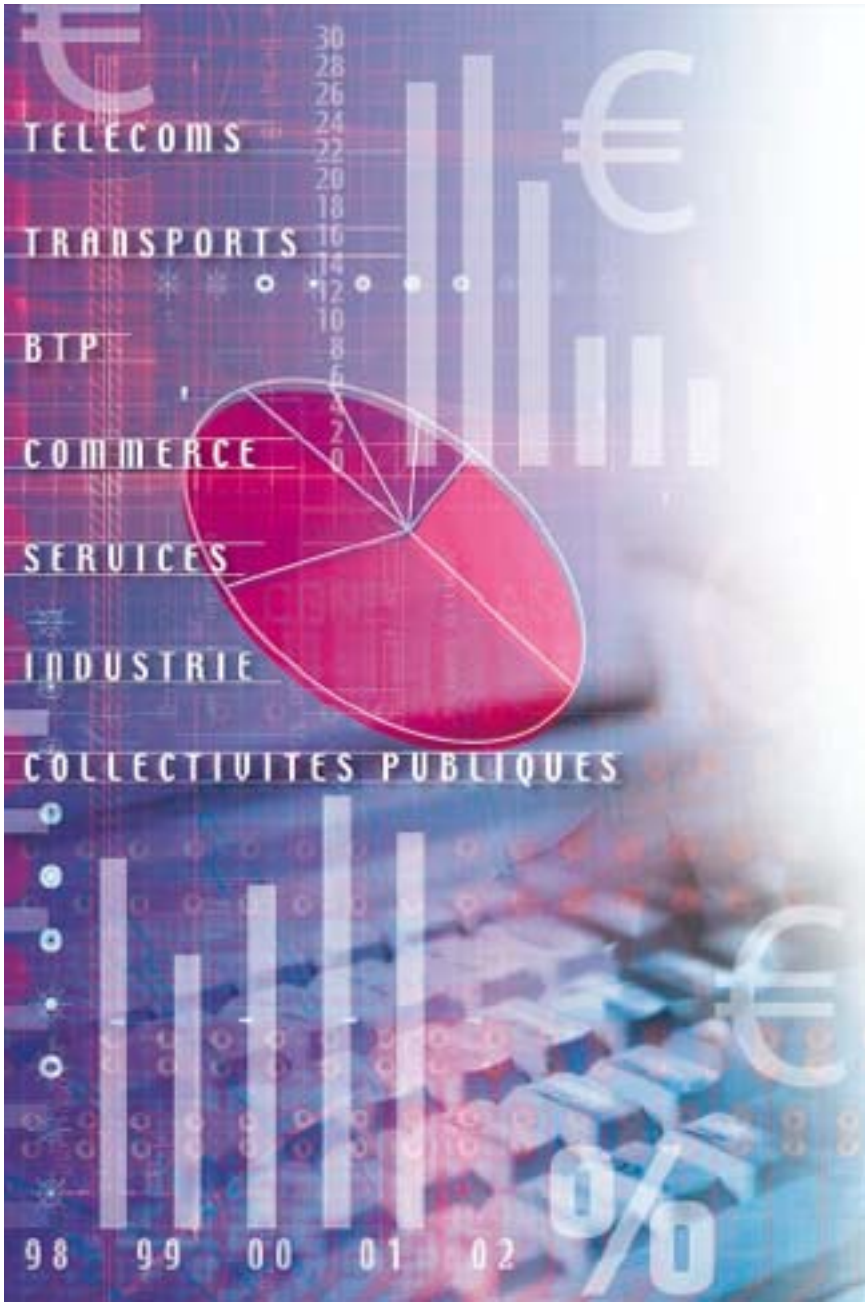
CLUSIF

Étude et statistiques sur la sinistralité informatique en France

Année 2002



Club de la Sécurité des Systèmes d'Information Français

Enquête nationale réalisée pour le Clusif par le cabinet GMV Conseil

Table des Matières

Remerciements

Le comité d'experts

Le Clusif remercie les entreprises et les collectivités publiques qui l'ont fait bénéficier des compétences de leurs experts.

Ace Europe, Clusif	Pascal Lointier
Clusif	Marie-Agnès Couwez
DCSSI	Dominique Chandesris
DL Consultant	Daniel Lasserre
Expertel Consulting	Stéphane Surget Roué
IRCGN	Eric Freyssinet
La Poste	Jean Marc Misert
Le Monde Informatique	Philippe Rosé
Mission de liaison Gendarmerie à la DGPN	Joël Ferry

Le comité sinistralité

Le Clusif remercie les membres actifs qui ont permis la réalisation de cette étude.

Ace Europe, Clusif	Pascal Lointier
Clusif	Marie-Agnès Couwez
DL Consultant	Daniel Lasserre
Expertel Consulting	Stéphane Surget Roué
IBM	Muriel Collignon
Le Monde Informatique	Philippe Rosé
Molines Consultants	Gérard Molines
XP Conseil - Groupe Devoteam	Paul Grassart

Note de synthèse

Créé en 1984, le CLUSIF est un espace d'échanges ouvert à tous les acteurs de la Sécurité des Systèmes d'Information : utilisateurs finaux comme prestataires de services et fournisseurs de solutions en SSI. Cette diversité fait sa force en favorisant le développement de synergies. Tous les secteurs de l'économie française, public et privé, y sont représentés. Il compte aujourd'hui plus de 600 membres qui bénéficient de ses services.

Pour la troisième année consécutive, le CLUSIF dresse le bilan de la sinistralité informatique en France, année 2002.
L'échantillon a été établi à partir des réponses complètes de 600 entreprises - 6 secteurs d'activité - et de 100 collectivités publiques - 3 catégories -. Les comparaisons entre 2002 et 2001 ne portent que sur le secteur privé.

L'année 2002 a été marquée par deux grandes tendances :
◆ une accélération de l'ouverture des systèmes d'information.
Ce sont la messagerie électronique et l'accès internet généralisés qui enregistrent la plus grande progression. Les opérations de commerce en ligne font exception à cette ouverture.

◆ une forte augmentation des infections par virus.
D'une part, 60 % des entreprises déclarent n'avoir subi aucun sinistre et il semble évident que de nombreux incidents ne sont pas détectés. D'autre part, l'évaluation de ces sinistres est toujours très peu réalisée, d'où une faible visibilité sur les coûts financiers réels engendrés. Ainsi, sur quoi repose le sentiment d'impact faible ? Concernant les virus, ils ont un impact fort pour seulement 15 % des entreprises.

Si les moyens humains, organisationnels, techniques, sont globalement en augmentation, la conception et la mise en place d'une stratégie globale de sécurité restent encore trop marginales. A l'heure d'une ouverture marquante des systèmes et d'une dépendance forte, la prise de conscience des risques liés est insuffisante.

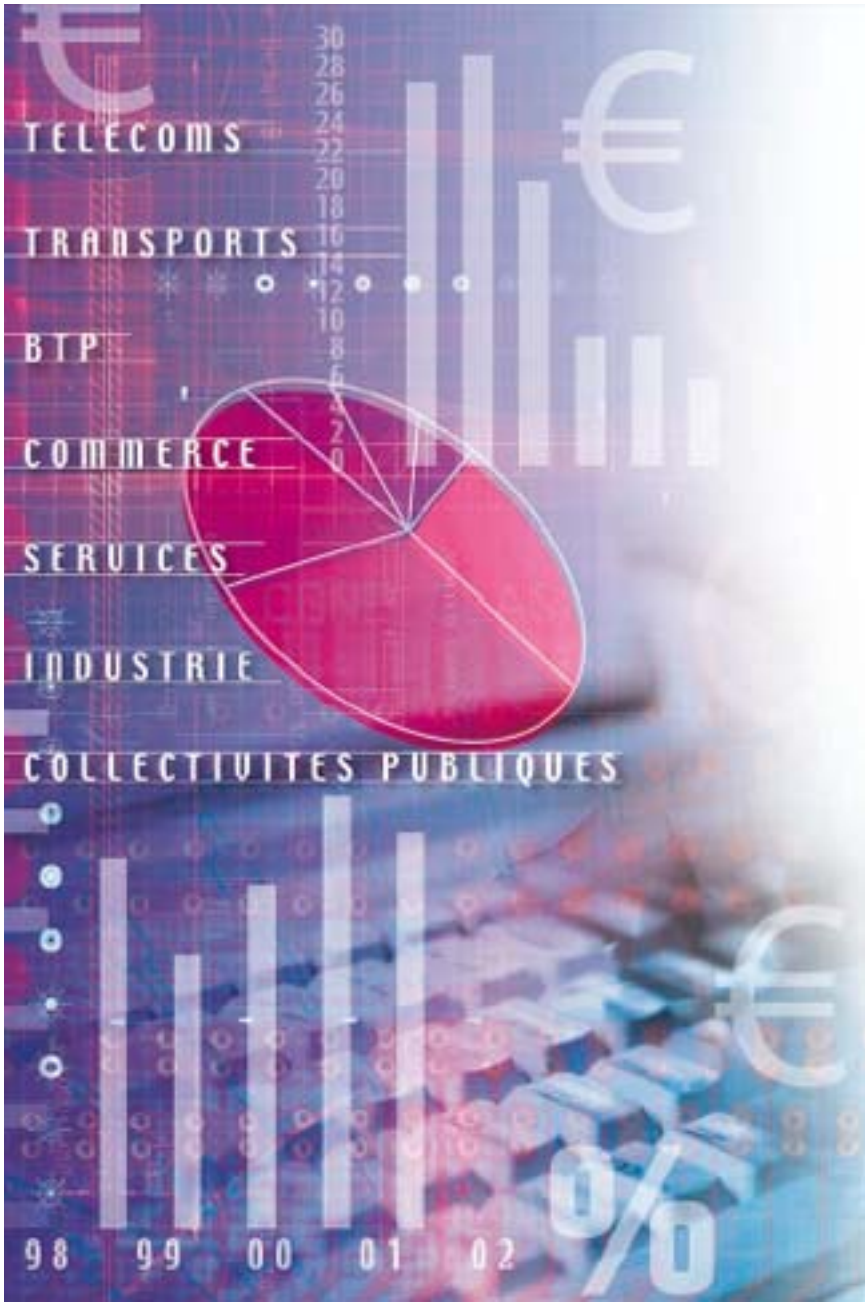
" Les entreprises forment, ne formalisent pas et contrôlent encore moins ".

Contrairement aux procédures de sauvegarde, très généralisées, les plans de secours et les plans de réaction restent toujours en retrait. Pourtant, en cas de sinistre grave, l'enjeu n'est plus la seule continuité d'un service informatique mais bien la pérennité de l'activité économique.

Le sentiment de protection déclaré par les entreprises est souvent en décalage par rapport à leur dépendance et aux moyens mis en œuvre. Les éléments qui peuvent expliquer ces résultats sont soit des délais dans le déploiement d'une politique de sécurité, soit une incohérence de démarche.

Le chemin est encore long pour passer d'un sentiment de confiance à une sécurité maîtrisée.
L'essor de la société numérique doit aller de pair avec une forte mobilisation de tous : décideurs, responsables techniques et opérationnels, utilisateurs finaux.

MÉTHODE D'ENQUÊTE



Méthode d'enquête

La méthode mise en place par le CLUSIF permet de réactualiser, chaque année plus finement, l'évaluation de la sinistralité informatique en France.

Ces études permettent :
◆ d'apprécier en terme de survenance, de récurrence et d'impact les sinistres informatiques suite aux accidents, erreurs et malveillances,
◆ de recenser les moyens mis en œuvre face à ces risques,
◆ de présenter une vision globale et les perspectives sur les besoins en sécurité.

Afin de les enrichir, le CLUSIF fait appel à des experts d'horizons variés, dont les commentaires sont intégrés et repérables par un encadré vert :

Exemple de commentaire d'expert

Ces études font partie intégrante de la mission de sensibilisation à la sécurité des systèmes d'information du CLUSIF.

Nouveautés 2002

Les évolutions principales concernent :
- la modification des questionnaires du secteur public et du secteur privé avec l'introduction de nouveaux items tels la mise en œuvre de chartes de sécurité, de contrats d'infogérance,
- l'augmentation du nombre de collectivités publiques répondantes de 31 à 100,
- la suppression du critère géographique, perçu comme non pertinent,
- la suppression de la mise en perspective de l'ensemble des données, les échantillons étant beaucoup trop différents.

Mode de recueil

Les données ont été recueillies sur la base d'un questionnaire adressé par fax, après avoir identifié par téléphone l'interlocuteur compétent.
Cette année, les réponses enregistrées directement par téléphone sont encore majoritaires, le niveau de confidentialité étant perçu comme supérieur au fax. D'autre part, les interviewés semblent préférer être accompagnés dans leur réponse à l'enquête compte tenu de la complexité relative de certaines questions. Le taux d'acceptation des entreprises du secteur des télécommunications a été beaucoup plus faible que celui des autres secteurs d'activité. Les collectivités publiques ont réservé un très bon accueil à l'étude avec un très faible taux de refus.

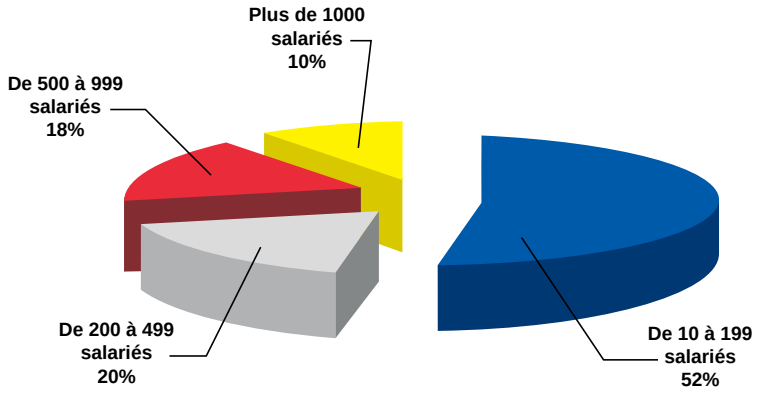
Caractéristiques de l'échantillon

L'échantillon a été constitué à partir de 600 réponses d'entreprises et de 100 réponses de collectivités publiques. Ces chiffres sous-entendent qu'environ 3000 entreprises ont été contactées et un peu moins de 300 collectivités publiques.
La part des collectivités publiques a été triplée pour cette étude, ce qui permet de disposer, pour la première fois, d'un échantillon minimum pouvant être redressé. *Les données qui ne franchissent pas la barre des 5 % en taux de réponse ne sont pas prises en compte, le résultat étant dans ce cas trop peu significatif. De plus, une variation annuelle inférieure ou égale à 5 % peut s'expliquer en partie par un écart statistique normal.*

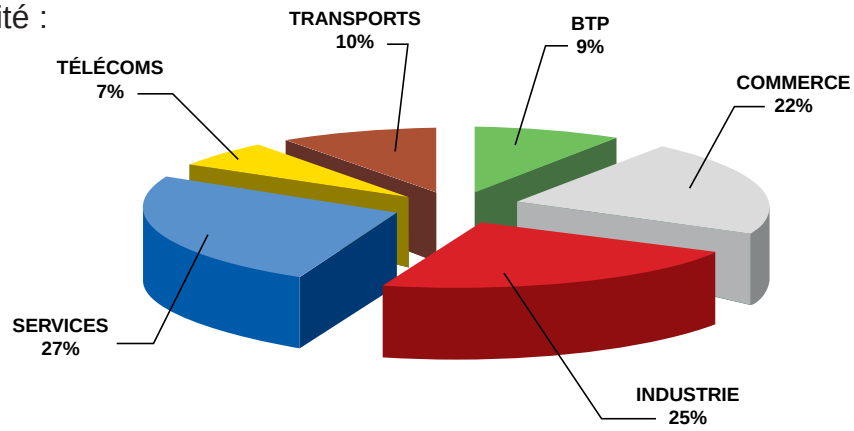
Entreprises

Sur la base de 600 entreprises de plus de 10 salariés, deux typologies ont été retenues, l'effectif et le secteur d'activité :

Répartition par effectif :



Répartition par secteur d'activité :



La majorité de ces entreprises ont un chiffre d'affaires inférieur à 7,6 M Euros (67 %) 28 % des entreprises de 200 à 499 salariés déclarent un chiffre d'affaires supérieur à 150 M Euros contre plus de 40 % au-delà de 500 salariés.

