EVALUATION DES CONSEQUENCES ECONOMIQUES

DES INCIDENTS ET SINISTRES RELATIFS

AUX SYSTEMES INFORMATIQUES

France, 1995

CLUSIF *Février 1996*

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).

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 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 1995, selon les causes.

2 - Estimation des pertes dues à des sinistres informatiques en France, en 1995, selon les conséquences.

3 - Commentaire sur la situation et l'évolution 1995/1994.

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, 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, "privacité", vie humaine, etc.

1 - ESTIMATION DES PERTES DUES A DES SINISTRES INFORMATIQUES(1) EN FRANCE EN 1995(2) SELON LES CAUSES(3)

Conséquences (4) / Types de risques(4)	DIRECTES C1 Matériel	DIRECTES C2 non-matériel	INDIRECTE C3 Frais supplémentaires et pertes d'exploitation	INDIRECTE C4 Pertes de patrimoine	INDIRECTE C5 Responsabilité civile	INDIRECTE C6 Divers	TOTAL
Accidents							
A1 - Physiques (incendie, Explosion, Dégâts des eaux, Pollution, etc.)	340	35	980		115		1 470
A2 - Pannes, dysfonctionnements		90	840		100		1 030
A3 - Force majeure (Evénements naturels)	60		40				100
A4 - Perte de services essentiels (Télécom., électricité, eau, etc.)		5	230		35		270
A5 - Autres							
Erreurs							
E1 - Erreurs d'utilisation		90	520	10	230		850
E2 - Erreurs de conception et de réalisation		90	730	10	170		1 000
Malveillance							
M1 - Vol, vandalisme (physique)	170	25	5				200
M2 - Fraude (non physique)			30	1 560	80		1 670
M3 - Sabotage (physique)	0						0
M4 - Attaque logique (non physique)		550	485	100	105		1 240
M5 - Divulgation		5		810	85		900
M6 - Autres			80 (5)			2 750 (6)	2 830
TOTAL	**570**	**890**	**3 940**	**2 490**	**920**	**2 750**	**11 560**

(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, calculettes, etc.).

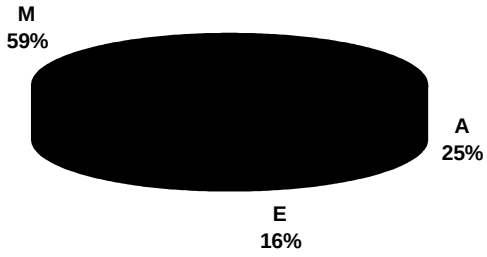
(2) Hors gouvernemental et administrations. Ces estimations qui correspondent à des ordres de grandeur établis à partir de la fraction des cas connus et des tendances sont plus ou moins précises selon les lignes et colonnes : globalement la précision est-elle même estimée à ± 30 %.

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

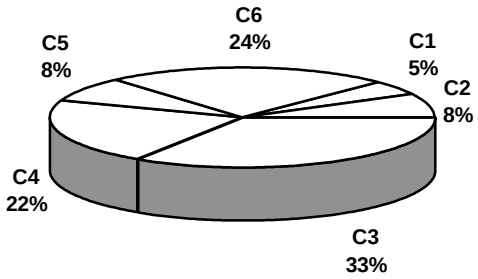
(6) - Copie illicite de progiciels (1 500). Cette évaluation, plus faible que celle des éditeurs de logiciels, repose sur une approche marginale des coûts que nous jugeons plus juste.
- Utilisation non autorisée de ressources informatiques : 1 250 (0,5 % Budget Informatique de la Nation).



Types de causes	%
A (Accidents)	+ 2,5
E (Erreurs)	=
M (Malveillance)	+ 4,4
TOTAL	**+ 3,25**

EVOLUTION 1995/1994

2 - LES CONSEQUENCES



Types de conséquences économiques	
C1	- 1,7 %
C2	- 2,2 %
C1 + C2	- 2,0 %
C3	+ 3,7 %
C4	+ 0,4 %
C5	+ 10,8 %
C6	+ 5,8 %
C3 + C4 + C5 + C6	+ 4,0 %
TOTAL	**+ 3,25 %**

Définitions :

Disponibilité (D) : Aptitude d'un système d'information a 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.

