

**EVALUATION DES CONSEQUENCES ECONOMIQUES
DES INCIDENTS ET SINISTRES RELATIFS
AUX SYSTEMES INFORMATIQUES**

France, 1996

PRESENTATION

L'APSAD¹, puis le CLUSIF² ont mis en place depuis 1983 un observatoire de la sinistralité des risques informatiques, permettant d'évaluer grossièrement l'impact économique³ et plus encore son évolution dans le temps (à méthode d'évaluation constante). **Le CLUSIF poursuit seul cette tâche délicate depuis 1990.**

Les chiffres indiqués dans ce rapport sont exprimés en millions de francs.

Cette évaluation qui doit être considérée avec précaution, ne concerne que le secteur non-gouvernemental, et uniquement vis-à-vis des conséquences économiques immédiatement exposables⁴. Il est clair qu'il existe d'autres conséquences⁵, dont certaines sont susceptibles d'avoir une incidence économique à moyen ou long terme, sans pour autant qu'elles puissent être facilement évaluées.

Ce document de synthèse comporte plusieurs volets :

- 1 - Estimation des pertes dues à des sinistres informatiques en France, en 1996, selon les causes.
- 2 - Estimation des pertes dues à des sinistres informatiques en France, en 1996, selon les conséquences.
- 3 - Commentaire sur la situation et l'évolution 1996/1995.
- 4 - Evolution de la sinistralité sur les dix dernières années.
- 5 - Tendances.
- 6 - Annexe (définitions).

Note : Les chiffres de l'évaluation 1996 ne sont que relativement comparables à ceux des années précédentes (en particulier pour la catégorie « Fraude »), car ils incluent, pour la première fois, les pertes liés à la malveillance téléphonique (« phreaking »).

¹ Assemblée Plénière des Sociétés d'Assurances Dommages, 26, boulevard Haussmann - 75009 PARIS.

² Club de la Sécurité Informatique Français, 26, boulevard Haussmann - 75009 PARIS.

³ Le mode d'estimation est le même que pour les années précédentes, c'est-à-dire que l'analyse du "chiffre noir" par rapport au chiffre connu est faite séparément pour chaque ligne (en fonction du calcul de surface des éléments de la courbe de distribution nombre/montant, la principale étant l'Assurance). D'autres estimations croisées (en ligne et en colonne) portent directement sur les tendances "à dire d'expert".

⁴ Evaluation immédiate ou dans les trois mois après la survenance du sinistre des frais et des pertes d'exploitation à douze mois.

⁵ Dérive de la responsabilité civile ou pénale, patrimoine immatériel (scientifique, industriel, commercial, etc.), déstabilisation (personnel, entreprise, secteur, marché, etc.), perte d'image, désordre civil ou défense, "privacités", vie humaine, etc.

**1 - ESTIMATION DES PERTES DUES A DES SINISTRES INFORMATIQUES(1) EN FRANCE EN
1996(2) SELON LES CAUSES(3) EN MF**

Conséquences (4)	DIRECTES		INDIRECTE				TOTAL
	C1 Matériel	C2 non- matériel	C3 Frais supplémentaires et pertes d'exploitation	C4 Pertes de patrimoine	C5 Responsabilité civile	C6 Divers	
Types de risques(4)							
Accidents							
A1 - Physiques (incendie, Explosion, Dégâts des eaux, Pollution, etc.)	400	30	1 100		100		1 630
A2 - Pannes, dysfonctionnements		100	900		110		1 110
A3 - Force majeure (Evénements naturels)	25		10				35
A4 - Perte de services essentiels (Télécom., électricité, eau, etc.)		5	250		25		280
A5 - Autres							
Erreurs							
E1 - Erreurs d'utilisation		100	500		200		800
E2 - Erreurs de conception et de réalisation		120	700		200		1 020
Malveillance							
M1 - Vol, vandalisme (physique)	220	20					240
M2 - Fraude(5) (non physique)			500	1 730	70		2.300
M3 - Sabotage (physique)	5						5
M4 - Attaque logique (non physique)		510	510	30	40		1 090
M5 - Divulgateion				1 000	100		1 100
M6 - Autres			60 (6)			3 050 ⁽⁷⁾	3 110
TOTAL	650	885	4 530	2 760	845	3 050	12 720

(1) Ensemble des systèmes informatiques, bureautique, télécommunication, matériel informatique et télécommunication annexe (serveurs, modems, processeurs, etc. hors téléphone et fax), périphériques divers et spécialisés (incluant la robotique mais hors monétique et cartes à puces, caleulettes, etc.).