40 % des entreprises appartiennent à un groupe.

84 % n'ont qu'un seul site d'implantation en France et sont implantées à l'étranger à seulement 16 %.

A) Définition des domaines d'activité

Transports
Transports par voie terrestre, maritime, fluviale, aérienne (NAF 60 à 62)
Services auxiliaires des transports (NAF 63)
Télécommunications
Services des postes et télécommunications (NAF 64)
Industrie
Industries extractives (NAF 10 à 14)
Industries manufacturières (NAF 15 à 37)
Production et distribution d'électricité, de gaz et d'eau (NAF 40 et 41)
Commerce
Commerces y compris réparations d'automobiles et d'articles domestiques (NAF 50 à 52)
Services
Hôtels et restaurants (NAF 55)
Activités financières (NAF 65 à 67)
Immobilier, locations et services aux entreprises (NAF 70 à 74)
BTP
Construction (NAF 45)

B) Redressement de l'échantillon des entreprises

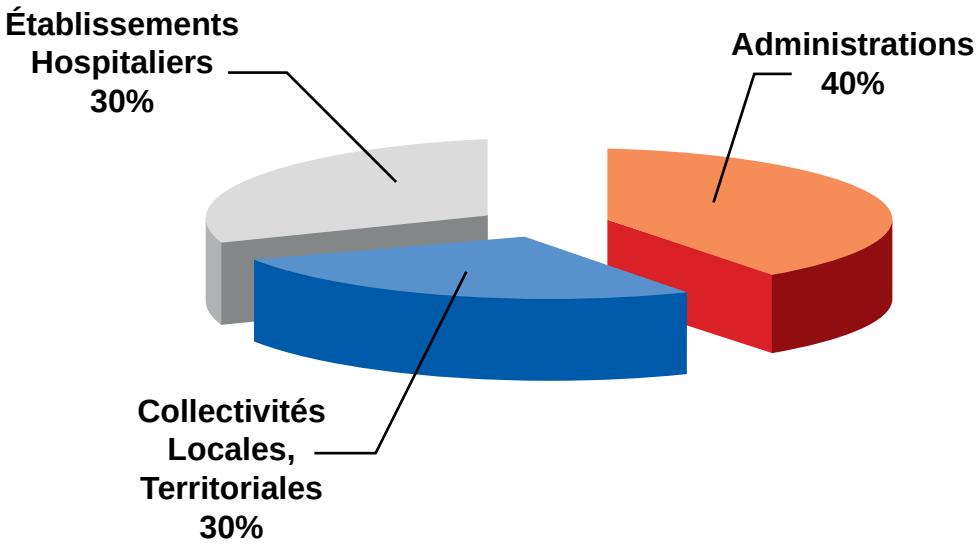
L'ensemble des données des entreprises a été redressé sur la base de la répartition réelle du nombre d'entreprises françaises, par effectif et par secteur d'activité, recensées dans les fichiers INSEE.

	De 10 à 199 salariés	De 200 à 499 salariés	De 500 à 999 salariés	Plus de 1.000 salariés	Total	Total en %		Données INSEE
BTP	41	10	4	1	56	9 %	⇨	12 %
COMMERCE	70	26	22	13	131	22 %	⇨	25 %
INDUSTRIE	65	39	33	15	152	25 %	⇨	25 %
SERVICES	72	28	41	20	161	27 %	⇨	27 %
TÉLÉCOMS	15	10	6	8	39	7 %	⇨	2 %
TRANSPORTS	53	6	1	1	61	10 %	⇨	9 %
Total	316	119	107	58	600			
Total en %	53 %	20 %	18 %	10 %				
⇩	⇩	⇩	⇩	⇩				
Données INSEE	96 %	2 %	1%	1 %				

N.B. Les parts respectives des petites entreprises et des secteurs d'activité dans l'économie française devront être gardés en mémoire pour mieux évaluer les résultats d'ensemble.

Collectivités publiques

Sur la base de 100 collectivités publiques, trois catégories ont été retenues :

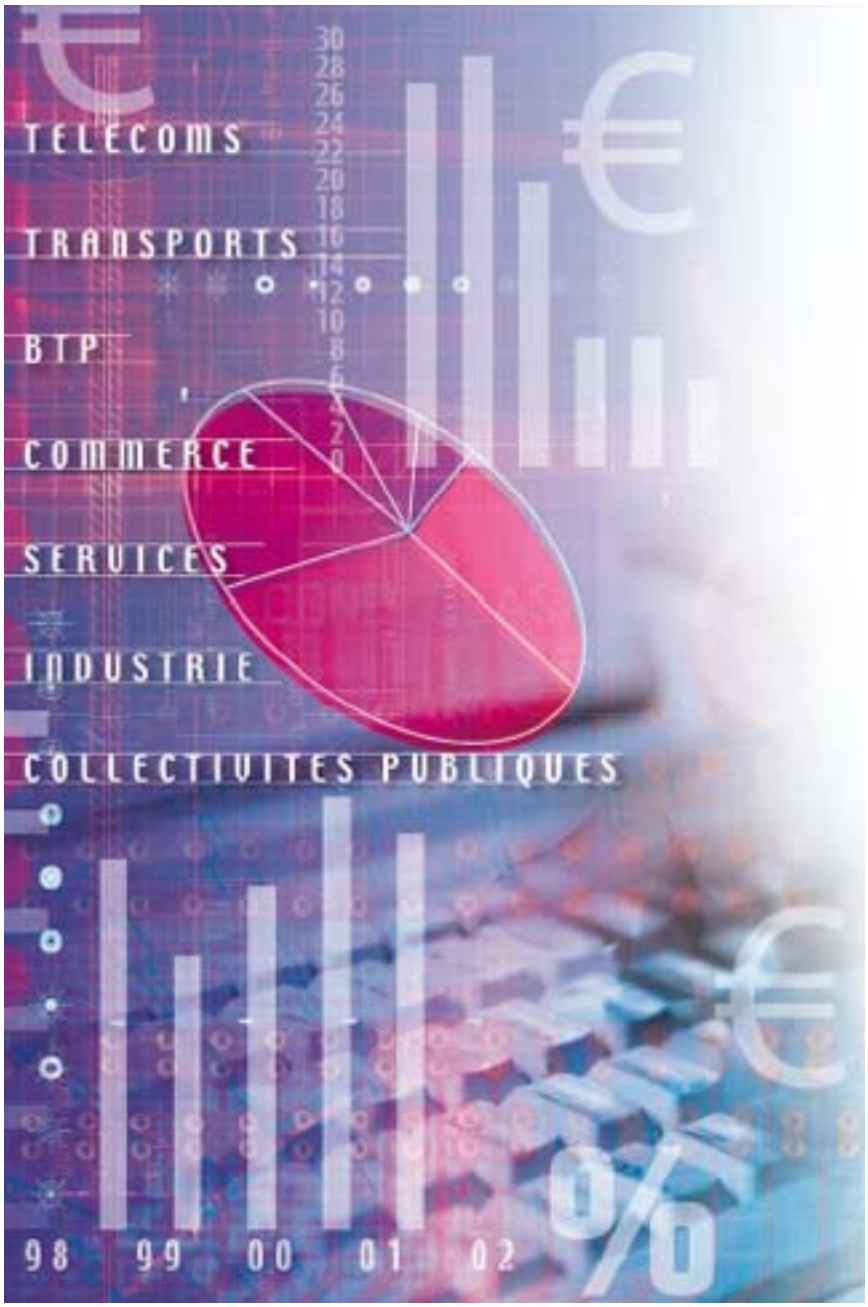


C) Redressement de l'échantillon collectivités publiques

Cet échantillon a été redressé sur la base des effectifs de la fonction publique.

	Total	Total en %		Effectifs de la Fonction Publique
Administrations	40	40 %	⇨	51 %
Collectivités locales, territoriales	30	30 %	⇨	30 %
Établissements hospitaliers	30	30 %	⇨	19 %
	100	100 %		100 %

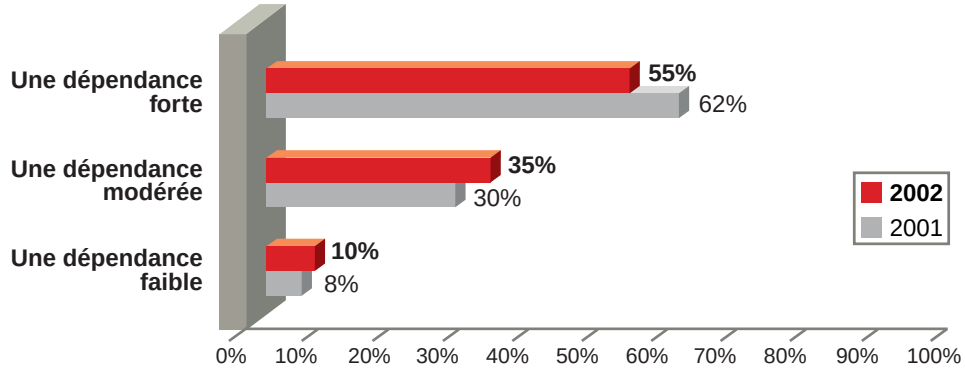
ENTREPRISES



Un sentiment de dépendance qui s'infléchit

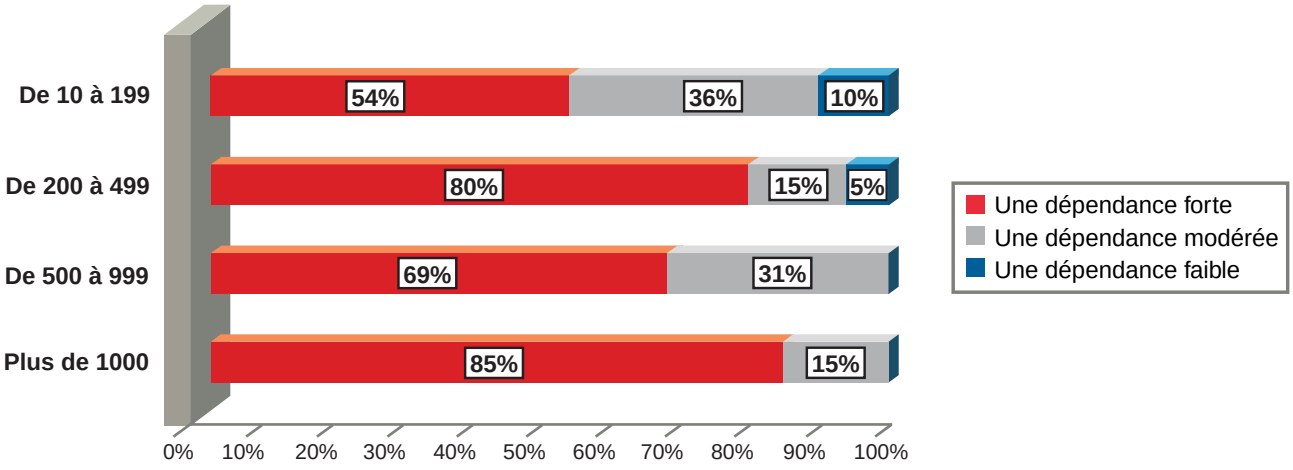
Si la dépendance faible annoncée reste toujours minoritaire, il est intéressant de constater que les entreprises annoncent une dépendance moins forte en 2002.

Elles considèrent avoir :



Dans une société de plus en plus numérique, la question se pose de savoir sur quels critères objectifs peut s'appuyer cet infléchissement.

L'analyse par effectifs fait ressortir des écarts importants :

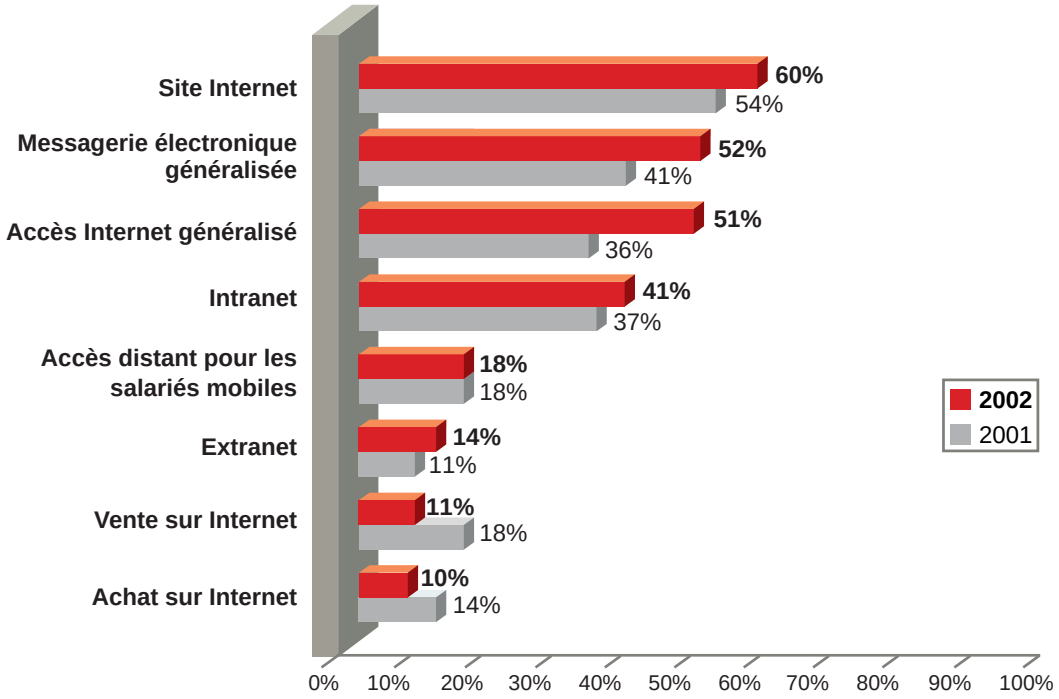


Les secteurs font apparaître une forte hétérogénéité dans la dépendance forte :

BTP, 33 %, Transports, 49 %, Industrie et Services, 53 %, Commerce, 67 % et Télécoms, 83 %.

Une ouverture en forte progression

A l'exception des opérations de commerce en ligne, l'ouverture des systèmes d'information progresse fortement en 2002 :



La baisse des ventes et achats sur Internet montre que la confiance en l'économie numérique ne s'est pas encore établie. Concernant les achats, seules les entreprises de plus de 1000 salariés se démarquent à 24 %. Ce chiffre s'explique par les commandes de masse et par la migration sur Internet des solutions d'EDI.

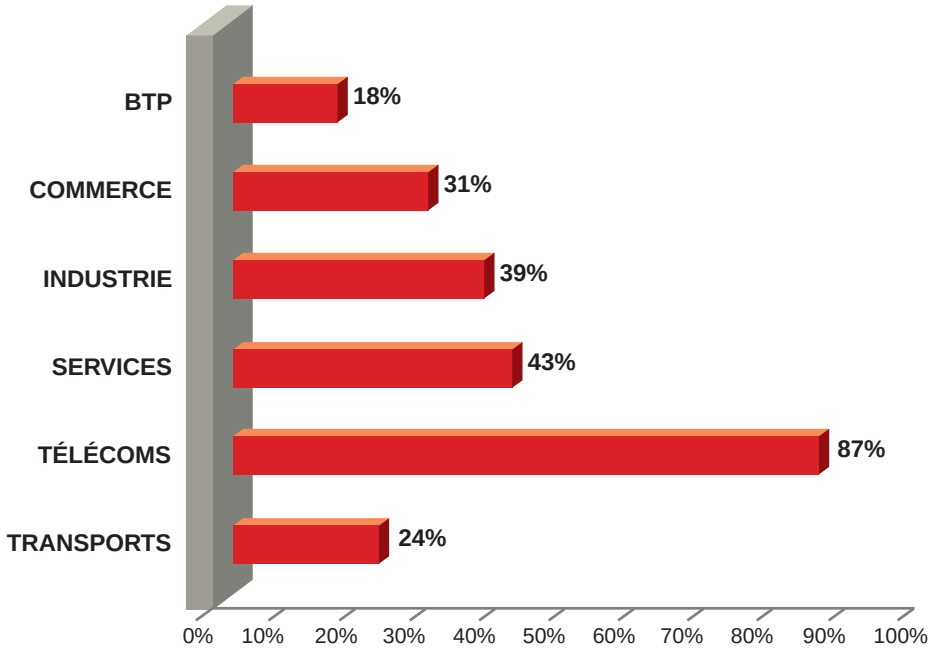
Cette ouverture est variable en fonction des effectifs et du secteur. Une scission très nette apparaît à partir de 200 salariés, avec 59 % de sites internet en deçà contre plus de 80 % au-delà. Les télécoms ont, en toute logique, une ouverture qui se démarque ; le BTP est en retrait concernant la messagerie électronique généralisée (35 %) et l'intranet (23 %).

