ESTIMATION DES PERTES ET CONSEQUENCES ECONOMIQUES DUES A DES SINISTRES INFORMATIQUES EN FRANCE

France, 1992

CLUSIF **Date de publication : 1993**

TABLE DES MATIERES

PRESENTATION

L'APSAD[1], puis le CLUSIF[2], ont mis en place depuis 1983 un observatoire de la sinistralité des risques informatiques, permettant d'évaluer grossièrement l'impact économique[3] et plus encore son évolution dans le temps (à méthode d'évaluation constante).

Cette évaluation qui doit être considérée avec précaution, ne concerne que le secteur non-gouvernemental, et uniquement vis-à-vis des conséquences économiques immédiatement exposables[4]. Il est clair qu'il existe d'autres conséquences[5], 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 1992, selon les causes.
2. Estimation des pertes dues à des sinistres informatiques en France, en 1992, selon les conséquences.
3. Commentaire sur la situation et l'évolution 1992 / 1991.
4. Evolution de la sinistralité sur les dix dernières années.
5. Tendances.
6. Annexe (définitions).

[1] Assemblée Plénière des Sociétés d'Assurances Dommages, 26, boulevard Haussmann -75009 PARIS.
[2] Club de la Sécurité Informatique Français, 30 rue Pierre Sémard -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, « privacité », vie humaine, etc.

Grille harmonisée européenne des risques informatiques (1)

1. ESTIMATION DES PERTES DUES A DES SINISTRES INFORMATIQUES (l) EN FRANCE EN 1994 (2) SELON LES CAUSES (3)

Conséquences / Types de risques	DIRECTES		INDIRECTES				TOTAL
	C1 Matériel	C2 Non-matériel	C3 Frais supplémentaires et pertes d'exploitation	C4 Pertes de patrimoine	C5 Responsabilité civile	C6 Divers	
Accidents							
A1 - Physiques (incendie, Explosion, Dégât des eaux, Pollution, etc.)	350	10	860		100		1 320
A2 - Pannes		50	850		50		950
A3 - Force majeure (événements naturels)	40		80				120
A4 - Perte de services essentiels (Télécom, électricité, eau, etc.)		10	200		20		230
A5 - Autres							
Erreurs							
E1 - Erreurs d'utilisation	10	60	600	50	220		940
E2 - Erreurs de conception et de réalisation	10	10	700	60	180		960
Malveillance							
M1 - Vol (physique)	110	10					120
M2 - Fraude (non physique)			50	1 450	50		1 550
M3 - Sabotage (physique)	0						0
M4 - Attaque logique (non physique)		550	330	120	50		1 050
M5 - Divulgation		10	130	700	60		770
M6 - Autres			130 (4)			2 300 (5)	2 430
TOTAL ►	**520**	**710**	**3 800**	**2 380**	**730**	**2 300**	**10 440**

(1) 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.

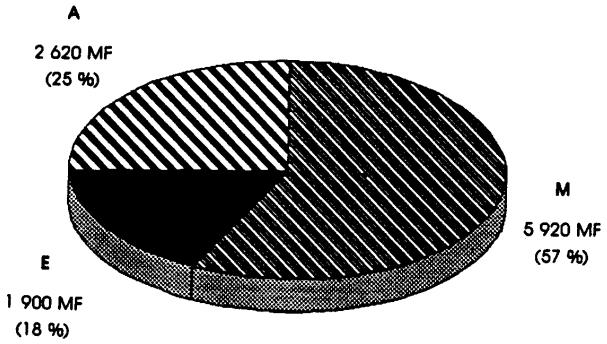
(2) Ensemble des systèmes informatiques, bureautique, télécommunication, matériel informatique et télécommunication annexe (serveurs, modems, processeurs, etc. hors téléphone et fax),

périphériques divers et spécialisés (incluant la robotique mais hors monétique et cartes à puces, calculettes, etc.).

(3) 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 %.

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

(5) Copie illicite de progiciels : 1 200
Utilisation non autorisée de ressources Informatiques : 1 100 (0.5 % Budget Informatique de la Nation).



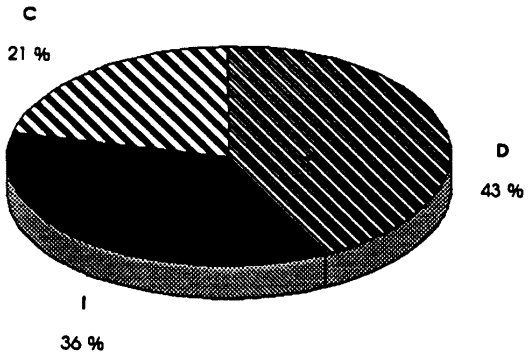
EVOLUTION 1992/1991

Types de causes	%
A (Accidents)	- 1,1
E (Erreurs)	+ 5,6
M (Malveillance)	+ 0,2
TOTAL ►	+ 0,8

2. LES CONSEQUENCES

Origine \ Destination	Disponibilité D	Intégrité I	Confidentialité C
A1	1 020	300	
A2	750	190	10
A3	90	30	
A4	220	10	
A5			
*** A	2 080	530	10
E1	300	640	
E2	430	510	20
*** E	730	1 150	20
M1	80	30	10
M2		1 500	50
M3	0		
M4	420	580	50
M5			770
M6	1 150 (6)		1 280 (6)
*** M	1 650	2 110	2 160
TOTAL ▶	4 460	3 790	2 190

(6) Rangement relativement arbitraire.



