CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Intégration de la sécurité physique à l'analyse de risque

Vers une méthode unifiée d'identification et d'appréciation des risques

SYLVAIN CONCHON

CONIX

Préambule

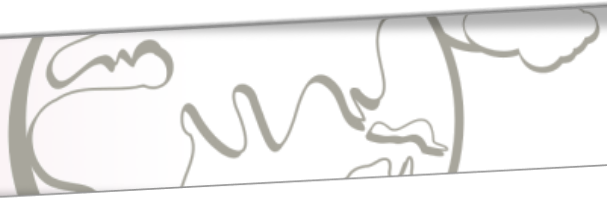
- Le présent support expose, pour partie, des travaux effectués en collaboration avec ORANGE, dont des extraits sont reproduits avec l'aimable autorisation d'ORANGE

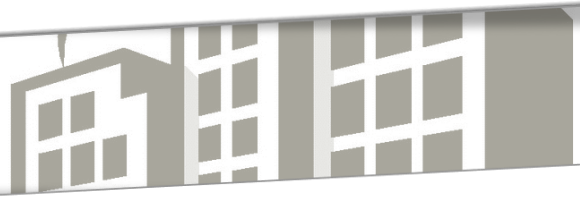
- Contacts ORANGE :
  - Denis MANGIN (denis.mangin@orange.com)
  - Laurence MARCHAL (laurence.marchal@orange.com)

Constats

Maturité des méthodes (d'analyse des risques) pour la sécurité de l'information

Maturité des pratiques pour la sécurité physique (fortement soutenues par la conformité)





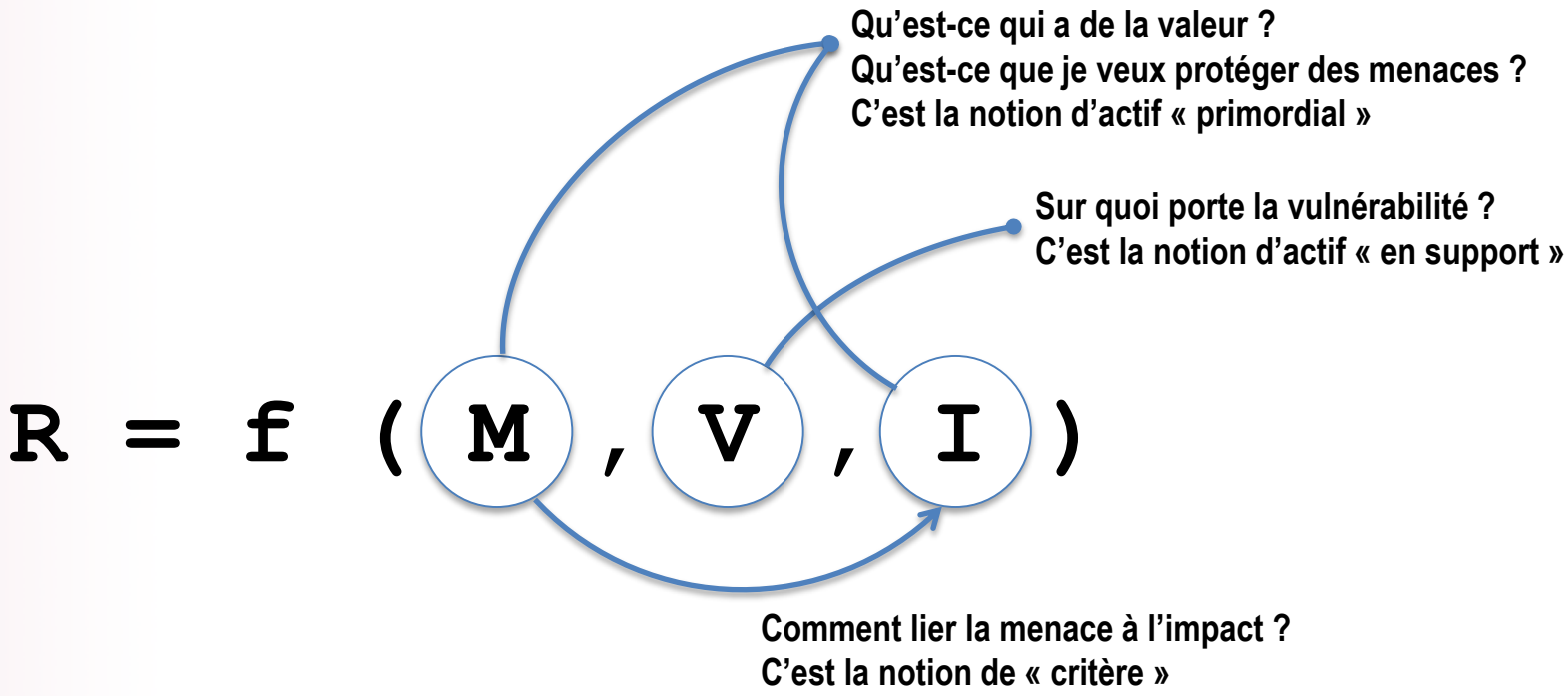
Faiblesse de la prise en compte de la sécurité physique dans les analyses sécurité de l'information