Une politique de sécurité à renforcer

64 % des entreprises n'ont toujours pas défini de politique de sécurité des systèmes d'information. C'est donc 36 % d'entreprises qui ont réalisé cette démarche, ce qui est faible au regard des 55 % qui se déclarent fortement dépendantes. Malgré une légère augmentation par rapport à 2001 (30%), cette constatation montre le chemin qu'il reste à parcourir en la matière.

Certaines entreprises se sachant dépendantes n'intègrent pas la continuité de service. Les possibilités de cette absence de réaction peuvent être imputées à différents critères :
- une politique SSI est, ou semble, chère à mettre en place,
- les entreprises ont " du retard à l'allumage ",
- elles sont en phase de sensibilisation, la démarche s'amorce,
- la rédaction de la politique est en cours.
La comparaison avec la dépendance forte pose la question de savoir s'il s'agit d'inconscience managériale, de manque de temps ou de prise de risque pleinement et volontairement assumée.
De façon prospective, l'augmentation des audits de sécurité (cf. infra), qui servent bien souvent à la cohérence et au déploiement des plans de sécurité, peut laisser supposer une amélioration.

Parmi ces 36 % la répartition par secteurs d'activité expose des disparités :

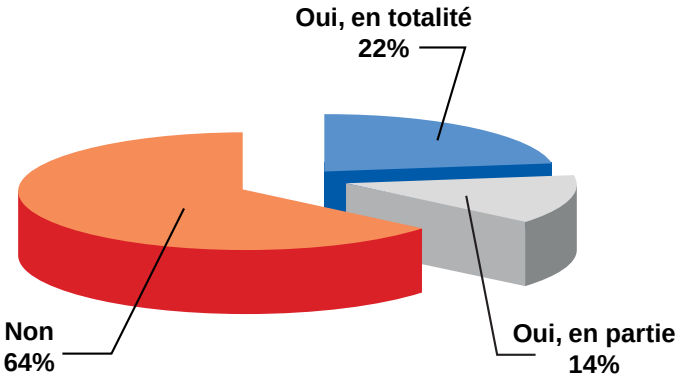


C'est à partir de 200 salariés que cette politique est définie, à 68 %, et encore plus au-delà de 500 salariés, à 85 %.
31 % des entreprises pratiquent une veille, en diminution de 6 points par rapport à 2001. Cette pratique est notamment en vigueur à partir de 500 salariés et dans le secteur des télécoms.

Il semblerait qu'il s'agisse plus d'une veille juridique, réglementaire, que technique : en effet, les exemples d'infection par virus s'appuyant sur des failles connues depuis longtemps et non corrigées sont là pour démontrer l'absence encore trop fréquente de ce type de veille.
D'autre part, la diminution de la veille pratiquée en interne peut s'expliquer par l'essor ces dernières années de l'offre externe de veille, notamment sur les vulnérabilités des produits.

Infogérance et prestataires externes

Une entreprise sur trois a placé tout ou partie de son système informatique et télécoms sous contrat d'infogérance.

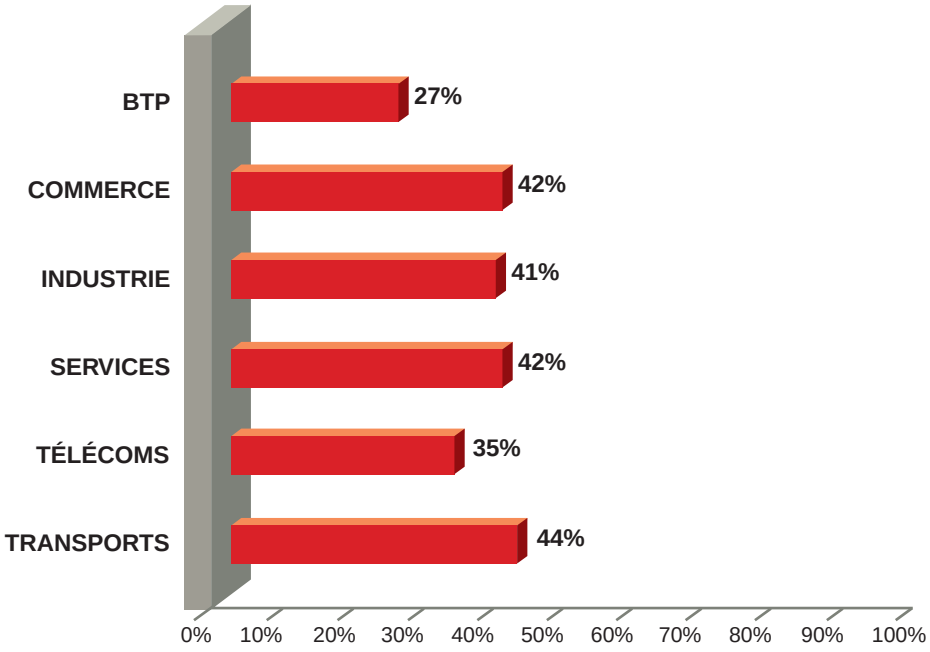


La taille de la société ne semble pas déterminante dans cette prise de décision.
Le commerce arrive en tête avec 51 % (totalité ou partie), suivi des télécoms avec 46 %.

40 % des entreprises font appel à des prestataires externes spécialisés. Ces derniers se répartissent à part égale entre services d'audit/conseil [1] et services opérationnels.
Tous les effectifs sont concernés à un niveau équivalent, de 32 % pour les plus de 1000 salariés à 47 % pour la tranche de 500 à 999. Il est surprenant de noter le taux de 40 % des plus petites entreprises.
Nous constatons que ce recours concerne :
- près de la moitié des entreprises qui ont mis en place une politique de sécurité,
- 37 % de celles qui n'ont personne en charge de la sécurité des S.I.

[1] Le questionnaire précise qu'il s'agit d'audit de sécurité et non d'un audit de contrôle ou opérationnel.

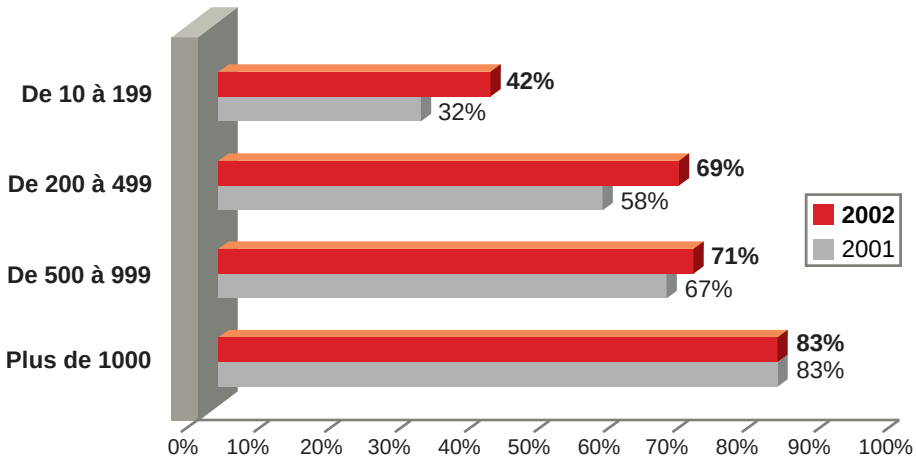
La répartition sectorielle se définit ainsi :



Des ressources sécurité en augmentation

44 % des entreprises ont au moins une personne en charge de la sécurité informatique, contre 34 % en 2001.

Proportion par tranche d'effectif :



Les plus fortes progressions sont enregistrées dans le BTP, qui passe de 15 % à 33 %, et dans les services, de 34 % à 55 %.

Cette augmentation des ressources humaines est-elle l'indice d'une montée en puissance de la fonction de responsable de la sécurité des S.I. en entreprise ?

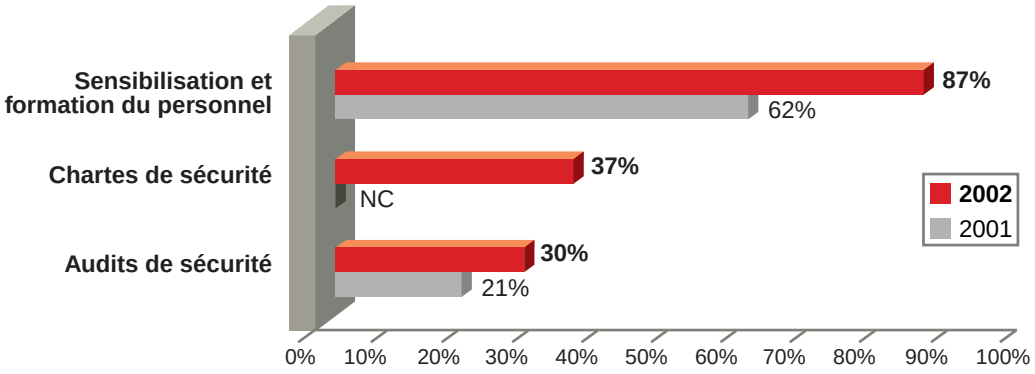
En 2002 les entreprises disposent en moyenne de 1,9 poste à équivalent temps plein (ETP), contre 1,4 en 2001. Même les entreprises de moins de 200 salariés déclarent 1,6 ETP affecté à la sécurité. Il existe toutefois d'importants écarts :
dans une PME, la fonction de responsable de sécurité des S.I. est fréquemment le résultat d'un cumul, tandis qu'elle devient ressource dédiée à part entière dans une société de plus grande taille.
Tous les secteurs sont concernés par cette évolution à l'exception des Télécoms qui passent de 8,3 postes à 5.

La visibilité sur le budget informatique est toujours incertaine, seulement la moitié des entreprises est capable de l'évaluer. En fonction des réponses obtenues, celui-ci s'établit cette année à 58 K euros en moyenne. Pour les 2/3 des entreprises répondantes, c'est ce budget qui finance les actions concernant la sécurité, très peu d'entre elles définissant un budget spécifique.

Sensibilisation des salariés en vedette

Management de la sécurité

La volonté des entreprises de développer une culture de la sécurité en interne est flagrante :



Le facteur humain qui est et restera toujours prépondérant, quels que soient les moyens techniques mis en œuvre, est réellement pris en compte.

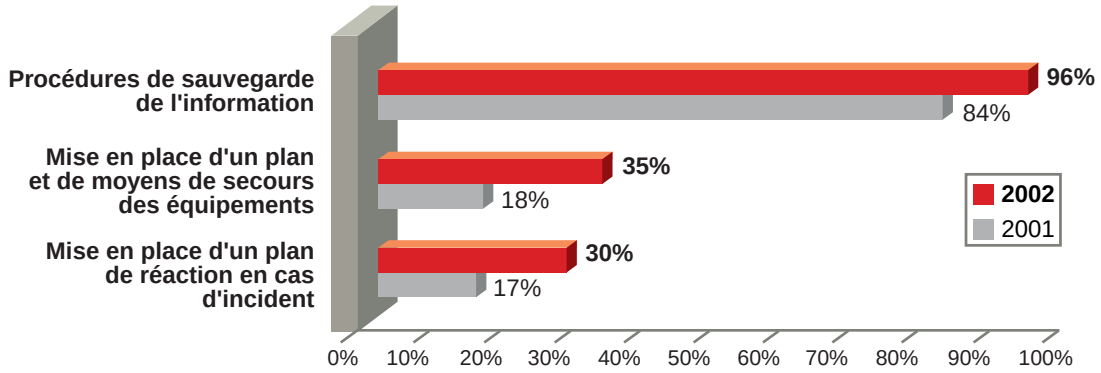
Ce graphe amène la réflexion suivante : les entreprises forment, ne formalisent pas et contrôlent encore moins. Le retentissement sur la vie de l'entreprise des problématiques soulevées par l'utilisation généralisée des moyens internet et intranet se fait pleinement ressentir. Cependant, le taux de mise en place de chartes de sécurité est assez faible, eu égard à l'engagement de responsabilité, y compris pénale, du salarié comme de l'entreprise et de ses dirigeants, en cas d'utilisation détournée de ces moyens [2].

La sensibilisation concerne, à plus de 85 %, tous les secteurs et effectifs.

[2] Le CLUSIF a édité en 2002 un "Guide d'élaboration d'une charte d'utilisation des moyens Intranet et Internet", précisant le contexte actuel du monde du travail, les risques et conséquences, les éléments de contenu d'une charte.

Continuité d'activité

Si les procédures de sauvegarde sont généralisées, des disparités existent dans la mise en œuvre de plans de secours et de plans de réaction :



A titre d'exemple, voici les pourcentages de mise en place d'un plan de réaction en cas d'incident :

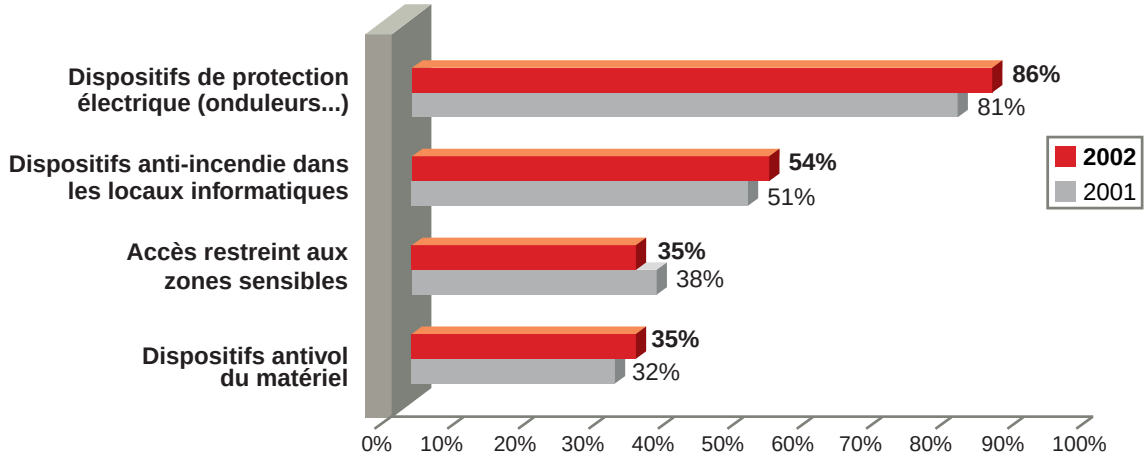
BTP	Commerce	Industrie	Services	Télécoms	Transports
13 %	34 %	32 %	31 %	60 %	26 %

De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1000
29 %	55 %	74 %	65 %

Nous posions l'an passé la question de savoir si le déclic concernant la mise en place de ces plans serait au rendez-vous en 2003. L'augmentation constatée semble le début d'une prise de conscience qui appelle un renforcement au regard des niveaux de dépendance. Les événements de l'automne 2001, aux Etats-Unis et à Toulouse, ainsi que les craintes liées à la crue centennale en région parisienne peuvent aussi se refléter dans ces chiffres.