EVOLUTION 1992/1991

Types de conséquences	%
D	+ 0,5
I	- 0,8
C	+ 4,8
TOTAL ▶	+ 0,8

3. COMMENTAIRES

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 source étant l'Assurance). D'autres estimations croisées (en ligne et en colonne) portent directement sur les tendances « à dire d'expert ».

A) Accidents

Il y a eu une forte baisse des sinistres de plus de 1 MF en 1992 ce qui différencie cette catégorie de risques des risques industriels en général où il y a eu une augmentation importante. Cette situation favorable est due au hasard plus qu'à l'efficacité des moyens de sécurité. En effet, 1992 a connu une baisse sensible des investissements et même de la maintenance des moyens de sécurité existants. On a eu en surcroît un accroissement élevé de phénomènes naturels (tempêtes et inondations pour l'essentiel) et une amélioration de la qualité des services essentiels,

B) Erreurs

Les chiffres ne sont pas directement comparables à ceux de 1991 car on a pris en compte les quelques dommages matériels induits par des erreurs. Pour le reste, la tendance est néanmoins à une légère hausse, qui est peut-être imputable au climat de crise chez les fournisseurs aussi bien que chez les utilisateurs.

C) Malveillance

La sinistralité est stable. On n'a pas constaté d'attentat. Le vol physique continue sa forte progression. Le phénomène marquant est la baisse importante de la fraude informatique (détournement de fonds et de biens), phénomène que l'on observe aussi dans d'autres domaines non informatiques, quoique de façon moins marquée. Les attaques logiques augmentent par contre significativement, en partie à cause de la masse des infections vraies qui créent des désordres; et en partie à cause d'attaques de systèmes centraux et de réseaux. Les ruptures de confidentialité augmentent assez considérablement et peuvent s'expliquer par l'exacerbation de la concurrence.

Annexe : DEFINITIONS

1. TYPES DE RISQUES

1.1 ACCIDENTS

AI -Incendie, explosion, implosion.

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.

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 A 1. Sont donc considérés en A3, ceux exceptionnels qui ne sont pas indemnisés au titre de Al.

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.

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.

1.2 ERREURS

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

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

1.3 MALVEILLANCE[6]

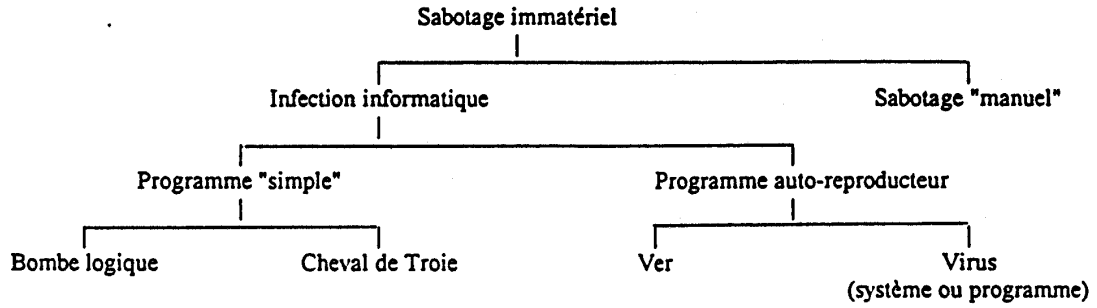
MI -Vol de matériels principaux ou accessoires.

[6] 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.

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,
- détournement de biens ou services (matériels ou immatériels).

M3- Sabotage : Action malveillante conduisant à un sinistre matériel (type Al ou A2).

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 :



M5 –Divulgation : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles[7].

M6 –Autres[8]

2 LES CONSEQUENCES

2.1 DIRECTES

2.1.1 Matériels (Cl) : Frais d'expertise, de déblaiement, de réparation ou de remplacement des matériels endommagés.

2.1.2 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 Cl.

2.2 INDIRECTES

2.2.1. 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.).

[7] S'il s'agit d'un vol de données, avec pertes de celles-ci par la victime, il y a combinaison de MS avec M4 ou Ml.
[8] Sont répertoriés à titre estimatif global les types de risques suivants :
- grèves,
- pertes ou indisponibilité de personnel,
- contrefaçon de progiciels.

2.2.2. 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.

2.2.3. Responsabilité civile (CS) 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.

2.2.4. Autres pertes (C6) :
- Pertes spéciales (utilisation non autorisée de ressources et copie illicite de logiciels).
- Qualitatives, réglementaires, déontologiques, etc.