Faiblesse de la restitution par le risque dans les pratiques de sécurité physique

Objectifs

- Définir un cadre de référence analytique commun
- Bénéficier d'une approche méthodologique éprouvée
  - Reproductible
  - Pertinente
  - Réaliste
- Mettre à l'épreuve par une étude de cas

L'équation (universelle) du risque



risque de sécurité de l'information

« possibilité que des menaces exploitent les vulnérabilités [d'un actif en support] et portent atteinte [à un actif primordial selon un critère de sécurité] induisant un impact sur l'organisation »

ISO/IEC 27005:2013 – 3.9 (reformulé)

L'équation (universelle) du risque

- Clefs de compréhension du risque de sécurité physique
  - Les **actifs primordiaux** propres au domaine
  - Les **actifs en support** propres au domaine
  - Les **critères de sécurité** propres au domaine
  - Les **menaces** propres au domaine
  - Les **vulnérabilités** propres au domaine

- Choix d'un cadre de référence formel : ISO 27005

Correspondance du vocabulaire

Sécurité de l'Information	**Sécurité Physique**
Actif primordial	Objet de risque
Actif en support	Cible
Un actif primordial est <u>parfois</u> un actif en support	Un objet de risque et <u>souvent</u> une cible

Objets de risque

Sécurité de l'Information	Sécurité Physique
Informations	Personne
Fonctions	Flux [1]
	Biens meubles
	Biens immeubles

Un actif primordial est toujours intangible

[1] Flux d'énergie, flux de matière, flux de personnes, flux d'information, flux financier

Cibles

Sécurité de l'Information	Sécurité Physique
Matériels	Personne
Logiciels	Flux
Réseau	Biens meubles
Personnel	Biens immeubles
Site	
Organisation	
Bases de connaissances existantes	Bases de connaissances à construire

Critères de sécurité

Sécurité de l'Information	Sécurité Physique
Disponibilité	Disponibilité
Intégrité	Intégrité (physique)
Confidentialité	Intégrité (mentale)
	Confidentialité (localisation)
Autres critères possibles (souvent composites) : conformité, imputabilité, authenticité, etc…	Conformité

Bases de connaissances : menaces

- Travaux
  - Identification des **menaces** par catégorie
  - Identifier les triplets [menaces, critères, objets de risque]

- Sources possibles
  - Base de connaissance référentiels CNPP [1]
  - Base de connaissance référentiels sécurité de l'information
  - Bon sens (!)

[1] *Centre National de Prévention et de Protection*

Bases de connaissances : menaces

- Extrait de travaux (voir support analytique)

index	code	menace de niveau 1	menace de niveau 2
001	M.01	Vol	
003	M.02	Agression	
004	M.02.01		Agression physique à l'intérieur du site
005	M.02.02		Séquestration à l'intérieur du site
006	M.03	Dégradation	
011	M.04a	Incendie à l'intérieur du site	
014	M.04b	Incendie à la périphérie du site	
018	M.05a	Explosion à l'intérieur du site	
021	M.05b	Explosion à la périphérie du site	
025	M.06	Pollution	
026	M.06.01		Pollution (eau, air, sol) intentionnelle du site à partir de sources internes (liquide frigorigène, produit polluant, etc.)
027	M.06.02		Pollution (eau, air, sol) accidentelle du site à partir de sources internes (liquide frigorigène, produit polluant, etc.)
028	M.06.03		Pollution (eau, air, sol) du site à partir de sources contingentes (eaux usées, eaux de ruissellement, etc.)
029	M.07	Evénement naturel	
035	M.08	Sinistre majeur	
039	M.09	Atteinte spécifique à la personne	
040	M.09.01		Accident du travail
041	M.09.02		Autres atteintes à la personne (dont : intoxication, malaise, maladie du aux conditions sanitaires)