Sécurité physique

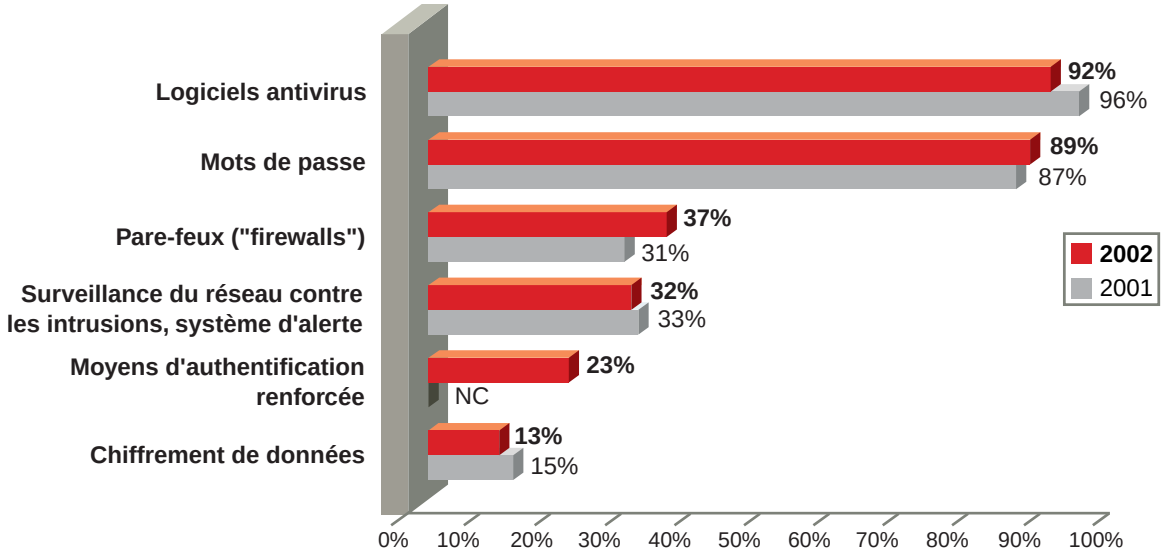
Après l'essor de 2001, la tendance est à la stabilité des moyens mis en œuvre :



Les dispositifs de protection électrique sont très répandus quel que soit l'effectif, à plus de 85 %, ou le secteur, à plus de 75 %.
La mise en place de dispositifs antivol du matériel est le fait principalement des entreprises de plus de 1000 salariés, à 71 %, et des Télécoms, à 60 %, contre 35 % pour tous les autres secteurs.

Sécurité logique

Les moyens mis en œuvre sont également stables, avec une légère avancée des pare-feux :



Cette stabilité mise en parallèle avec l'ouverture marquante des systèmes d'information montre le caractère insuffisant du développement des politiques de sécurité et d'outils idoines. Bon nombre d'entreprises ne semblent pas avoir pris conscience des risques qu'elles encourent.

Les tableaux ci-dessous donnent une image plus précise de la répartition des pare-feux, par effectif et secteur.

Mise en place de pare-feux :

BTP	Commerce	Industrie	Services	Télécoms	Transports
15 %	40 %	45 %	42 %	43 %	18 %

De 10 à 199	De 200 à 499	De 500 à 999	Plus de 1000
35 %	80 %	83 %	89 %

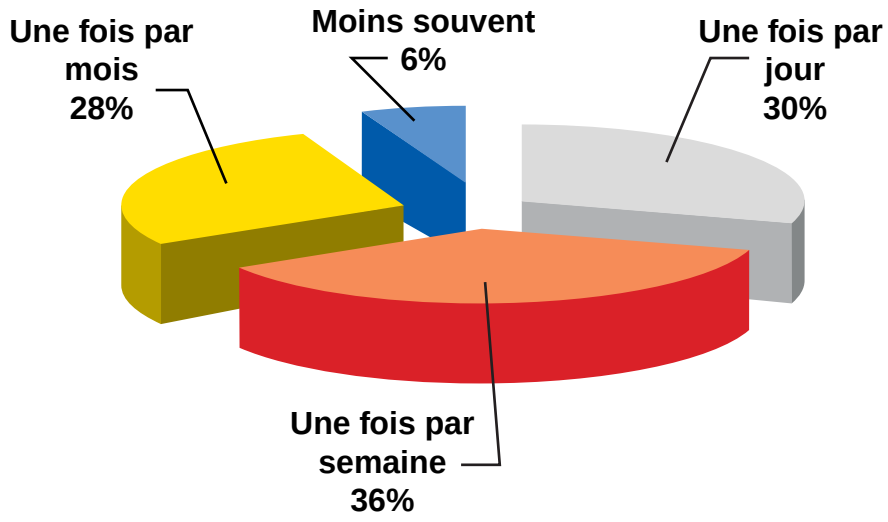
La corrélation entre l'ouverture des systèmes d'information et le niveau de sécurité logique donne la représentation suivante :

	Site internet	Messagerie électronique généralisée	Accès internet généralisé
Logiciels antivirus	96 %	95 %	95 %
Mots de passe	93 %	92 %	91 %
Pare-feux	45 %	49 %	45 %
Surveillance du réseau contre les intrusions, système d'alerte	38 %	42 %	34 %
Moyens d'authentification renforcée	27 %	28 %	24 %
Chiffrement de données	17 %	19 %	15 %

Logiciels antivirus

90 % des entreprises qui ont installé des logiciels antivirus procèdent à leur mise à jour. Seulement 30 % d'entre elles procèdent à une mise à jour quotidienne.

Fréquence de mise à jour :



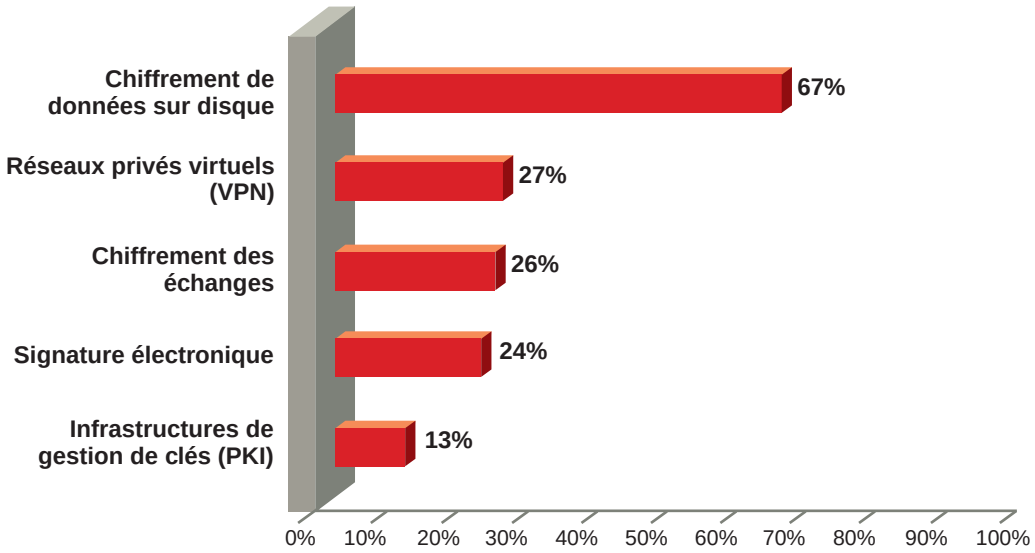
Ces mises à jour sont automatiques dans 74 % des cas, contre 61 % en 2001. Elles progressent avec la taille de l'entreprise, passant de 73 % pour la tranche 10 à 199 salariés, à 89 % pour les plus de 1000 salariés.
Quatre secteurs se situent aux environs de 70 % : le BTP, l'industrie, les services, les transports. Le commerce atteint 85 % et les télécoms 92 %.

Il est à noter qu'environ un tiers des entreprises déclare des mises à jour mensuelles, voire moins souvent, alors que l'infection par virus est en forte augmentation (+ 12 points). Cette périodicité est nettement insuffisante si l'on considère certains virus dont la propagation est extrêmement rapide [3]. Il est recommandé de réaliser une consultation automatique au moins quotidienne des sites des éditeurs pour rechercher une disponibilité éventuelle d'une mise à jour.
Signalons toutefois qu'il existe des technologies antivirus génériques qui ne cherchent pas à identifier nominativement le virus mais à détecter un comportement viral. Elles ne dépendent pas d'une mise à jour de la base de signatures.

Chiffrement de données

Seulement 13 % des entreprises pratiquent le chiffrement de données, principalement pour la sécurisation du contenu du poste de travail. Le chiffrement des transactions et les PKI n'ont pas encore réussi à percer.

Moyens de chiffrement utilisés :



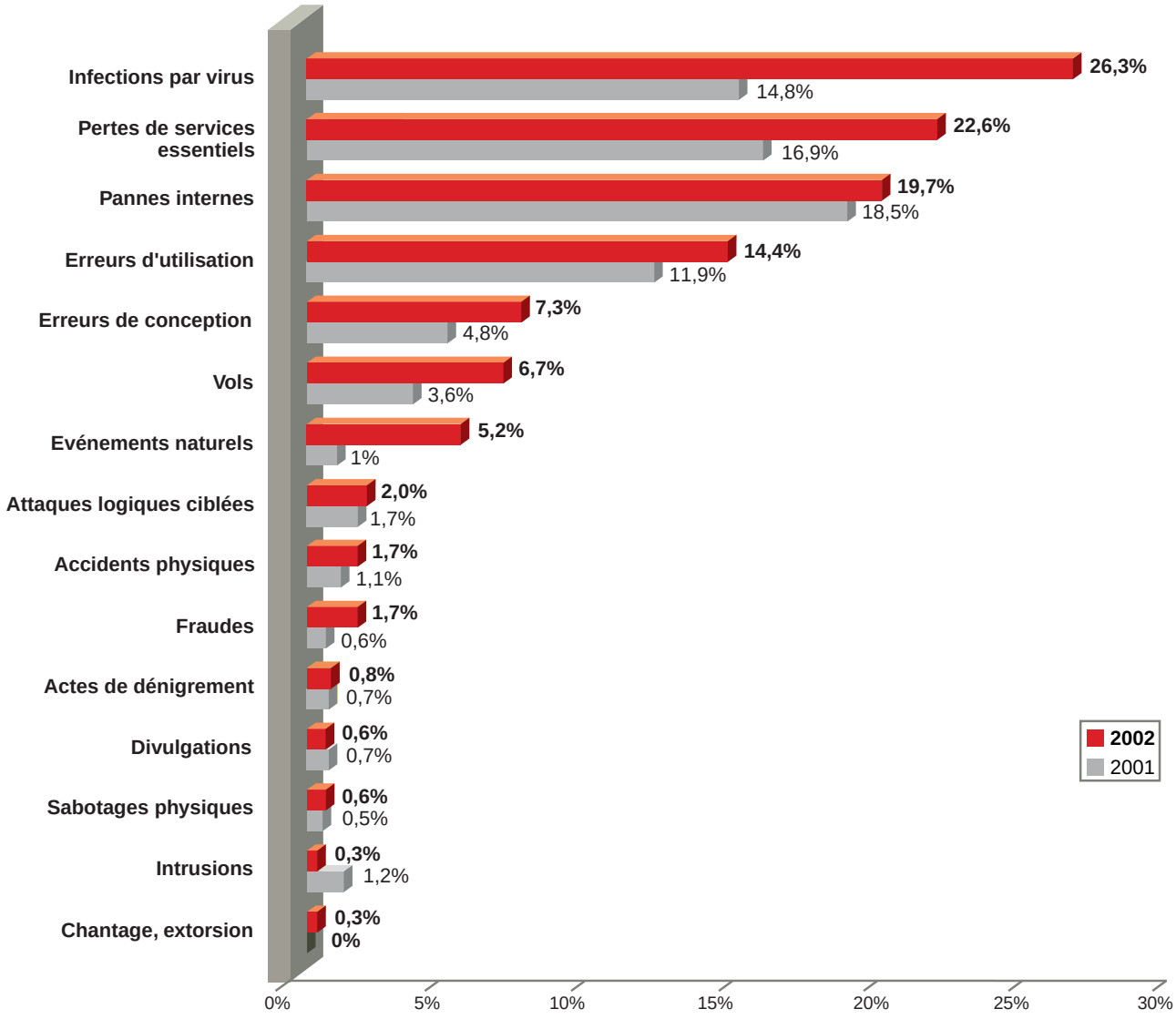
[3] L'enquête menée par le CLUSIF auprès de ses membres sur le virus Lirva a montré qu'une mise à jour quotidienne était même parfois insuffisante ; plusieurs sociétés ont décidé de procéder à plusieurs mises à jour par jour.

Des sinistres déclarés en progression

60 % des entreprises déclarent n'avoir subi aucun sinistre : ignorance ou manque de transparence ? Il semble évident que de nombreux incidents ne sont pas comptabilisés, car non détectés.

Parmi les 40 % qui en annoncent, le niveau se situe à moins de 10 incidents, pour 36 % des entreprises. La décomposition de ces 36 % nous renseigne sur les populations impactées : les entreprises de 200 à 999 salariés sont touchées à 49 %. Les deux tranches extrêmes se situent à presque 36 %. Le commerce est atteint à 40 %, l'industrie, les services et les transports à 35 %, le BTP à 32 % et les télécoms à 27 %.

Certains types de sinistres enregistrent une progression marquée :



Voici l'analyse sectorielle des items principaux en pourcentage :

	Secteur le plus touché		Secteur le moins touché	
Infections par virus	Services	35 %	Télécoms	13,5 %
Pertes de services essentiels	Industrie	28 %	BTP	16 %
Pannes internes	Télécoms	33 %	BTP	12 %
Erreurs d'utilisation	Commerce	24 %	BTP	6 %
Vols	Industrie	12 %	Transports	0,4 %

Le vol est nettement plus fréquent dans les grandes entreprises, 54 %, alors qu'il n'affecte qu'à 5 % les structures de moins de 200 salariés.

Impact des sinistres

La tendance générale est de relativiser l'impact des sinistres récurrents, tous types confondus.

Degré d'impact annoncé :

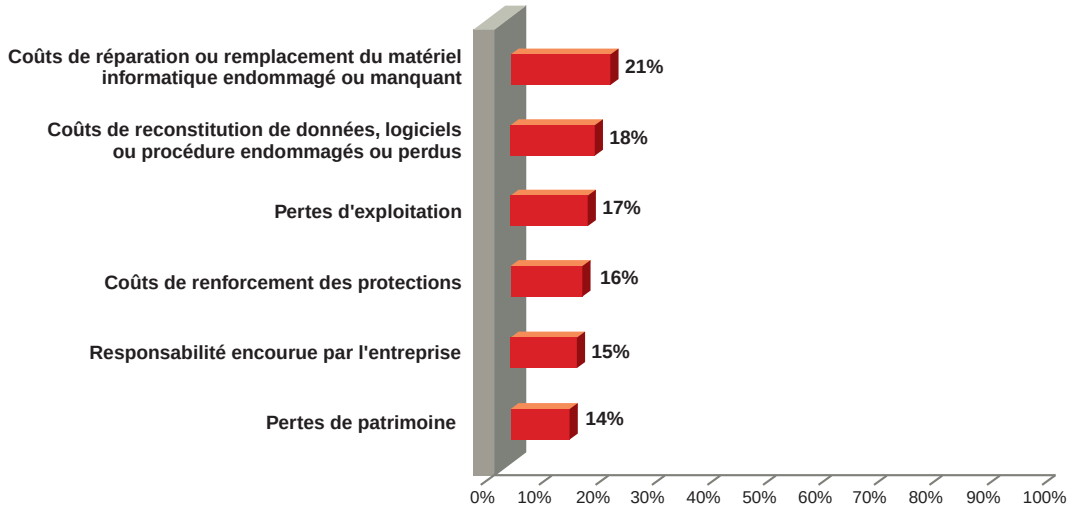
	Impact faible	Impact moyen	Impact fort
Infections par virus	60 %	25 %	15 %
Pertes de services essentiels	68 %	20 %	12 %
Pannes internes	58%	32 %	10 %
Erreurs d'utilisation	77 %	18 %	5 %
Erreurs de conception	50 %	35 %	15 %
Vols	54 %	24 %	22 %
Evénements naturels	52 %	25 %	23 %

Seulement 14 % des entreprises impactées procèdent à une évaluation financière, ce qui reste encore très marginal. Bien que les chiffres recueillis soient faibles, nous pouvons indiquer que le vol ou la disparition de matériel ou de logiciel entraîne l'activation d'une telle évaluation.