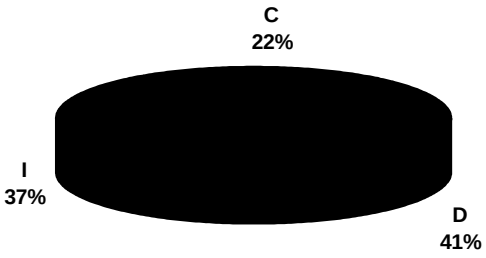
Confidentialité (C) : Propriété qui assure que seuls les utilisateurs habilités dans les conditions normalement prévues ont accès aux informations.

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

Destination / Origine	Disponibilité D	Intégrité(1) I	Confidentialité C
A1	1 170	300	
A2	760	260	10
A3	100	0	
A4	260	10	
A5			
*** A	2 290	570	10
E1	150	700	
E2	430	550	20
*** E	580	1 250	20
M1	190		10
M2		1 670	
M3	0		
M4	445	730	65
M5			900
M6	1 230 (2)		1 600 (7)
*** M	1 865	2 400	2 575
TOTAL	4 735	4 220	2 605

(1) Incluant l'imputabilité (W).

(2) Rangement relativement arbitraire.



Types de conséquences directes	%
D	+ 2,0
I	+ 3,6
C	+ 4,8
TOTAL	**+ 3,25**

EVOLUTION 1995/1994

3 - COMMENTAIRE SUR LA SITUATION ET L'EVOLUTION 1995/1994

A) Accidents

La sinistralité continue d'augmenter, à un rythme moins soutenu. Il y a moins de grands sinistres, mais la fréquence des sinistres petits et moyens continue d'augmenter considérablement. L'augmentation continue de la micro-informatique, "stand alone", en réseau, et portable, explique en partie le mouvement. Le relatif désinvestissement en sécurité physique (dispositifs et surtout tests et entretien des dispositifs) accentue la situation de risque. L'ambiguïté des positions concernant les installations d'extinction automatique au gaz en substitution du halon, joue également dans le mauvais sens.

Pour la catégorie A1, ce sont les pertes indirectes qui augmentent significativement : l'informatique concerne des applications de plus en plus stratégiques et intégrées, les entreprises travaillent de plus en plus en flux tendus, de nouveaux secteurs sont de plus en plus concernés dans l'industrie, la distribution, le transport, la santé, les services, etc., il s'agit de plus en plus d'applications décisionnaires. La catégorie RC augmente significativement, liée aux exigences des contrats de services aux tiers, notamment en FM et en secours.

Les moyens de secours et de sauvegarde continuent à progresser très favorablement sur les grandes et moyennes-grandes installations, mais le problème se déplace du fait de l'informatique répartie. (Il y a encore fort peu d'offres et de réalisations valables en mode client/serveur).

Les conséquences de pannes augmentent également très significativement, notamment en conséquences directes, et plus particulièrement en RC. En revanche, les sinistres "cat nat" ont baissé, mais on sait que l'aléa est important. Les pertes liées aux pertes de services sont en faible croissance : les phénomènes liés à l'eau de refroidissement (importants en 1994, notamment du fait de l'explosion de la centrale de Nanterre et de la sécheresse) et aux coupures d'électricité, ont chuté de plus de 50 % en 1995. En revanche, les conséquences d'inconsistances ou de pannes de télécommunication ont fortement augmenté, malgré les efforts des opérateurs : la qualité et les moyens de continuité s'améliorent, mais les conséquences sérielles sont de plus en plus graves (les entreprises ont peu réfléchi et peu investi en matière de continuité et secours télécom). Notons que la part RC est encore faible, mais la déréglementation de 1998, pourrait entraîner, en même temps que le développement des EDI, une très forte augmentation de ce poste. Les conséquences des pertes d'autres services (papier, supports magnétiques, optoélectroniques, cartes, etc.) ont également progressé.

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 continue 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 performancielles. Ici encore les SSII en subissent souvent le contrecoup en RC.

C) Malveillance

L'augmentation du vol est très forte, mais cependant moindre qu'au Royaume-Uni ou en Allemagne. Une partie des vols tient à la pénurie actuelle de composants sur le marché européen. Pour le reste, il s'agit pour l'essentiel de vol par le personnel, et à usage restreint (un quart environ), et de plus en plus de vols organisés pour revente au "marché gris" (trois quarts environ). Marginalement, il y a une fraction de vols visant le contenu des disques durs (dont l'accès et le contenu sont souvent mal protégés).