(2) Hors gouvernemental et administrations. Ces estimations qui correspondent à des ordres de grandeur établis à partir de la fraction des cas connus et des tendances sont plus ou moins précises selon les lignes et colonnes : globalement la précision est-elle même estimée à ± 30 %.

(3) Cette grille harmonisée a été mise au point en 1991 par la Commission Assurance et Sécurité des Risques Informatiques du CEA (Comité Européen des Assurances) qui regroupe les délégués des principaux pays CEE + AELE.

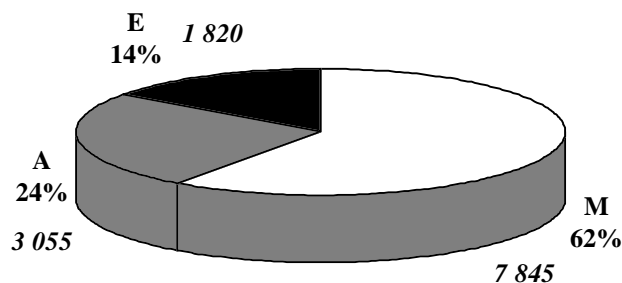
(4) Voir définitions en annexe.

(5) Cette rubrique incorpore les fraudes d'origine informatique et télécom. (ou la "part imputable à ..."). Elle inclut depuis 1996 la fraude associée à la carte à microprocesseur et aux différents modes de paiement électronique. Cette rubrique incorpore le détournement de fonds et le détournement de biens, mais n'inclut pas le chantage et l'extorsion (pas plus que la rubrique M4).

(6) Risques humains (départs de personnel, pénurie de personnel, grève, etc.).

(7) - Copie illicite de progiciels (1 700). Cette évaluation, plus faible que celle des éditeurs de logiciels, repose sur une approche marginale des coûts que nous jugeons plus juste.

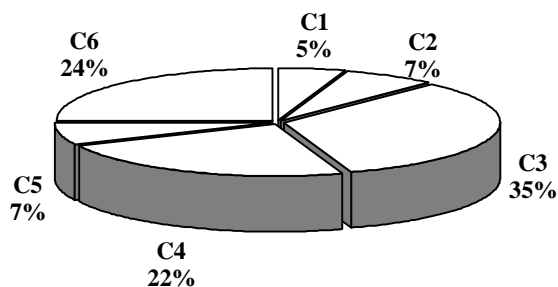
- Utilisation non autorisée de ressources informatiques : 1 350 (0,5 % Budget Informatique et Télécom/informatique de la Nation).



Types de causes	%
A (Accidents)	+ 6,4 %
E (Erreurs)	- 1,6 %
M (Malveillance)	+ 14,7 %
TOTAL	+ 10 %

EVOLUTION 1006/1005

2 - LES CONSEQUENCES



Types de conséquences économiques	
C1	+ 14,0 %
C2	- 0,6 %
C1 + C2	+ 5,1 %
C3	+ 15,0 %
C4	+ 10,8 %
C5	- 8,2 %
C6	+ 10,9 %
C3 + C4 + C5 + C6	+ 10,7 %
TOTAL	+ 10,0 %

Définitions :

Disponibilité (D) : Aptitude d'un système d'information à pouvoir être employé par les utilisateurs habilités dans les conditions d'accès et d'usage (notamment performancielles) normalement prévues.

Intégrité (I) : Propriété qui assure qu'une information n'est modifiée que par les utilisateurs habilités dans les conditions d'accès normalement prévues.

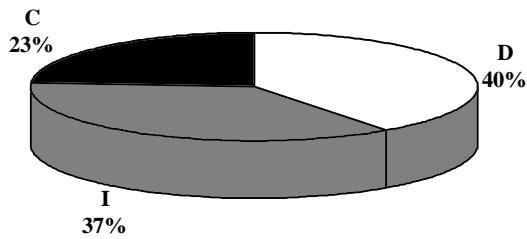
Confidentialité (C) : Propriété qui assure que seuls les utilisateurs habilités dans les conditions normalement prévues ont accès aux informations.