Dans une période de réduction globale des budgets, de mise en avant du retour sur investissement et considérant l'enjeu majeur que représente la sécurité des systèmes pour une entreprise, il est étonnant que ce calcul d'impact ne soit pas réalisé systématiquement. Pourtant, c'est l'un des moyens permettant de justifier les dépenses en matière de sécurité. Pour un RSSI [4], il s'agit d'un levier pour dégager des budgets. Nous constatons que les entreprises estiment globalement les impacts de sinistres comme faibles mais ne procèdent pas à une évaluation, d'où la question de savoir sur quels éléments tangibles repose leur réponse.

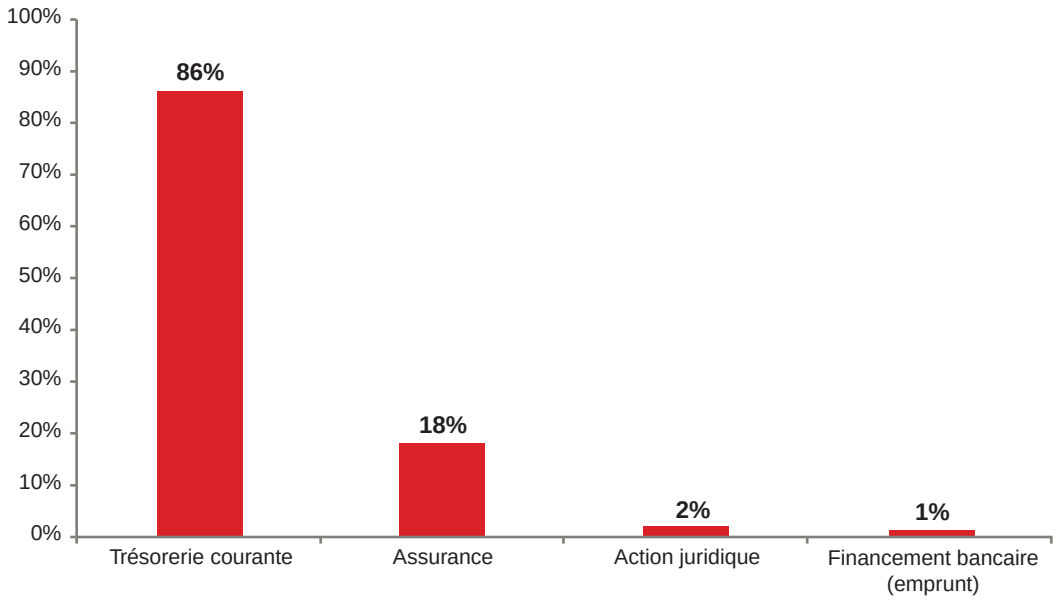
[4] Responsable Sécurité des Systèmes d'Information.

Le graphe ci-dessous exprime la répartition approximative de l'impact financier entre différentes conséquences possibles :



Concernant la perte d'exploitation, nous faisons le constat que nous sommes dans une société dépendante de l'information numérique puisque le sinistre matériel ou immatériel va générer ce type de perte ; sur le plan assuranciel il y a lieu de souscrire les garanties relatives. Rappelons que même si la répartition exprimée dans ce graphe est relativement homogène entre les différentes formes de dépenses, le coût d'un équipement est souvent largement inférieur à celui d'une perte d'exploitation journalière.

Dans 86 % des cas, l'impact financier des sinistres est résorbé par la trésorerie courante :

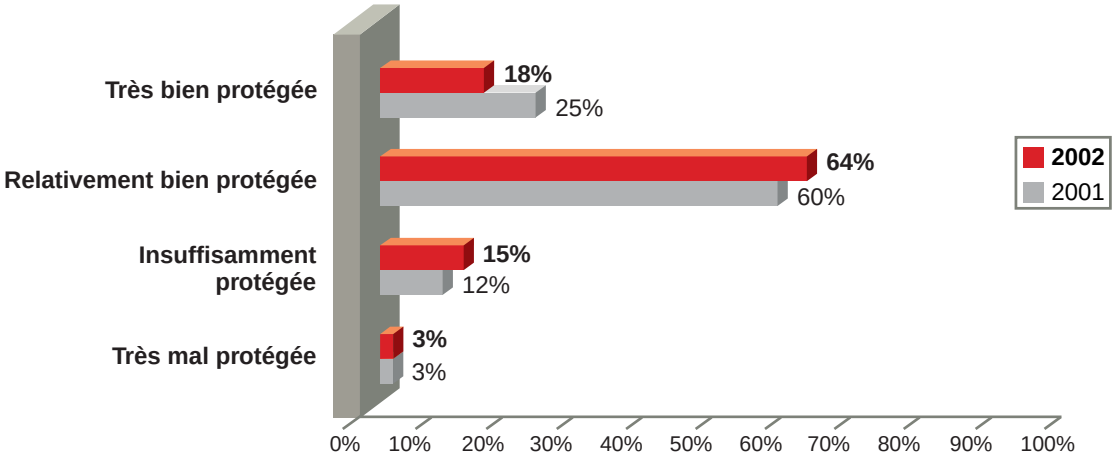


Ce très fort recours à la trésorerie peut s'expliquer soit par la faiblesse des impacts, pour un montant inférieur à la franchise, soit par un défaut d'assurance.

Synthèse et tendances

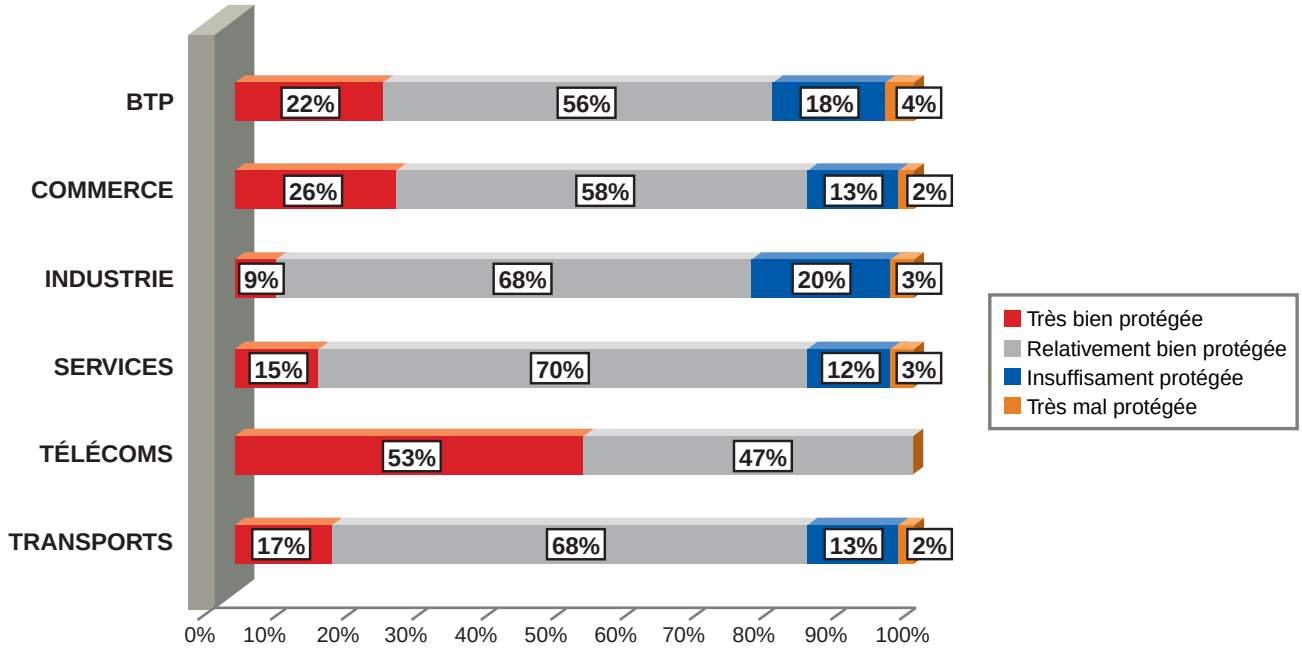
Les entreprises estiment majoritairement que leur système d'information est bien ou très bien protégé, à 82 %. Seulement 3 % des entreprises s'estiment très mal protégées, chiffre constant sur trois ans.
L'évolution 2002/2001 fait apparaître des divergences.

Sentiment de confiance des entreprises face aux risques :

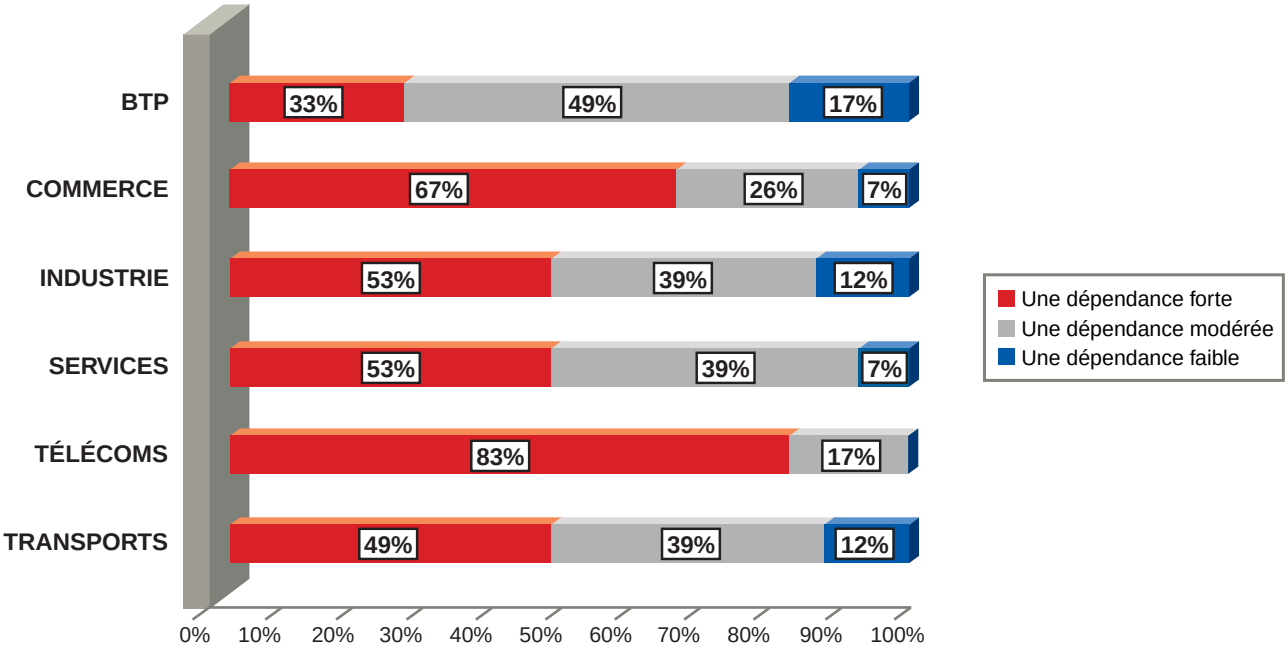


Les écarts par tranche d'effectif sont très importants par rapport à 2001. Le recul de "très bien protégée" est très significatif : ainsi, de 500 à 999 salariés, le pourcentage s'affiche à 17 % contre 41 % l'an passé.
Globalement, c'est de 200 à 499 salariés que la confiance est la plus marquée : 13 % de "très bien protégée" et 80 % de "relativement bien protégée".

Les secteurs se différencient ainsi :



Il est intéressant de comparer ces données avec le sentiment de dépendance déclaré par les entreprises.

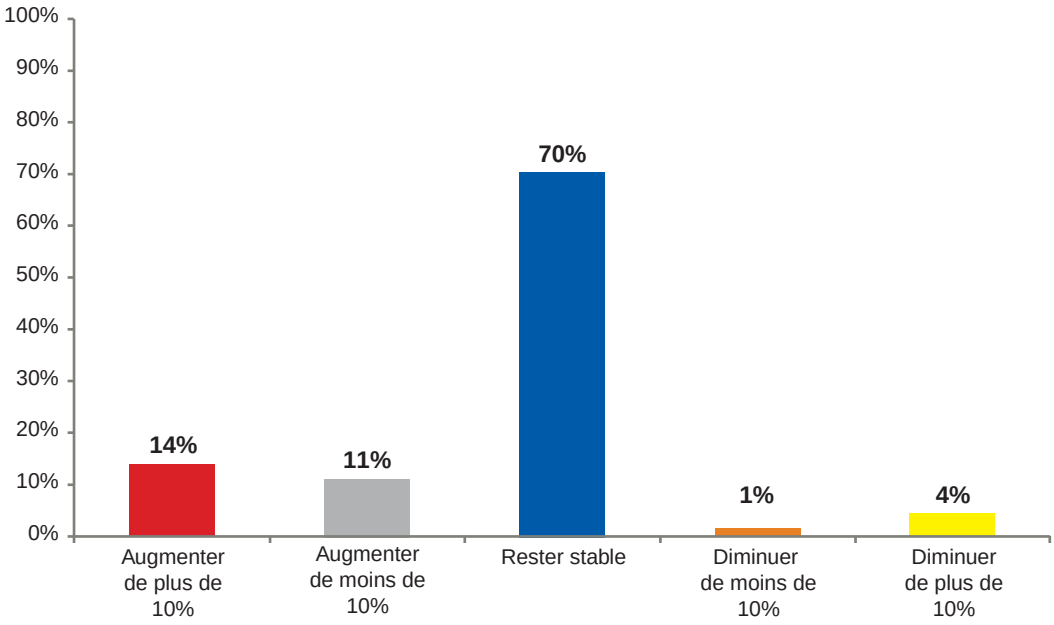


Les télécoms se sentent à 100 % "très bien" ou "relativement bien" protégés malgré une ouverture et une dépendance très forte et la mise en œuvre à 43 % de pare-feux.

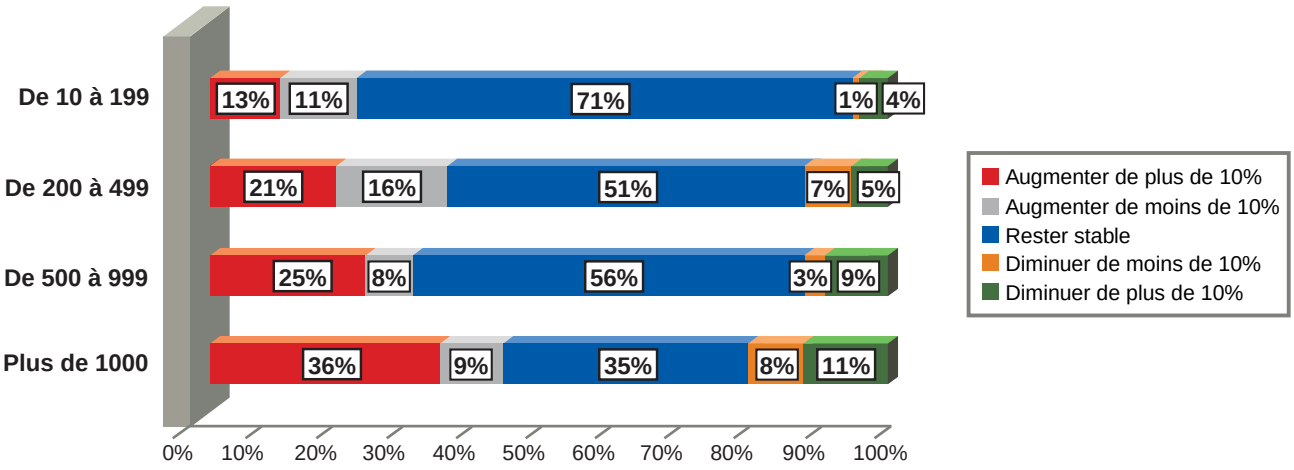
Perspectives budgétaires et techniques à deux ans

C'est peut être ce sentiment de sécurité relative qui entraîne la stabilité à deux ans du budget consacré à la sécurité.