La fraude progresse à un rythme moindre que par le passé. Le détournement de fonds est pratiquement stable, avec une stabilité pour le secteur financier (baisse pour les banques, augmentation pour l'assurance, la prévoyance et les organismes financiers), une légère augmentation pour le secteur industrie-énergie-BTP, et une augmentation plus importante pour le secteur des services (notamment distribution, transport, loisirs, santé, etc.). En revanche, le détournement de biens progresse de plus en plus rapidement, notamment dans les établissements commerciaux. Les types d'attaques sont simples - profitant de failles existantes et d'opportunités - dans la très grande majorité des cas. Des personnels de l'entreprise concernée sont souvent impliqués (deux tiers des cas), avec des chaînes de collusion intérieur/relais extérieurs d'autant plus importantes que l'enjeu est élevé. Le rôle "d'officines d'intermédiation" et de la criminalité organisée se font de plus en plus sentir.

Il n'y a pas eu de sabotage physique (hors vandalisme) en 1995, mais l'aléa existe. Les attaques logiques continuent à se développer. Le poids de ces conséquences augmente pour la part micro/LAN et passe aux environs de 35 %, contre 65 % pour les grands systèmes/WAN. Les attaques de première catégorie sont non ciblées, alors que celles de la deuxième le sont, essentiellement motivées par la concurrence. Les actions correspondantes sont peu nombreuses (quelques dizaines de cas), mais avec des conséquences unitaires très élevées.

4 - EVOLUTION DE LA SINISTRALITE EVALUEE ENTRE 1984 ET 1994 (en francs courants)[6]

	1984	1994		1984	1994	t %/an
A	1 770	2 800	A1 - Physiques	740	1 430	+ 6,8
			A2 - Pannes	900	970	+ 0,8
	t = + 4 %/an		A3 - Force majeure	50	140	+ 10,8
			A4 - Perte de services essentiels	80	260	+ 12,5
E	2 030	1 850	E1 - Erreurs d'utilisation	1 480	900	- 9,5
	t = - 1 %/an		E2 - Erreurs de conception et de réalisation	550	950	+ 5,6
M	2 200	6 550	M1 - Vol (physique)	10	170	+ 32,7
			M2 - Fraude (non plysique)	700	1 620	+ 8,7
			M3 - Sabotage (physique)	40	-	NS
	t = + 10 %/an		M4 - Attaque logique (non plysique)	350	1 200	+ 13,1
			M5 - Divulgation	200	860	+ 15,7
			M6 - Autres	900	2 700	+ 11,6
TOTAL	6 000	11 200				
	t = + 6 %/an					

[6] t est le taux moyen de variation annuelle.

	1984	1994
A	29 %	25 %
E	34 %	17 %
M	37 %	58 %

Ventilation par cause

	1984	1994
D	53 %	41 %
I	30 %	37 %
C	17 %	22 %

Ventilation par conséquence primaire

Pertes	1984	1994
Directes (matériel et non-matériel)	12,7 %	13,3 %
Frais supplémentaires et PE	47,8 %	34,0 %
Pertes de patrimoine	20,7 %	22,1 %
Responsabilité civile	3,8 %	7,4 %
Divers	15,0 %	23,2 %

Ventilation par conséquence économique

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 1984, 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	103	+
A2 - Pannes	109	+ +
A3 - Force majeure	90	#
A4 - Perte de services essentiels	110	+
E1 - Erreurs d'utilisation	105	•
E2 - Erreurs de conception et de réalisation	112	+
M1 - Vol (physique)	120	+ +
M2 - Fraude (non physique)	110	+
M3 - Sabotage (physique)	-	#
M4 - Attaque logique (non physique)	111	+ +
M5 - Divulgation	115	+ +
M6 - Autres	NS	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 remanence 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 1993 ; estimation à dire d'experts.

[8] Légende :

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

EVOLUTION GLOBALE DU NIVEAU DE SECURITE

(Référence : Enquête Clusif 95/Enquête Clusif 94)

Rappel : Les cotations, comprises entre 0 (nul) et 4 (excellent) résultent de l'application des questionnaires d'audit Marion, au niveau d'assurance qualité A1.