Imputabilité (W) : Propriété qui permet d'imputer de façon certaine une opération à un utilisateur à un moment donné.

Origine	Destination	Disponibilité D	Intégrité(1) I	Confidentialité C
A1		1 450	180	
A2		860	250	
A3		35	0	
A4		260	20	
A5				
*** A		2 605	450	
E1		100	700	
E2		400	600	20
*** E		500	1 300	20
M1		230		10
M2		200	2 100	
M3		5		
M4		270	820	
M5				1 100
M6 (2)		1 350		1 760
*** M		2 055	2 920	2 870
TOTAL		5 160	4 670	2 890

(1) Incluant l'imputabilité (W).

(2) Rangement relativement arbitraire.



Types de conséquences directes	%
D	+ 9,0 %
I	+ 10,7 %
C	+ 10,9 %
TOTAL	+ 10,0 %

EVOLUTION 1996/1995

3 - COMMENTAIRE SUR LA SITUATION ET L'EVOLUTION 1996/1995

A) Accidents

La sinistralité a plutôt régressé en 1996, mais les chiffres de la ligne A1 sont perturbés par la survenance d'un très gros sinistre. L'augmentation de l'informatique nomade "communicante" continue d'alimenter le "bruit de fond". On constate une relative détérioration de la prévention sur les grands sites, mais une intégration croissante de la prévention sur les sites petits et moyens, pour les techniques courantes (régulation de l'alimentation électrique, sauvegarde). Les plans de secours sur les sites moyens-grands et grands sites s'améliorent.

La ligne A1 augmente atypiquement de 10,9 % ; la ligne A2 augmente de 7,8 %, notamment en raison des problèmes de télécommunication (liaisons entre réseaux hétérogènes). La ligne A3 est en baisse de 65 %, mais il faut analyser le risque sur le long terme. La ligne A4 n'augmente que de 3,7 %, mais principalement à cause des télécommunications (C3/A1 : + 8,7 %).

B) Erreurs

Bien qu'elles soient difficiles à évaluer, les pertes liées à la saisie, à l'exploitation et à la télétransmission des données ont continué à baisser, malgré le développement continu des volumes. En revanche, les pertes liées à la transmission de supports de données continuent d'augmenter (le laxisme est stable à cet égard dans les entreprises) et les erreurs d'interprétation (exemple : EIS) ont tendance à augmenter (faute de clarté de certains produits, et faute d'éducation).

Les erreurs de conception de logiciels et progiciels continuent à augmenter, dans tous les compartiments : bugs graves et inadmissibles dans certains progiciels lancés trop tôt du fait de la concurrence, fautes architecturales graves ayant des conséquences fonctionnelles ou performanciennes. Ici encore les SSII en subissent souvent le contrecoup en RC.

C) Malveillance

La France, qui avait été relativement épargnée par la vague de vol de matériels et de composants d'informatique et de télécommunications, est à son tour touchée (M1 : + 20 %).

Le Clusif a cherché à incorporer en 1996 dans la ligne fraude, l'ensemble des fraudes complètement ou significativement imputables à l'informatique et aux télécommunications, de sorte que les chiffres 96 ne sont pas exactement comparables à ceux 95 (avec notamment l'incorporation des moyens de paiement électronique par des dispositifs - cartes ou autres - dotés au moins d'un microprocesseur et moyens de paiement à carte simple complétés par un protocole d'échange ainsi que de la malveillance téléphonique). L'augmentation apparente de la ligne M2 (+ 37,7 %) serait ramenée à environ + 5 % à définition constante. Cette augmentation traduit une inflexion à la hausse après deux ans de calme relatif. Les fraudes observées portent davantage sur le détournement de biens que sur celui de fonds. Les scénarios sont plus complexes au plan fonctionnel, mais pas au plan technique. Ils font intervenir davantage d'acteurs (et de plus en plus de "professionnels" à l'extérieur des entreprises), étant entendu que les personnels de l'intérieur de l'entreprise sont plus ou moins impliqués dans 70 % des cas. Les enjeux visés évoluent vers le haut du compte d'exploitation ou du bilan (à l'actif comme au passif).