Prévisions sur le budget sécurité :



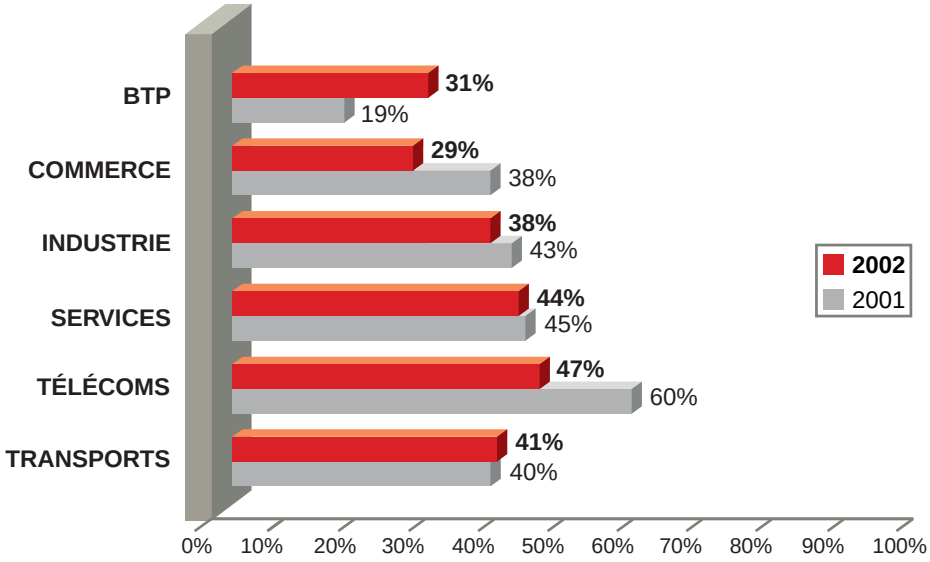
La corrélation entre le sentiment de dépendance et l'augmentation de ce budget n'est pas significative ; il semblerait que le facteur important soit plus la taille de l'entreprise :



A l'exception des télécoms qui envisagent, à 54 %, de l'augmenter, l'ensemble des autres secteurs se situe entre 20 % et 26 %.

Quant au renforcement des dispositifs de sécurité, 37 % des entreprises annoncent cette intention. Là encore, l'effectif est déterminant. Le fossé se creuse entre les structures de moins de 200 salariés, qui se situent à 36 % d'intention d'augmentation, et les autres catégories d'effectif qui s'échelonnent entre 62 % et 72 %.

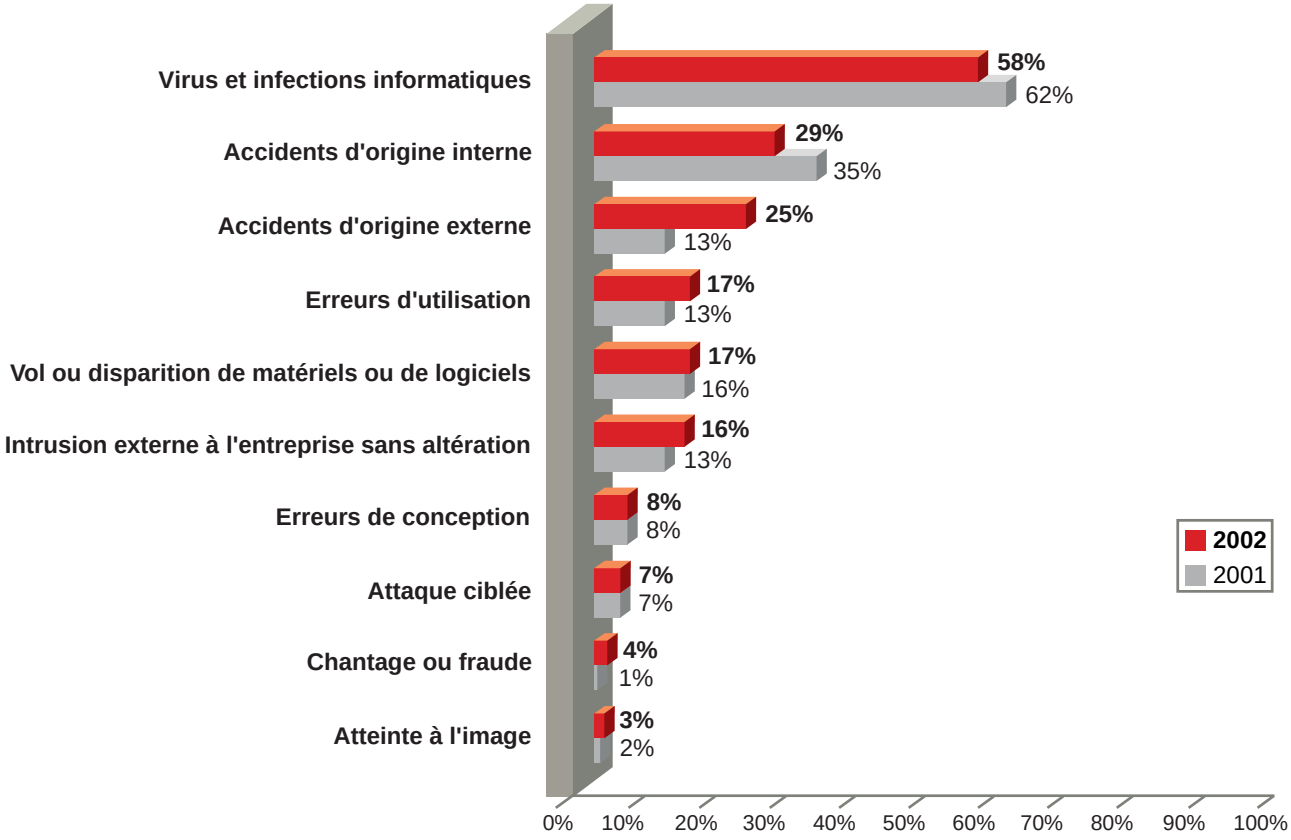
Le comparatif sectoriel 2002/2001 nous donne quelques indications :



Quels risques pour l'avenir ?

Les risques redoutés évoluent sensiblement par rapport à l'année dernière. Ce sont les accidents d'origine externe qui font le plus grand bond.

Hit parade des risques perçus :

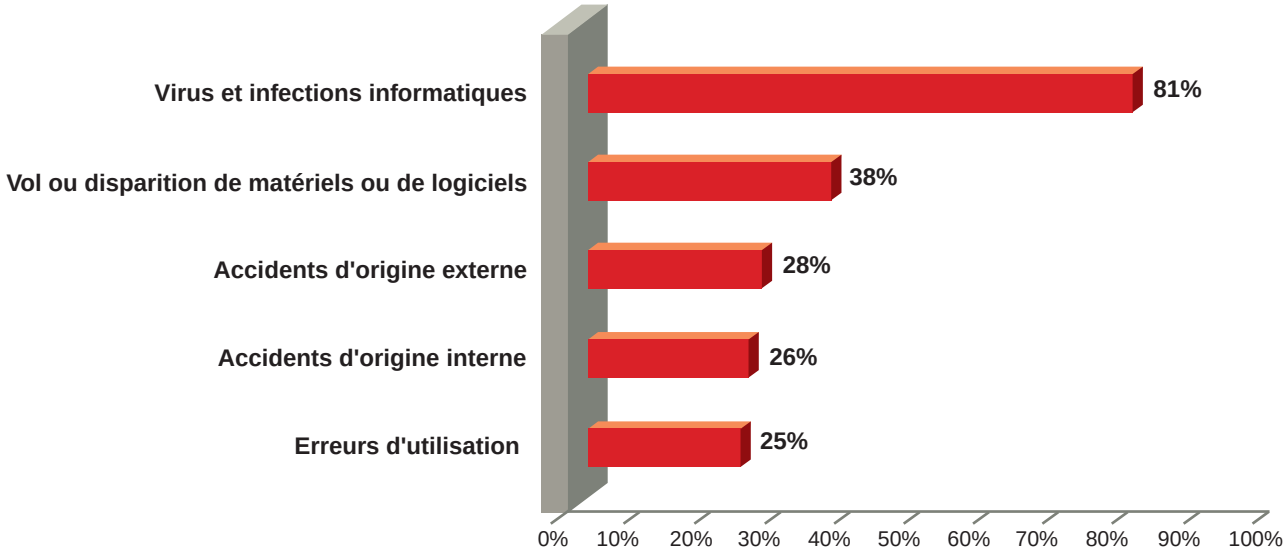


Malgré une régression non significative, les virus apparaissent pour la troisième année consécutive en tête de ce classement.

Le mythe du virus se poursuit. Dans le même temps, il est perçu comme le risque le plus inquiétant mais son impact est considéré comme faible dans la réalité des incidents avérés. Pourquoi cette prédominance ? Plusieurs raisons peuvent être avancées : les derniers virus qui, comme toujours, ont défrayé la chronique ; l'aspect facilement identifiable du virus et son analogie avec la santé ; et enfin, le fait que ce sinistre touche directement un grand nombre d'utilisateurs.

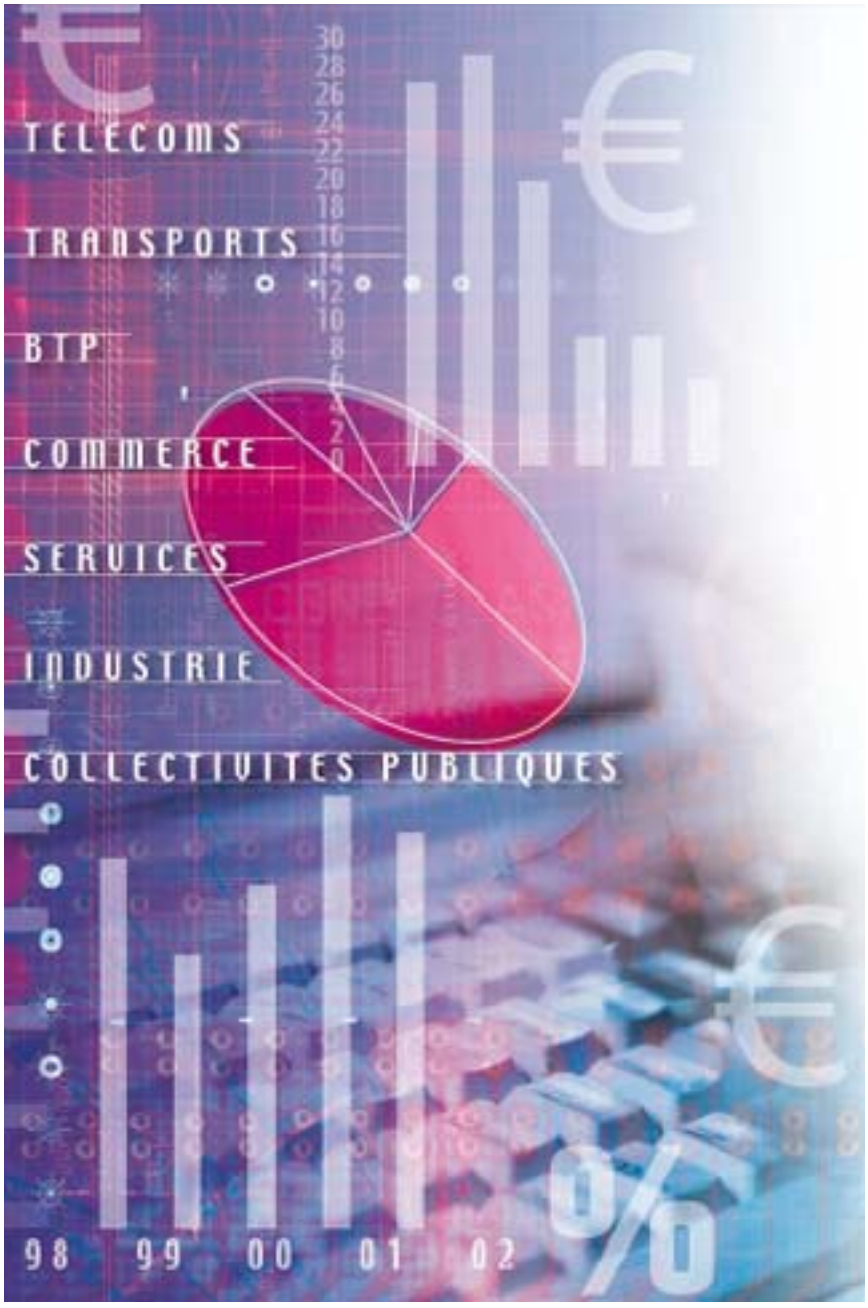
L'effectif influe peu sur la perception de l'ensemble des risques.

La corrélation entre les sinistres subis dans l'année et les risques potentiels donne le schéma suivant :



N.B. Ce graphe se lit de la façon suivante : les entreprises victimes d'une infection par virus en 2002 redoutent à 81 % ce type de sinistre pour le futur.

COLLECTIVITÉS PUBLIQUES



Environnement des systèmes d'information

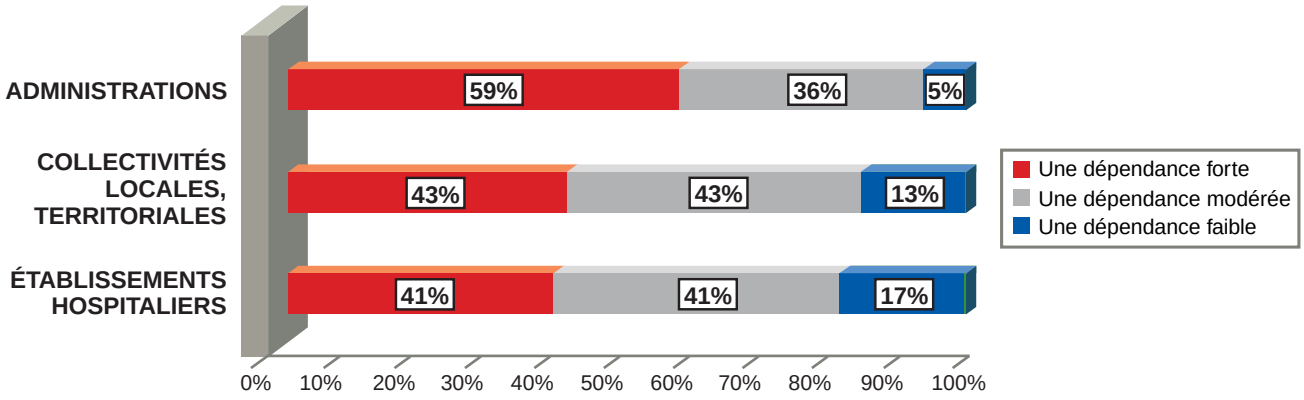
Avertissement

Nous rappelons au lecteur les modifications majeures de l'échantillon 2002, tant en terme de taille que de redressement [5]. En conséquence, aucune comparaison entre les données présentées dans cette étude et celles de l'année dernière n'est établie.

****

La moitié (51 %) des collectivités publiques s'estime fortement dépendante du système d'information. Cette dépendance est modérée pour 39 % d'entre elles et faible pour 10 %.