Bases de connaissances : vulnérabilités

- Travaux
  - Identification de **cibles** par catégorie
  - Identification de **vulnérabilités** par catégorie
  - Associer chaque **vulnérabilité** à une (ou plusieurs) **menaces**
  - Associer chaque **vulnérabilité** à une (ou plusieurs) **cibles**

- Sources possibles
  - Règlementation (code du travail, règlementation anti-incendie, etc.)
  - Référentiels internes ORANGE
  - Base de connaissance référentiels sécurité de l'information
  - Déduction à partir de vulnérabilités

Bases de connaissances : cibles

- Extrait des travaux (voir support analytique)

index	code	sélection	catégorie de la cible	nature de la cible
001	IMM		Bien immeuble	
002	IMM.SIT		Bien immeuble	Site
008	IMM.BAT		Bien immeuble	Bâtiment
015	IMM.LOC		Bien immeuble	Locaux
030	MBL		Bien meuble	
031	MBL.EQT		Bien meuble	Equipements
044	MBL.FLX		Bien meuble	Biens relatifs au transport des flux
048	MBL.DIV		Bien meuble	Autres biens meubles
051	PER		Personne	
052	PER.INT		Personne physique	Personnel interne
057	PER.EXT		Personne physique	Personnel externe

Bases de connaissances : cibles

- Extrait des travaux (voir support analytique)

index	code	sélectio	catégorie de la cible	nature de la cible	cible
030	MBL		Bien meuble		
031	MBL.EQT		Bien meuble	Equipements	
032	MBL.EQT.01		Bien meuble	Equipements	Equipement électrique
033	MBL.EQT.02		Bien meuble	Equipements	Batteries
034	MBL.EQT.03		Bien meuble	Equipements	Dispositif de détection d'incendie
035	MBL.EQT.04		Bien meuble	Equipements	Centrale de détection d'incendie
036	MBL.EQT.05		Bien meuble	Equipements	Alarme d'évacuation
037	MBL.EQT.06		Bien meuble	Equipements	Installation d'extinction d'incendie
038	MBL.EQT.07		Bien meuble	Equipements	Détecteur de gaz
039	MBL.EQT.08		Bien meuble	Equipements	Extincteurs mobiles
040	MBL.EQT.09		Bien meuble	Equipements	Robinets d'incendie armés
041	MBL.EQT.10		Bien meuble	Equipements	Dispositif de désenfumage
042	MBL.EQT.11		Bien meuble	Equipements	Dispositif de protection contre la foudre
043	MBL.EQT.12		Bien meuble	Equipements	Bornes et poteaux incendie
044	MBL.FLX		Bien meuble	Biens relatifs au transport des flux	
045	MBL.FLX.01		Bien meuble	Biens relatifs au transport des flux	Conducteurs et câbles électriques
046	MBL.FLX.02		Bien meuble	Biens relatifs au transport des flux	Gaines de circulation d'air
047	MBL.FLX.03		Bien meuble	Biens relatifs au transport des flux	Gaines et canalisations de fluide (autre que l'air)
048	MBL.DIV		Bien meuble	Autres biens meubles	

Bases de connaissances : vulnérabilités

- Voir support analytique
  - KDB d'environ 500 vulnérabilités
  - Distinction par catégories et sous-catégories
  - Association avec les cibles portant les vulnérabilités
  - Association avec les menaces correspondantes

Bénéfices de l'approche analytique

- Apport pour la **cohérence** des conclusions de l'audit terrain :
  Causes différentes + Effets identiques → Impacts identiques
- Apport pour la **complétude** des conclusions de l'audit terrain :
  Causes identiques + Effets différents → Impacts différents

- Démarche **reproductible** et **répétable**

ATTENTION

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

Conclusion / Ouverture

- L'approche proposée s'exporte à de nombreux domaines
  - Sûreté de fonctionnement (par ailleurs mature)
  - Domaine des risques psycho-sociaux
  - Domaine des risques projet
  - Domaine des risques de responsabilité sociétale

- Vers un management unifié des risques ?

Merci de votre attention

- Pour aller plus loin : http://blog.conixsecurity.fr/?p=1535

SYLVAIN CONCHON
sylvain.conchon@conix.fr