Il semble en revanche que l'on observe une baisse des attaques logiques (- 12,1 %). La fréquence des contaminations virales a légèrement augmenté, mais les conséquences sont mieux maîtrisées que par le passé. L'année 96 est en outre probablement atypique, en ce sens que peu d'attaques logiques ciblées ont été déclarées. Il faut toutefois rester prudent du fait qu'en contrepartie, les opérations de chantage et d'extorsion à l'attaque logique ont pu augmenter, alors que nous ne les comptabilisons pas.

L'espionnage économique, très difficile à évaluer, semble toutefois progresser très significativement (M5 : + 22,2 %), même si de nombreuses formes d'attaques sont à la limite de la légalité.

Enfin, la copie illicite de logiciels demeure un problème préoccupant, et nous avons du réévaluer nos estimations, même si celles-ci restent très inférieures à celles des éditeurs de logiciels.

4 - EVOLUTION DE LA SINISTRALITE EVALUEE ENTRE 1987 ET 1996 (en francs courants)⁶

	1987	1996		1987	1996	t %/an
A	2150	3 055	A1 - Physiques	1180	1 630	+ 3,7
			A2 - Pannes	970	1 110	+ 1,5
			A3 - Force majeure	NS	280	NS
			A4 - Perte de services essentiels	NS	0	NS
E	1790	1 820	E1 - Erreurs d'utilisation	1090	800	- 3,4
			E2 - Erreurs de conception et de réalisation	700	1 020	+ 4,3
M	3970	7 845	M1 - Vol (physique)	70	240	+ 14,7
			M2 - Fraude (non physique)	1200	2 300	+ 7,5
			M3 - Sabotage (physique)	NS	5	NS
			M4 - Attaque logique (non physique)	800	1 090	+ 3,5
			M5 - Divulgateion	380	1 100	+ 12,5
			M6 - Autres	1520	3 110	+ 8,3
TOTAL	7910	12 720				t = +5,4 %/an

	1987	1996
A	28 %	24 %
E	23 %	14 %
M	49 %	62 %

Ventilation par cause

	1987	1996
D	51 %	40 %
I	31 %	37 %
C	8 %	23 %

Ventilation par conséquence primaire

Pertes	1987	1996
Directes (matériel et non-matériel)	5,6 %	12,1 %
Frais supplémentaires et PE	64,9 %	35,6 %
Pertes de patrimoine	23,4 %	21,7 %
Responsabilité civile	6,2 %	6,6 %
Divers	n/a	24,0 %

Ventilation par conséquence économique

⁶ t est le taux moyen de variation annuelle

Commentaire : La situation a considérablement évolué en dix ans. Il faut toutefois évaluer avec prudence cette évolution, du fait que certaines définitions ont changé depuis 1987, de l'imprécision des chiffres, de l'évolution des mentalités (diminution de la propension de non déclaration selon les catégories), et de la modification du contexte (information, appareil juridique réglementaire et juridique, actions des services de l'Etat, etc.).

5 - TENDANCES

Type de risque	Tendance 1997 ⁷	Tendance long terme ⁸
A1 - Physique	102-104	+
A2 - Pannes	103-105	+
A3 - Force majeure	-	#
A4 - Perte de services essentiels	104-110	+
E1 - Erreurs d'utilisation	90 - 95	NS
E2 - Erreurs de conception et de réalisation	100 - 105	+
M1 - Vol (physique)	110 - 120	++
M2 - Fraude (non physique)	106 - 108	++
M3 - Sabotage (physique)	-	#
M4 - Attaque logique (non physique)	110 - 120	+
M5 - Divulgateion	110 - 120	++
M6 - Autres	105 - 115	NS

Commentaire : Nous pensons que la croissance de la malveillance va continuer à être forte, en nous fondant sur plusieurs critères :

- Poursuite de la crise en général et rémanence de ses paramètres : insécurité de l'emploi et chômage, tensions sociales, concurrence, etc.
- Risques de tensions internationales.
- Poursuite de la crise informatique et apparition de tensions dans le secteur des télécommunications, et rémanence de ses paramètres : mutation des systèmes et architectures, budgets restrictifs, mutation des fonctions des informaticiens, déstabilisation de certaines fonctions informatiques, etc.
- Complexification, interconnexion des systèmes.
- Evolution des mentalités, manque d'éducation.
- Banalisation, diversification de l'informatique.
- "Explosion" des communications.
- Augmentation des "enjeux" supportés par les systèmes d'information.
- Etc.

⁷ Indice 100 en 1996 ; estimation à dire d'experts.