Répartition sectorielle :



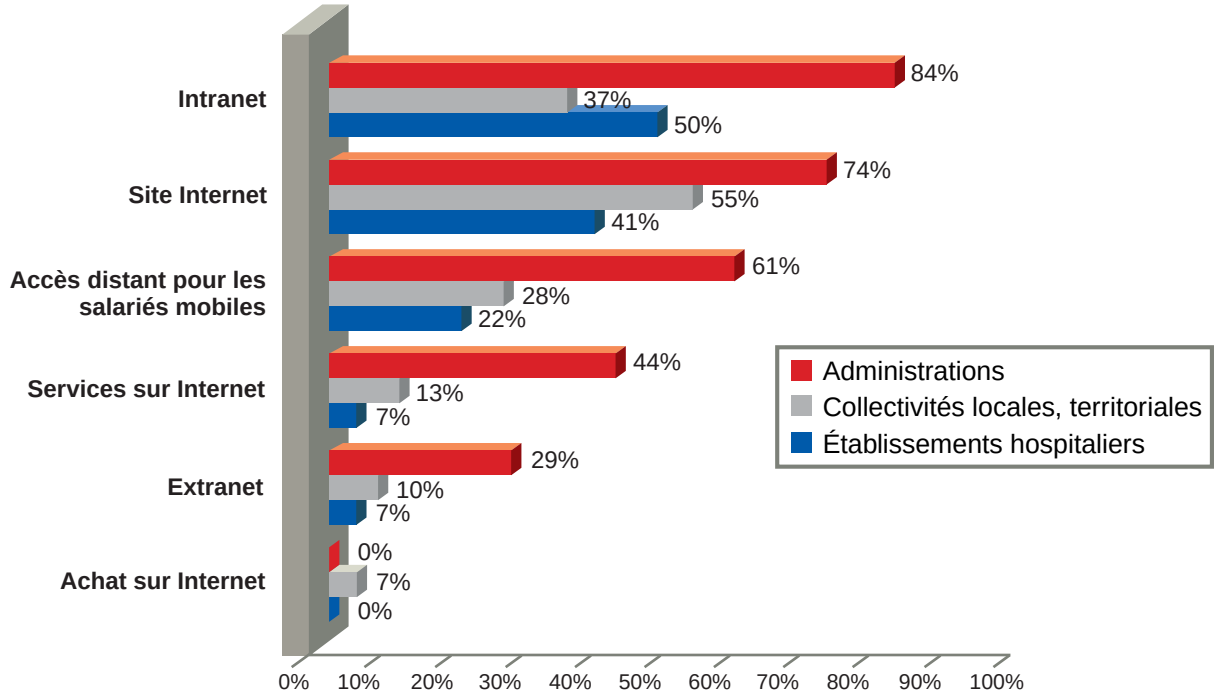
Les administrations [6] sont nettement plus conscientes de leur dépendance.

Les différences constatées dans le sentiment de dépendance vis-à-vis du système d'information s'expliquent par les différences d'organisation des trois catégories. Les administrations centrales et déconcentrées gèrent des réseaux nationaux alors que les collectivités territoriales et les établissements hospitaliers présentent des situations très disparates.

[5] Cf chapitre " Méthode d'enquête ".

[6] Les administrations regroupent les administrations centrales et services déconcentrés.

L'ouverture des systèmes d'information est conséquente pour toutes les catégories :



Il est à noter l'importance de l'accès distant pour les administrations.

Les programmes développés par l'administration qui visent à promouvoir le canal internet pour faciliter les relations entre l'usager et l'administration (démarches d'état civil, télédéclarations diverses …) entrent sans nul doute pour une bonne part dans les chiffres ci-dessus.

36 % des collectivités publiques déclarent avoir défini une politique globale de sécurité. C'est le cas pour 41 % des administrations, 30 % des collectivités locales et 31 % des établissements hospitaliers.

La veille est pratiquée par 36 % d'entre elles : les administrations et les établissements hospitaliers l'exercent à 41 % et les collectivités locales 23 %.

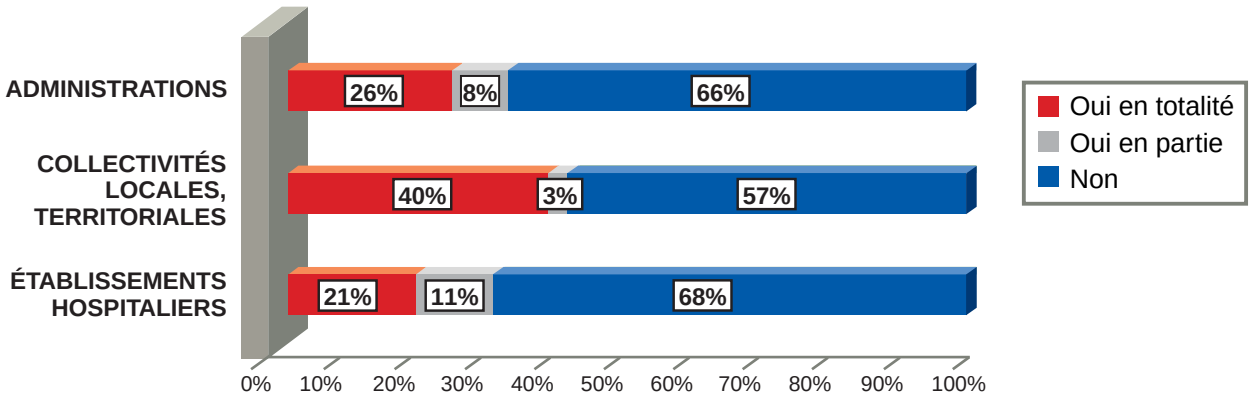
Concernant la veille, les administrations ont toutes une démarche analogue ce qui n'est pas le cas des collectivités locales. Ces dernières ont un comportement assez proche de celui des PME où le rôle d'un maire peut être comparé à celui d'un chef d'entreprise.

Lorsque les collectivités publiques ont mis en place une politique de sécurité, elles ont recours, à 38 %, à des prestataires externes spécialisés.

Infogérance et prestataires externes

Plus d'un tiers des collectivités publiques ont souscrit un contrat d'infogérance de leur système d'information, soit pour partie, à 7 %, ou en totalité, à 30 %.

Répartition sectorielle du recours à l'infogérance :

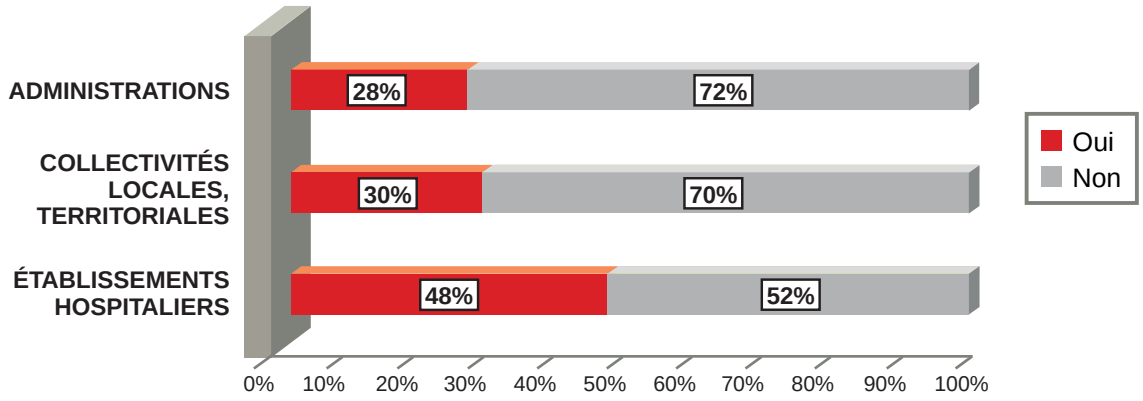


L'étude montre que les collectivités locales ont plus tendance à recourir à l'infogérance.

Les collectivités locales bénéficient de revenus différents, notamment par les impôts locaux. Ce nombre suscite les interrogations suivantes : - Sur le plan budgétaire, est-il plus intéressant d'externaliser les systèmes d'information ? - Est ce que cette différence est une conséquence de la décentralisation ?

33 % des collectivités publiques font appel à des prestataires externes spécialisés.
Les établissements hospitaliers se démarquent dans cette démarche.

Répartition sectorielle du recours aux prestataires externes :



Ressources sécurité

40 % des collectivités publiques ont au moins une personne en charge de la sécurité des systèmes d'information :
- administrations, 46 %,
- établissements hospitaliers, 41 %,
- collectivités locales, 30 %.

Elles disposent en moyenne d'un poste à équivalent temps plein.
Parmi celles qui n'ont pas de personne spécifique en charge, elles ont recours à 39 % à des prestataires externes.

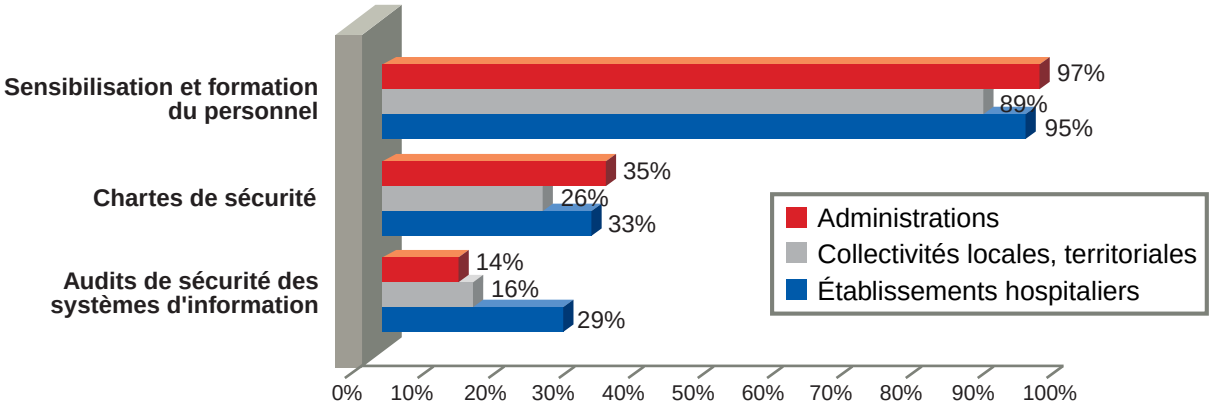
31 % affectent des ressources budgétaires spécifiques à la sécurité des systèmes d'information.
En l'absence de budget spécifique, les actions en sécurité sont financées quasi exclusivement par le budget informatique.

Nous précisons qu'en ce qui concerne les collectivités publiques, les budgets informatiques et télécoms sont communs. Il n'existe qu'un ou deux ministères qui aient une ligne de budget dédiée à la sécurité ; globalement, les collectivités ne font pas figurer cette ligne dans un domaine comptable apparent, le budget n'est qu'estimé.

Management de la sécurité

Parmi les moyens utilisés en terme de management, la sensibilisation des salariés arrive en tête. Ce résultat quasi unanime indique clairement que le message est passé sur le plan opérationnel.

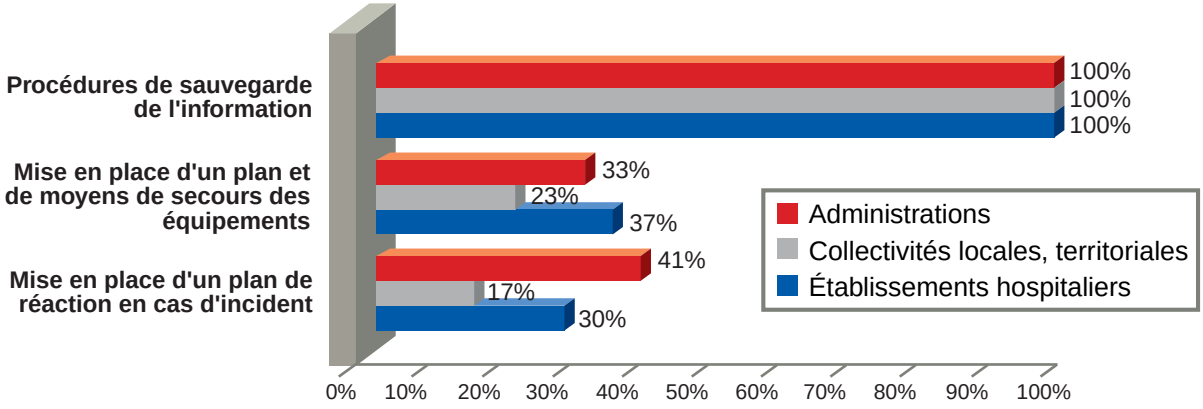
Moyens mis en œuvre :



Le chiffre moyen concernant les chartes de sécurité s'explique par le fait qu'il existe un contrat moral, des règles à respecter, mais pas de règlement intérieur.
Le faible pourcentage des audits peut être relativisé ; en effet, des démarches organisationnelles dont l'objectif est identique sont réalisées sans pour autant recevoir cette appellation.

Continuité d'activité

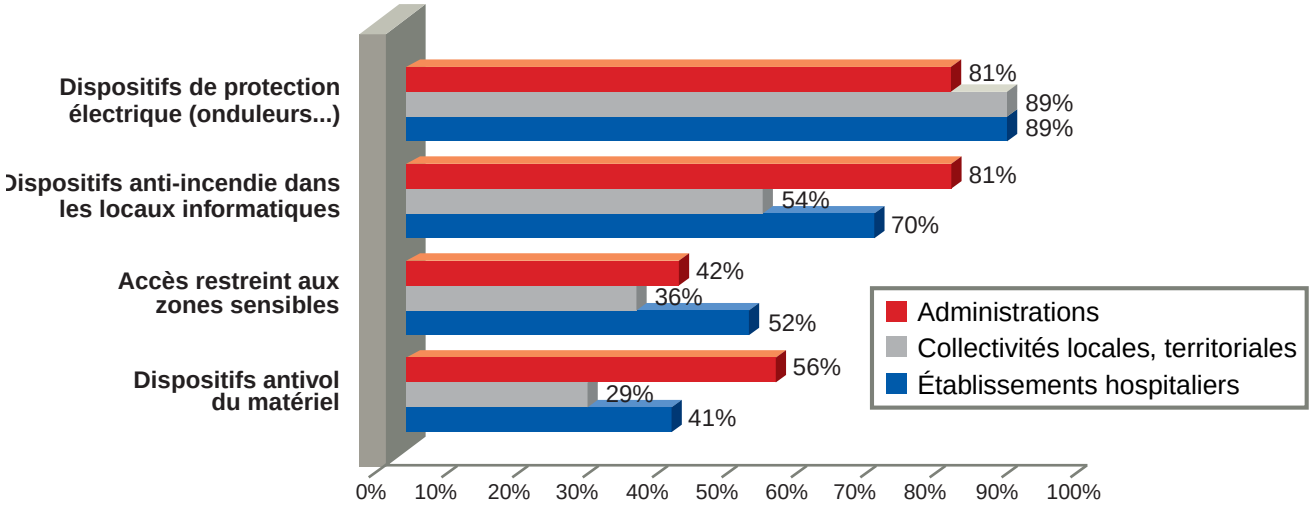
La continuité d'activité ne semble pas mise en œuvre à haut niveau, sauf en ce qui concerne les procédures de sauvegarde.



Pour les établissements hospitaliers, l'absence de différenciation entre l'informatique médicale et l'informatique de gestion fait certainement chuter le taux de mise en place d'un plan de réaction. L'informatique médicale fait l'objet de plans spécifiques, ce qui n'est pas toujours vrai dans l'autre cas.