Facteur	Libellé	Cotation 1994	Enquête 1995	Ecart
	L'appréciation générale de la sécurité			
101	L'organisation générale	2.06	2.08	+ 0.02
102	Les contrôles permanents	2.29	2.31	+ 0.02
103	La réglementation et l'audit	2.21	2.21	-
	Les facteurs socio-économiques			
201	Les facteurs socio-économiques	2.84	2.72	- 0.12
	Les principes généraux de la sécurité			
	Sécurité physique			
301	L'environnement de base	1.51	1.49	- 0.02
302	Le contrôle d'accès physique	1.91	1.93	+ 0.02
303	La pollution	1.99	1.94	- 0.05
304	Les consignes de sécurité physique	2.32	2.21	- 0.11
305	La sécurité spécifique incendie	2.40	2.30	- 0.10
306	La sécurité spécifique dégâts des eaux	1.34	1.34	-
307	La fiabilité de fonctionnement des matériels informatiques	2.35	2.33	- 0.02
	Sécurité de l'organisation informatique			
308	Les systèmes et procédures de secours	1.75	1.80	+ 0.05
309	Les protocoles utilisateurs-informaticiens	2.10	2.12	+ 0.02
310	Le personnel informatique	2.45	2.49	+ 0.04
311	Les plans informatique et de sécurité	2.70	2.42	- 0.28
	La sécurité logique et télécommunications			
401	La sécurité logique de base	2.51	2.56	+ 0.05
402	La sécurité des télécommunications	1.97	2.17	+ 0.20
403	La protection des données	2.06	2.10	+ 0.04
	La sécurité de l'exploitation			
501	L'archivage/désarchivage	1.67	1.60	- 0.07
502	La saisie et le transfert des données	1.80	1.78	- 0.02
503	La sauvegarde	2.58	2.78	+ 0.20
504	Le suivi de l'exploitation	2.59	2.60	+ 0.01
505	La maintenance	2.75	2.40	- 0.35
	La sécurité des études et réalisations			
601	Les procédures de recette	1.77	1.78	+ 0.01
602	Les méthodes d'analyse-programmation	2.55	2.51	- 0.04
603	Les contrôles programmés	1.64	1.66	+ 0.02
604	La sécurité des progiciels	1.79	1.97	+ 0.18
	Ensemble	2.15	2.17	+ 0.02

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** : Hyperdessication 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 faire 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 quittancement 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. MALVEILLANCE[9]

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

***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.*

***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.*

---

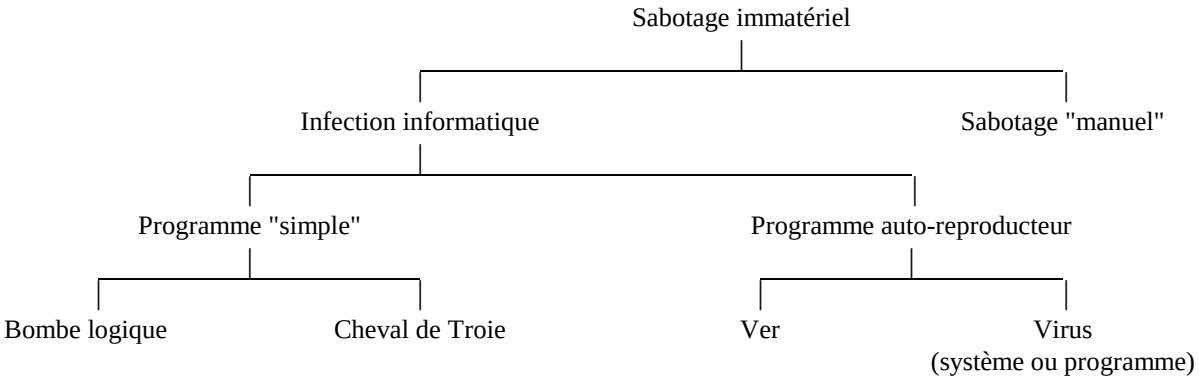
[9] Toutes actions commises directement ou indirectement par des personnes intérieures ou extérieures à l'entreprise ou à l'organisme concerné, y compris actions commises à l'occasion d'émeutes ou de mouvements populaires, les actes de terrorisme et de guerre étrangère.

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)).

***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 fais supplémentaires, pertes d'exploitation et pertes de clientèle sont estimés à environ 155 MF.*



M5 - Divulgation : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles[10].

***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 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 - Autres[11].

***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).*

---

[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.

[11] Sont répertoriés à titre estimatif global les types de risques suivants :
- grèves,
- pertes ou indisponibilité de personnel,
- contrefaçon de progiciels.

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.