⁸ Légende :

•	Croissance non significative	#	Croissance impossible à prévoir
+	Faible croissance	-	Faible décroissance
++	Croissance significative à forte	--	Décroissance significative

Annexe : DEFINITIONS

1 - TYPES DE RISQUES

11. ACCIDENTS

A1 - Incendie, explosion, implosion, dégâts des eaux, bris de machine

***Banque** : Incendie d'un centre informatique de traitement de chèques. Ce centre disposait d'un contrat de télé-back-up avec une société de services, mais il avait été insuffisamment testé, notamment au plan des télécommunications. La chaîne n'a pu fonctionner à nouveau - en mode très dégradé - que vingt jours après le sinistre. Le dommage matériel (essentiellement dû aux fumées et au gaz de décomposition du gaz extincteur) est évalué à 1,1 MF, tandis que les pertes indirectes sont évaluées à 15 MF.*

A2 - Pannes (matérielles et logiques) : Il s'agit de l'ensemble des causes d'origine ou de révélation interne entraînant l'indisponibilité ou le dysfonctionnement (non conformité aux fonctionnalités et performances nominales) total ou partiel du système.

***Services** : Hyperdessiccation de l'atmosphère de la salle ordinateurs due à une défaillance de la climatisation (report d'alarme défectueux) : la température s'élève à plus de 60° C. Le constructeur, BULL, estime que le matériel est irréversiblement endommagé et refuse toute maintenance en cas de sauvetage partiel. Les données sont également endommagées et les sauvegardes lacunaires ne permettront pas de tout récupérer. Pertes matériels et frais : environ 50 MF, autres pertes évaluées à 60 MF.*

A3 - Evénements naturels : Il s'agit des événements naturels d'origine externe au système : inondation, tempête, cyclone, ouragan, vent, poids de la neige sur les toitures, foudre, grêle, avalanche, coulée de boue, glissement de terrain, phénomènes sismiques et volcaniques, etc.

NB : Certains événements peuvent figurer en A1. Sont donc considérés en A3, ceux exceptionnels qui ne sont pas indemnisés au titre de A1.

***Banque** : Dégâts des eaux dans les locaux techniques de l'informatique suite à une inondation "catastrophique naturelle". Le matériel endommagé est évalué à 6 MF, les frais supplémentaires à 4 MF et les pertes d'exploitation à 8 MF (arrêt une semaine).*

A4 - Perte de services essentiels : Il s'agit de l'ensemble des causes d'origine externe entraînant l'indisponibilité ou le dysfonctionnement (non conformité aux fonctionnalités et performances nominales) total ou partiel du système :

- . électricité, télécommunications, eau,
- . fluides divers,
- . fournitures spécifiques.

***Finance** : L'explosion d'une centrale thermique en région parisienne, produisant également de l'eau glacée pour le refroidissement d'une centaine de systèmes, a privé ceux-ci de climatisation pendant plusieurs semaines, entraînant des arrêts de fonctionnement dont le total des conséquences dépasse 50 MF.*

A5 - Autres risques accidentels :

Physiques : Il s'agit de l'ensemble des causes d'origine interne ou externe au système endommagé qui ont conduit à son endommagement accidentel total ou partiel :

- . chocs, collisions, chutes,
- . introduction de corps étrangers solides, liquides, gazeux ou mixtes, ayant des actions physiques ou chimiques (y compris pollution),

- . bris de machine accidentels de type mécanique, électrique, électronique, électromagnétique,
- . pollution par rayonnement (thermique, électromagnétique, nucléaire, etc.), effets électrostatiques, etc.

12. ERREURS

E1 - Erreurs d'utilisation (logiques) : Erreurs de saisie et transmission des données quelqu'en soit le moyen, erreurs d'exploitation du système.

Assurance : Erreurs de transmission en chaîne, pendant plusieurs semaines, sans détection, de la télésauvegarde des fichiers de base. C'est essentiellement le fichier des contrats automobiles qui a été touché. Sa reconstitution a pu être faite à partir d'une sauvegarde ancienne (trois mois) à haute protection et de la collecte d'informations complémentaires (qui a duré deux mois). La perte d'exploitation due au retard de quittance est de 4 MF.

E2 - Erreurs de conception et de réalisation de logiciels et procédures d'application.

