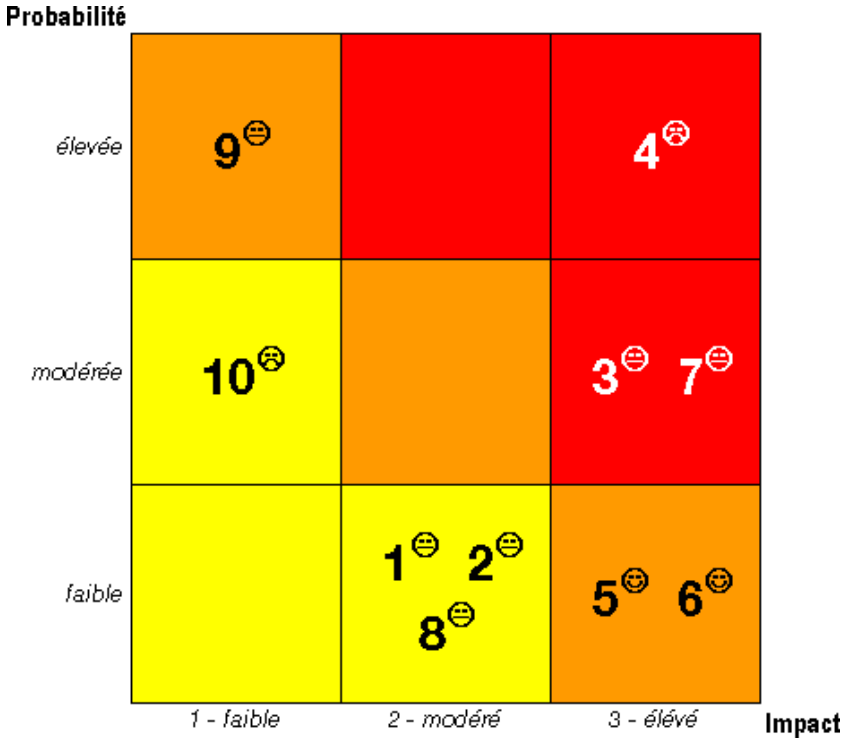


Etude de cas (partielle) : synthèse des résultats
Phase de restitution 2/2

- Par type de risque (actuel)



- Par risque et niveau de couverture



Conclusion

- Le cadre de référence EBIOS ne se substitue pas au terrain, il se sert des conclusions du terrain pour mieux les représenter

- Bénéfices du cadre de référence analytique (cf. étude de cas) :
  - > Formaliser les cibles pour identifier les périmètres d'action d'une cible donnée
  - > Formaliser les triplets objet de risque / critère / type d'impact pour assurer la cohérence
  - > Assurer la complétude (« être sur de ne rien oublier ») via l'utilisation des bases existantes

- Bénéfices de la réflexion sur les formes de restitution (outillée) :
  - > Proposer différentes représentations des risques selon l'audience (ex. : porteur du risque)
  - > Enregistrer les résultats de l'analyse de risque de façon auditable
  - > Rendre possible le suivi des risques dans la durée
  - > Comparer plusieurs analyses de risque de même nature
  - > Faciliter le travail de l'auditeur