**MANAGEMENT DE LA SURETE**

**1/ Introduction**

         Dans le domaine du nucléaire civil, la sécurité est définie comme l’aptitude d’une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques. La sûreté est la sécurité vis-à-vis des actes de malveillance.

         Si dans le monde nucléaire, la sûreté atteint son paroxysme (maximum), cette discipline concerne également l’ensemble des établissements tertiaires et industriels. Toutefois, les enjeux ne seront pas les mêmes dès lors qu’il s’agit de protéger l’information (sûreté de l’information et des moyens de communication) ou les matériels (sûreté physique). En terme de malveillance, les risques liés aux activités de bureaux, aux laboratoires de recherche ou aux équipements d’installations classées sont différents. En effet, hormis les risques de spoliation (vol)

ou autres actes de criminalité courante qui concernent à la fois les sites tertiaires et industriels, le risque lié à l’espionnage méritera une plus grande attention sur les bâtiments administratifs et laboratoires alors que la prévention des actes de sabotage ou de terrorisme concernera plus les infrastructures industriels. Certes, quel que soit le site, aucun scénario de malveillance ne doit être écarté, mais à l’heure du choix des moyens de protection, un arbitrage sera nécessaire pour se prémunir de certaines catégories d’actes de malveillance.

         Le présent document a pour objectif de fournir une première approche du management de la sûreté qui implique tout d’abord l’analyse des risques sûreté, puis l’élaboration d’un état des lieux sécuritaires et organisationnels selon l’identification des menaces pouvant peser sur le site, et enfin la définition des moyens de protection.

**2/ La mise en œuvre de la démarche sûreté**

**2.1 L’analyse des risques**

 La première étape de mise en œuvre de la démarche sûreté au sein d’un établissement consiste à analyser les risques sûreté et les différentes catégories de menaces pouvant peser sur le site. Bien que l’imagination des criminels soit débordante, il est néanmoins possible d’établir une typologie de la malveillance. Qu’ils soient d’origine interne ou externe à l’établissement, les actes de malveillance peuvent être regroupés selon les catégories suivantes :

**-Criminalité courante**

**-Troubles sociaux**

**-Sabotage**

**-Terrorisme**

**-Espionnage**

**\*Niveau de risque**

Criminalité courante XXX

Troubles sociaux XX

Sabotage X

Terrorisme X

Espionnage XXX

1-Faible X

2-Modéré X X

3-Elevé X XX

4-Très élevé X XXX

           Sur cet exemple, il apparaît que les risques d’espionnage et de criminalité courante sont les plus élevés. Les efforts de protection porteront prioritairement sur ces risques. Mais avant de définir les moyens de protection, il est nécessaire de réaliser un état des lieux sécuritaire et organisationnel du site à la lumière de l’analyse des risques.

**2.2 Etat des lieux sûreté d’un site :**

          La sûreté d’un site concerne d’une part la sûreté de l’information, et d’autre part la sûreté physique de l’établissement. Pour la sûreté de l’information, un test d’intrusion informatique pourra être mené. En effet, il est important de connaître la capacité d’un hacker à pénétrer informatiquement sur un site pour soustraire des informations confidentielles ou manœuvrer des procédés industriels.

          Pour la sûreté physique, la Check List suivante permet d’élaborer un état des lieux sur le niveau de sécurité sûreté d’un établissement. Cette Check List, non exhaustive, a été élaborée pour les sites tertiaires et industriels.

         Elle sert de trame à un audit terrain des installations et permet de détecter les vulnérabilités selon les items suivants :

**\*Management de la sûreté :**

-Clôture

-Végétation

-Eclairage

-Vidéosurveillance extérieure

-Vidéosurveillance intérieure

-Localisation du poste de sûreté

-Entrée sur site

-Accès du personnel à l’intérieur du site

-Accès logistique

-Accès sous-traitant

-Gestion des badges

-Gestion des visiteurs

-Gestion des flux de personnels

-Gestion des flux des transporteurs

-Gestion des flux ferroviaires

-Gestion des flux maritimes

-Zonage du site

-Zonage des bureaux

-Détection des zones blanches, grises, noires et rouges et exposition sûreté

-Prestation des gardiens

-Documents tenus à jour par les gardiens

-Procédures de gardiennage

-Organisation générale de la prestation du service de sûreté

-Gestion de Crise

-Gestion des alarmes

-Plans d’urgence et de Continuité

-Confidentialité des plans de gestion de crise

-Protection de la confidentialité

-Conservation des documents sensibles

-Destruction des documents

-Gestion des télécopieurs

-Gestion des photocopieurs

-Circuit de notoriété

-Gestion des salles de réunion

-Gestion des clés

-Traitement de l’information électronique

-Recrutement du personnel permanent, intérimaire et des stagiaires

**MALVEILLANCE ET PROTECTION PHYSIQUE**

**Contexte thèmes sécurité**

**LES AGRESSIONS**

\*les vols:

-matériels

-informations

\*les actions malveillantes

-internes

-Externes

**PREVENTION ET PROTECTION**

\*Sensibilisation du personnel:

-Encadrement

-Exploitant

\*Protection de l’information:

-Confidentialité

-Sécurité informatique

**Contexte(suite)**

\*Protection des dirigeants:

-analyse d’un phénomène d'agression

-méthodologie en matière de prévention et de protection

-protection physique in-situ

\*les barrières

-La protection mécanique

-Le contrôle d’accès

\*la détection

-La détection électronique

-La vidéosurveillance

-Protection physique à distance

\*télésurveillance

\*télé sécurité

**LES AGRESSIONS**

**LE VOL**

**LA MALVEILLANCE**

**Malveillance interne**

-La malveillance interne est réalisée par un agent de l’entreprise ou d’une entreprise sous-traitante ayant normalement accès aux différents locaux

**\*LES MOTIVATIONS**

-La vengeance due à un sentiment de mécontentement ou de jalousie,

-Le dérangement mental

-L’intérêt personnel

**\*LA CIBLE**

-Nuire à une ou des personnes de l’entreprise

-Dégrader la qualité de la production ou la ralentir

-Détruire l’outil de travail partiellement ou totalement

**\*LES MOYENS**

-Subreptices : Il s’agit de réaliser un ou des sabotages en prenant des précautions pour ne pas être particulièrement suspecté(cas 1 et 2 ci-dessus)

De plus grande ampleur : cas n°3 sans se soucier d’être éventuellement démasqué.

**Malveillance externe**

-La malveillance externe est réalisée par un ou des agresseurs désirant endommager ou paralyser l’entreprise éventuellement en causant des nuisances hors du Site.

**\*LES MOTIVATIONS**

-L’impact médiatique;

-Le terrorisme;

-La vengeance;

-La concurrence.

**\*LA CIBLE**

-Nuire à la direction de l’entreprise;

-Détruire ou paralyser l’outil de travail;

-Nuire à une installation importante pour la Nation;

..Causer des dégâts matériels et personnels significatifs.

**\*LES MOYENS**

-Individu seul ou commando amateur : ne cherchant pas forcément à faire des victimes;

Groupe organisé: commando terroriste éventuellement Kamikaze disposant d’explosifs performants et de moyens de déplacement sophistiqués.

**PREVENTION ET PROTECTION**

Comment protéger un établissement ou une installation ?

**METHODOLOGIE EN MATIERE DE PREVENTION ET DE PROTECTION**

**\*ANALYSE D’UN PHENOMENE D'AGRESSION**

-La menace est fonction de 3 conditions : la motivation –la facilité de l’action –la perspective d’impunité.

-L’objectif : personne à risque (le décideur –le fortuné–l’homme-clé –le symbole).

-L’agresseur : type droit commun (motivation criminelle) –idéologique (politique –religieuse…)

 –psychopathe ou déséquilibré (investi d’une mission –vengeance).

-Modes opératoires : harcèlement, violence physique –compromission, chantage –enlèvement, prise d’otage –attentat, assassinat.

**METHODOLOGIE EN MATIERE DE PREVENTION ET DE PROTECTION**

-Elle peut être élaborée en interne (politique de prévention).

-Ou en faisant appel à des spécialistes (politique de protection).

**\*Etude méthodique des moyens de prévention et de protection** :

-Vis-à-vis du vol : L’étude de Sécurité(**EDS**).

-Vis-à-vis du sabotage : Le Dossier de prévention contre les Actes de Malveillance**(DPAM**).

**\*Contenu d’une Etude de Sécurité** :

-Introduction;

--Identification des zones sensibles (Etude de sensibilité);

-Définition des menaces prises en compte;

-Identification des cibles et des zones de protection;

-Recensement des cheminements (Etude de vulnérabilité);

-Analyse des cheminements et détermination des chemins critiques;

-Analyse des interventions;

-Améliorations envisageables.

**\*Contenu d’une Etude de Malveillance :**

**DEUX TYPES DE MENACES :**

**1) -MENACE INTERNE**

Agent appartenant à l’entreprise ou à une entreprise extérieure, ayant habituellement accès aux installations, et cherchant à réaliser subrepticement (discretement) :

-Vol de matériel ou vol d’informations;

-Sabotage.

**2) -MENACE EXTERNE**

**\*Menace aléatoire (type A) :**

-Equipe limitée d’agresseurs, munis de matériel de cambriolage usuel et disposant d’explosifs courants cherchent à dérober du matériel ayant une valeur marchande ou à saboter les installations.

**\*Menace ciblée (type B) :**

-Commando d’agresseurs bien renseignés, munis de matériel de cambriolage sophistiqué et d’explosifs performant.

.Cherchent à dérober une quantité d’objets conséquente, de renseignements confidentiels détenus dans l’installation;

.Cherchent à créer des dégâts importants dans les installations y compris avec nuisances pour l’environnement (**AZF**).

**IDENTIFICATION DES CIBLES**

A titre d’exemple

**\*3 cibles identifiées** :

-Cible 1 : matériel informatique (procédé);

-Cible 2 : objets réalisés dans l’installation (entreposage des produits finis);

-Cible 3 : secrets de fabrication (coffre).

**\*Localisation des cibles identifiées** :

-Localisation géographique de chaque cible (plans);

-Dispositions de sécurité associées à chaque cible (moyens de surveillance, de protection et d’alerte).