Assurance : Erreur de conception d'un logiciel d'optimisation des placements financiers, conduisant à une perte de fonds de 20 MF en deux mois (temps de fonctionnement avant détection de l'anomalie).

13. MALVEILLANCE⁹

M1 - Vol de matériels principaux ou accessoires
Vandalisme sur le matériel.

Services : Vol de matériel (la plus grande partie des micro-ordinateurs et machines de traitement de texte) dans un cabinet de services juridiques et fiscaux (CA annuel 8 MF) en une seule nuit : dommages matériels évalués à 0,5 MF et dommages immatériels évalués à 0,3 MF plus 2 MF en responsabilité civile.

M2 - Fraude : Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice évaluable monétairement pour la victime, essentiellement formé par le détournement de biens au profit du criminel :

- . détournement de fonds (direct ou indirect),
- . détournement de biens ou services matériels ou immatériels (direct ou indirect),
- . les attaques ciblées vers une entreprise pour récupérer des informations ou modifier des dispositifs en vue d'opérer ultérieurement une autre opération malveillante (par exemple de type M4).

Banque : Un cadre ayant autrefois travaillé au service informatique, entre sur écran une série d'écritures, dont le compte d'origine est "Réserves" et le compte d'aboutissement est un numéro de compte personnel dans une banque étrangère. Les opérations sur réserves sont rejetées en anomalies dans un fichier d'attente, afin d'être ultérieurement recyclées. Le fraudeur utilise alors une chaîne de recyclage batch, normalement employée en mode dégradé dans le cadre du plan de secours. Cette chaîne, ancienne, n'est pas à jour, et les écritures passent. Ce n'est que le lendemain, lors du contrôle quotidien, que l'anomalie est identifiée. Les mouvements de fonds ont déjà été réalisés pour 7,5 MF.

⁹ Toutes actions commises directement ou indirectement par des personnes intérieures ou extérieures à l'entreprise ou à l'organisme concerné, y compris actions commises à l'occasion d'émeutes ou de mouvements populaires, les actes de terrorisme et de guerre étrangère.

Industrie : Modification des programmes de facturation de quelques gros clients en deux temps : mise à zéro du prix de certains produits sur la première facture ; puis envoi d'une seconde facture (non comptabilisée), avec la mention "régularisation par virement au compte..." portant sur les produits facturés zéro. Le compte "produits à facturer" était soldé par la première facture. La différence était récupérée sur le compte de l'informaticien fraudeur. La fraude a été stoppée à la quatrième facture, pour un montant de 3,5 MF.

M3 - Sabotage : Attentat, vandalisme, action malveillante conduisant à un sinistre matériel (type A1 ou A2).

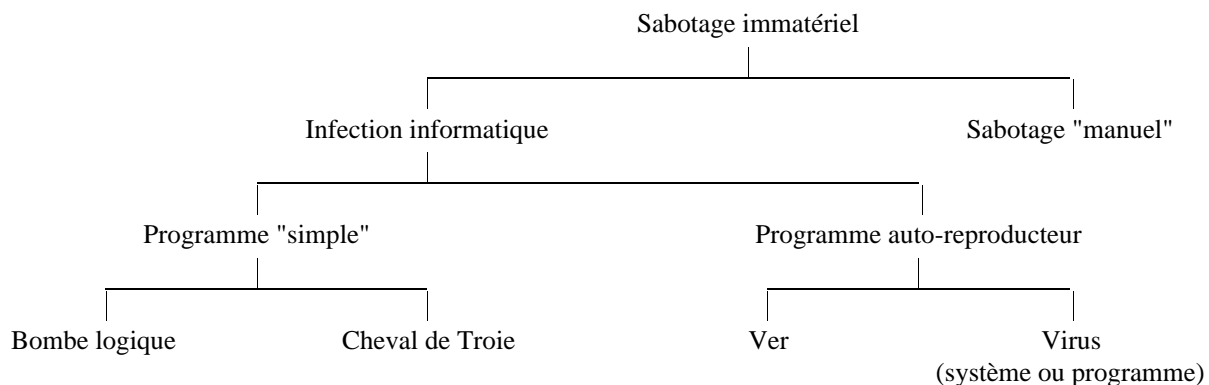
Banque : Sabotage physique d'une trieuse de chèques très spécialisée (5 MF). Le retard de traitement (transfert vers un centre régional) a entraîné environ 2 MF de pertes supplémentaires. Le budget informatique annuel de cette banque est de l'ordre de 45 MF).

M4 - Attaque logique : Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice au moins qualitatif pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant le plus souvent un profit indirect pour le criminel et/ou le commanditaire éventuel (sabotage immatériel, infection informatique, programme "simple", bombe logique, cheval de Troie, sabotage "manuel", programme auto-reproducteur, ver, virus (système ou programme)).

Cette rubrique se subdivise en deux catégories :

- les attaques non ciblées (comme les virus) qui représentent l'immense majorité des attaques en nombre, mais avec un impact modéré,
- les attaques ciblées vers une entreprise (bombe logique, manipulation de données ou de programmes, etc.) dans le but de la paralyser au moins momentanément. Ces attaques sont très peu nombreuses, mais leur impact est très élevé.

Crédit : Destruction de tous les fichiers et tous les programmes, ainsi que des sauvegardes d'une mutuelle. La reconstitution des données faite à partir des archives et d'un appel aux sociétaires a coûté 20 MF. La reconstitution des programmes, qui a duré onze mois, a coûté 75 MF. Les autres faits supplémentaires, pertes d'exploitation et pertes de clientèle sont estimés à environ 155 MF.



M5 - Divulgaration : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles¹⁰.

Distribution : Copie du fichier fournisseur au profit d'un concurrent (collusion d'un informaticien de la société avec un concurrent). Ce dernier a pu obtenir des fournisseurs avec lesquels il avait de moins bonnes conditions une mise à niveau et ainsi gagner environ 0,4 point de marge. Il a pu alors pratiquer une attaque de

¹⁰ S'il s'agit d'un vol de données, avec pertes de celles-ci par la victime, il y a combinaison de M5 avec M4 ou M1.

son concurrent sur les produits pour lesquels celui-ci était moins bien placé. La perte en un an est estimée à 45 MF et il est possible que l'entreprise ne puisse survivre (CA annuel de l'hypermarché : 400 MF).

M6 - Autres¹¹.

Industrie : Suite à un conflit avec la direction, départ de la presque totalité de l'équipe informatique d'un petit centre. Les pertes d'exploitation dues à l'impossibilité d'exploiter et de corriger les programmes par manque de documentation, même avec l'aide de personnes compétentes extérieures, ont été évaluées à plus de 2 MF (soit le budget informatique annuel de cette entreprise).

2 - LES CONSEQUENCES

21. DIRECTES

211 - Matériels (C1) : Frais d'expertise, de déblaiement, de réparation ou de remplacement des matériels endommagés.

212 - Non-matériels (C2) : Frais d'expertise et de restauration des éléments non-matériels du système atteint : système d'exploitation, données, programmes, procédures, documentations et divers.

NB : Tous les frais de reconstitution, quelle que soit leur ampleur (liée par exemple à l'insuffisance de sauvegardes), sont conventionnellement comptabilisés en C2.

22. INDIRECTES

221 - Frais supplémentaires (C3) : Ensemble des frais correspondant à des mesures conservatoires destinées à maintenir pour le système des fonctionnalités et performances aussi proches que possible de celles qui étaient les siennes avant le sinistre jusqu'à remise en état (matériel et non-matériel).

Pertes d'exploitation : Pertes de marge dues à des frais supplémentaires et/ou à des pertes de revenu directes ou indirectes (pertes d'affaires, de clients, d'image, etc.).

222 - Pertes de fonds et de biens (C4) :

- pertes de fonds ou de biens physiques,
- pertes d'informations confidentielles, de savoir-faire, etc.,
- pertes d'éléments non reconstituables du système (essentiellement données ou programmes) évalués en valeur patrimoniale.

223 - Responsabilité civile (C5) encourue par l'entreprise ou l'organisme du fait des préjudices causés à autrui, volontairement ou pas, du fait de la survenance d'un sinistre dans son enceinte juridique.

224 - Autres pertes (C6) :

- Pertes spéciales (utilisation non autorisée de ressources et copie illicite de logiciels).
- Qualitatives, réglementaires, déontologiques, etc.

EVAL96.DOC

¹¹ Sont répertoriés à titre estimatif global les types de risques suivants :

- grèves,
- pertes ou indisponibilité de personnel,
- contrefaçon de logiciels.