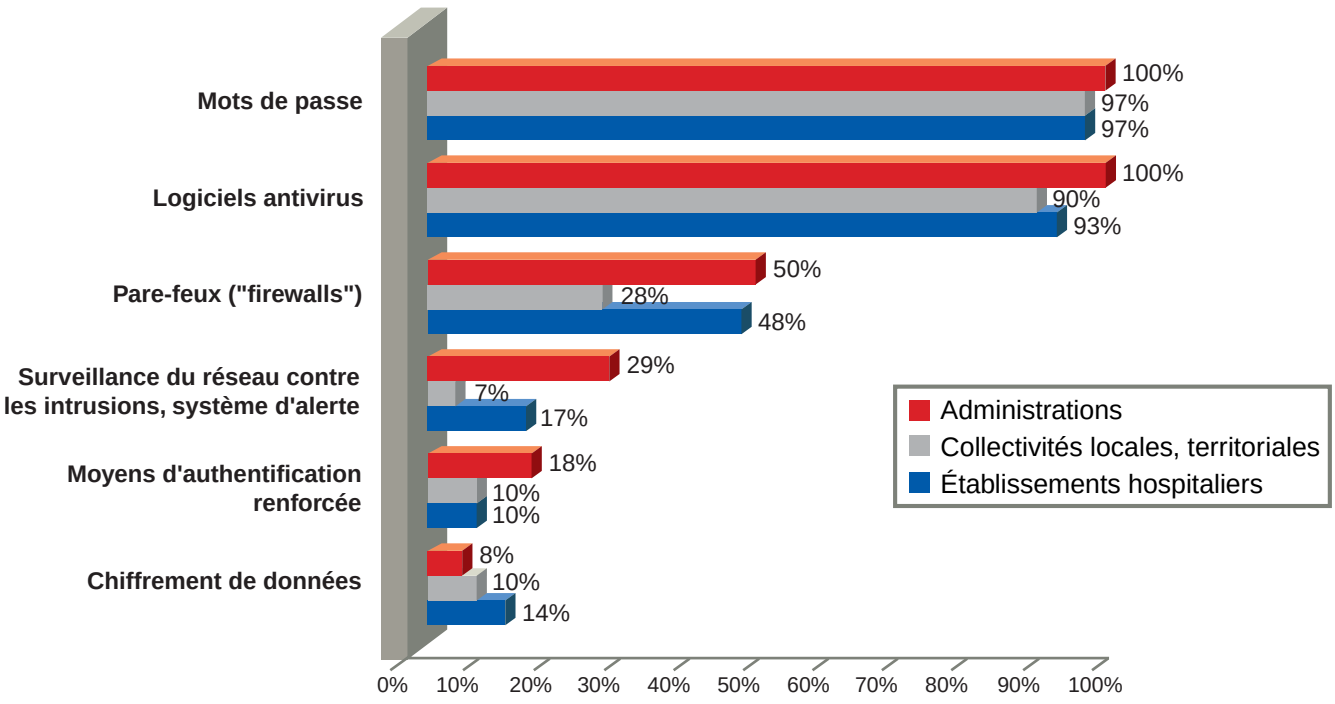
Sécurité physique

La sécurité physique est développée dans tous les secteurs ; dispositifs de protection électrique et anti-incendie sont particulièrement présents :

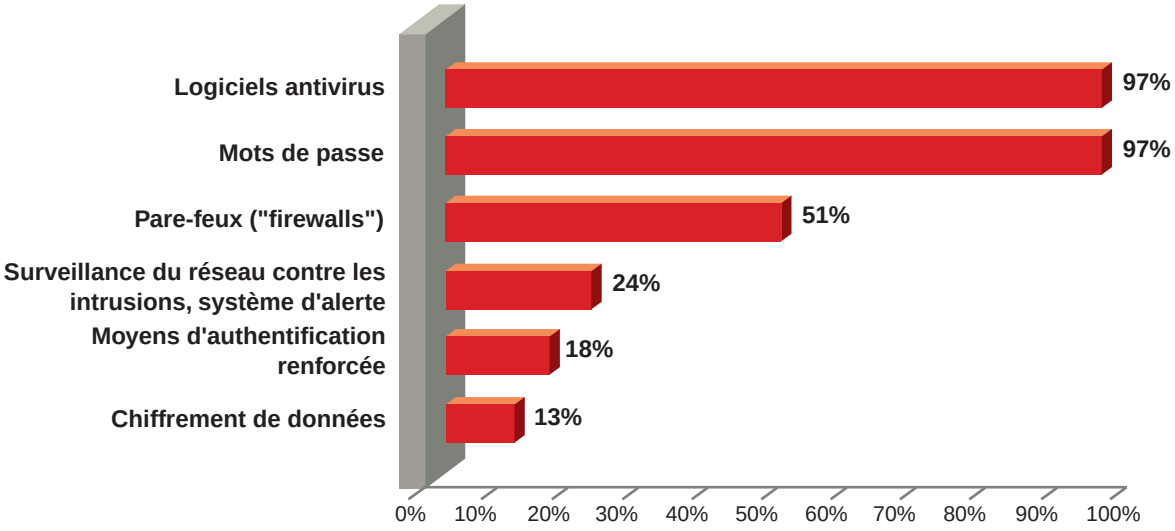


Sécurité logique

Les mots de passe et les logiciels antivirus sont banalisés.
Les collectivités locales ne semblent pas mettre en œuvre directement de pare-feux ou de surveillance du réseau :



Si l'on établit la corrélation entre l'ouverture d'un site internet et les moyens de protection logique mis en œuvre, les résultats sont les suivants :

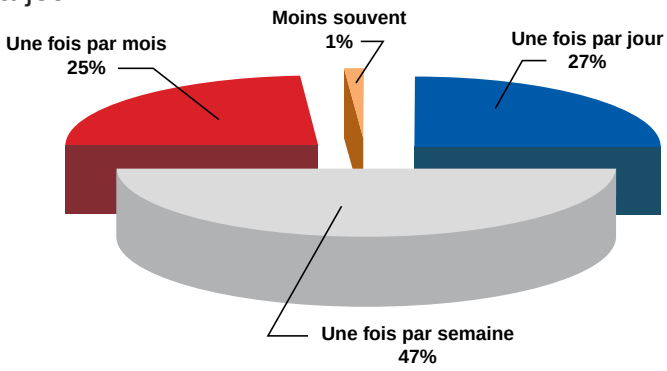


Ces résultats doivent être relativisés du fait que les agents de l'administration n'ont pas toujours conscience des équipements qui sont mis en œuvre par les hébergeurs ou les prestataires. Le faible taux de moyens d'authentification renforcée traduit une réalité qui est la suivante : le passage de la mise en place de mots de passe ou d'accès protégés à d'autres moyens de protection est un processus de longue haleine.

Logiciels antivirus

91 % des collectivités publiques qui les utilisent procèdent à des mises à jour. Celles-ci ont lieu au moins une fois par semaine pour 74 % d'entre elles.

Fréquence de mise à jour :



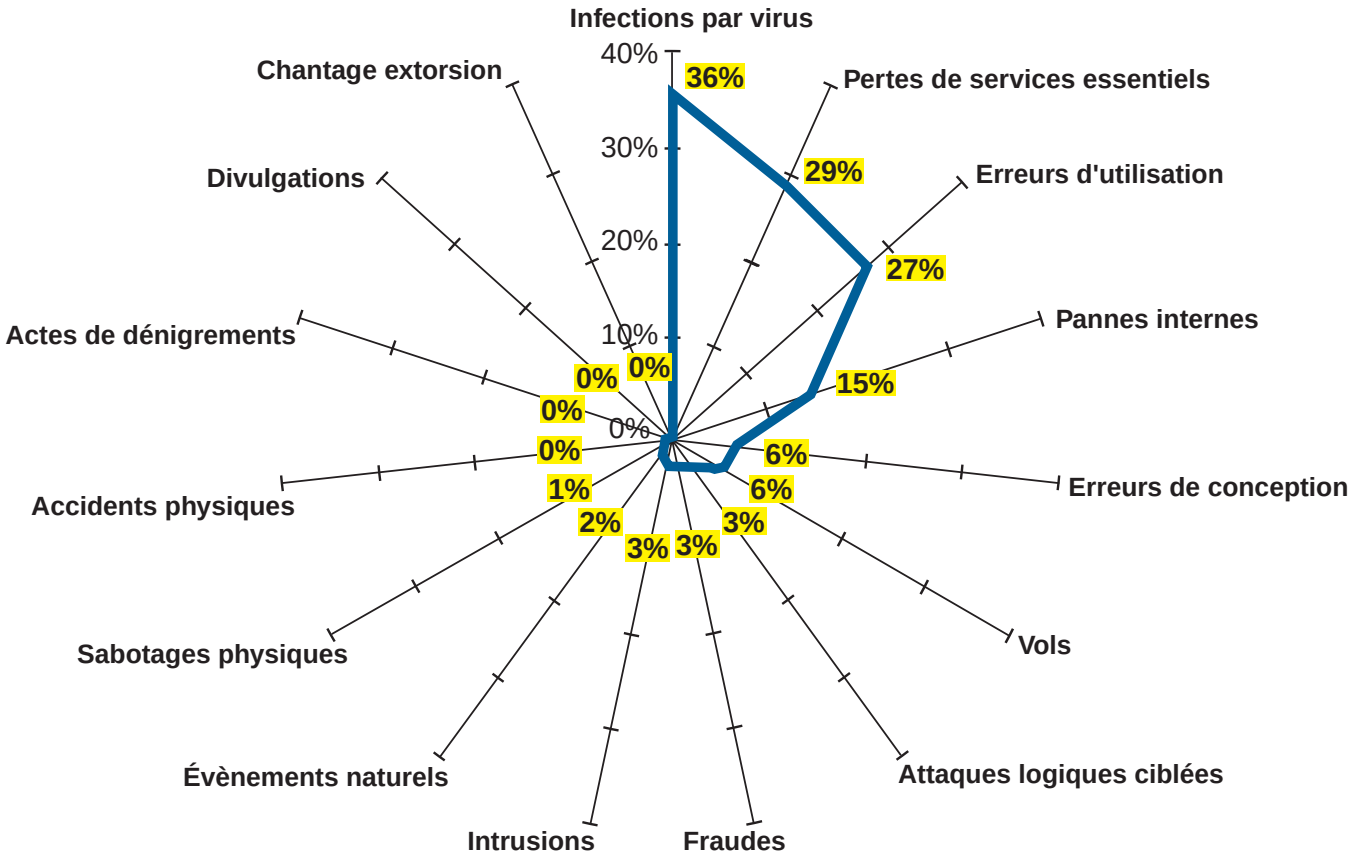
Il est nécessaire de distinguer l'antivirus de passerelle de messagerie de l'antivirus de poste de travail. La recommandation générale qui est appliquée dans l'administration est l'utilisation de deux antivirus distincts.

Ces mises à jour sont automatiques dans 77 % des cas.
Les administrations sont les plus automatisées, à 94 %, contre 64 % pour les collectivités territoriales et 46 % pour les établissements hospitaliers.

Evaluation de la sinistralité

Près de 2/3 des collectivités publiques ne déclarent aucun incident et 27 % en déclarent moins de dix. Dans ce cas, la répartition par secteur est assez uniforme, de 24 % à 29 %.

Les causes des sinistres constatés sont les suivantes :

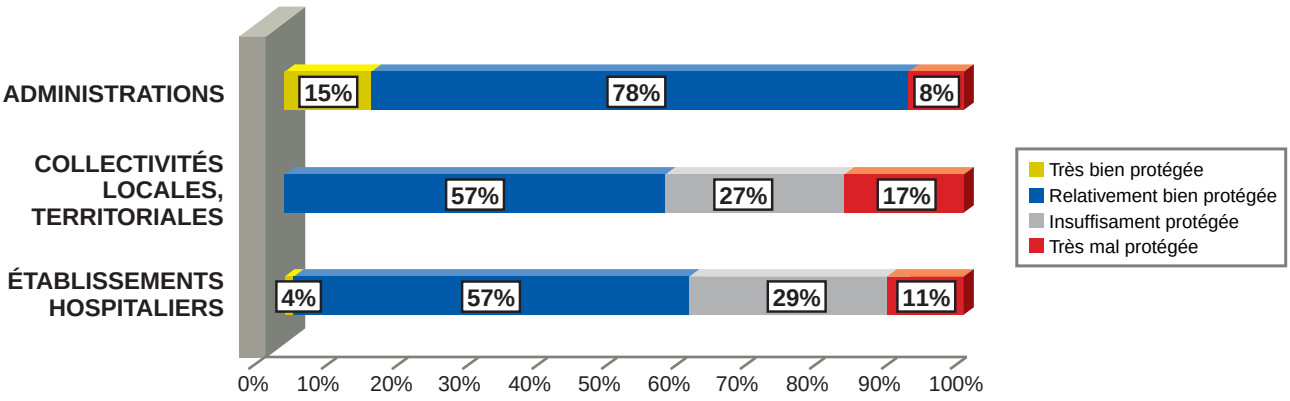


Le pourcentage d'erreurs d'utilisation correspond à une réalité opérationnelle. Sur la partie droite de ce graphe, les sinistres allant de l'infection par virus aux attaques logiques ciblées représentent bien la situation réelle. L'autre partie traduit quant à elle la difficulté de traiter les déclarations d'incidents et d'instaurer une relation de confiance entre l'enquêteur et l'enquêté.

Synthèse et tendances

Le sentiment positif de protection des collectivités publiques s'établit à 76 %, répartis entre 8 % de "très bien protégée" et 68 % de "relativement bien protégée".

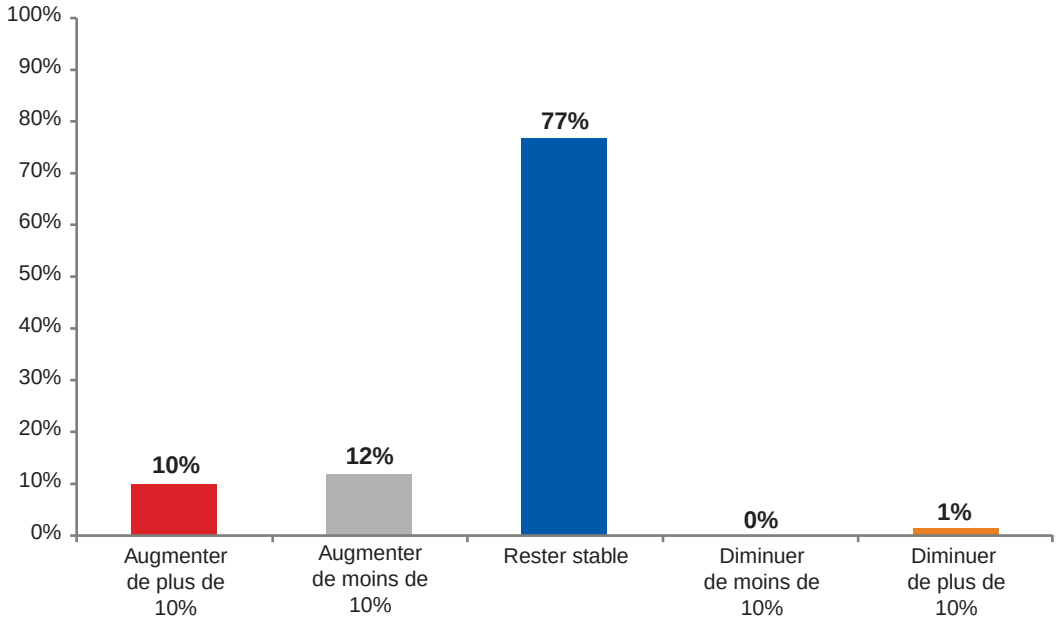
Répartition par secteur :



Les établissements hospitaliers, malgré un engagement important des moyens mis en œuvre, ne développent pas un sentiment de confiance corrélatif.
Les collectivités territoriales expriment un sentiment plus fort d'inquiétude.

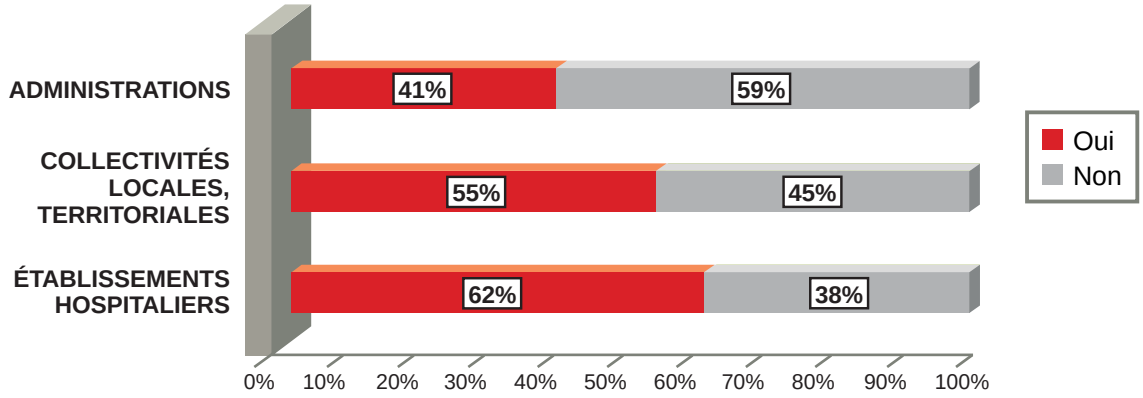
<u>Perspectives financières et techniques à deux ans</u>

Majoritairement, l'augmentation des ressources sécurité n'est pas envisagée :



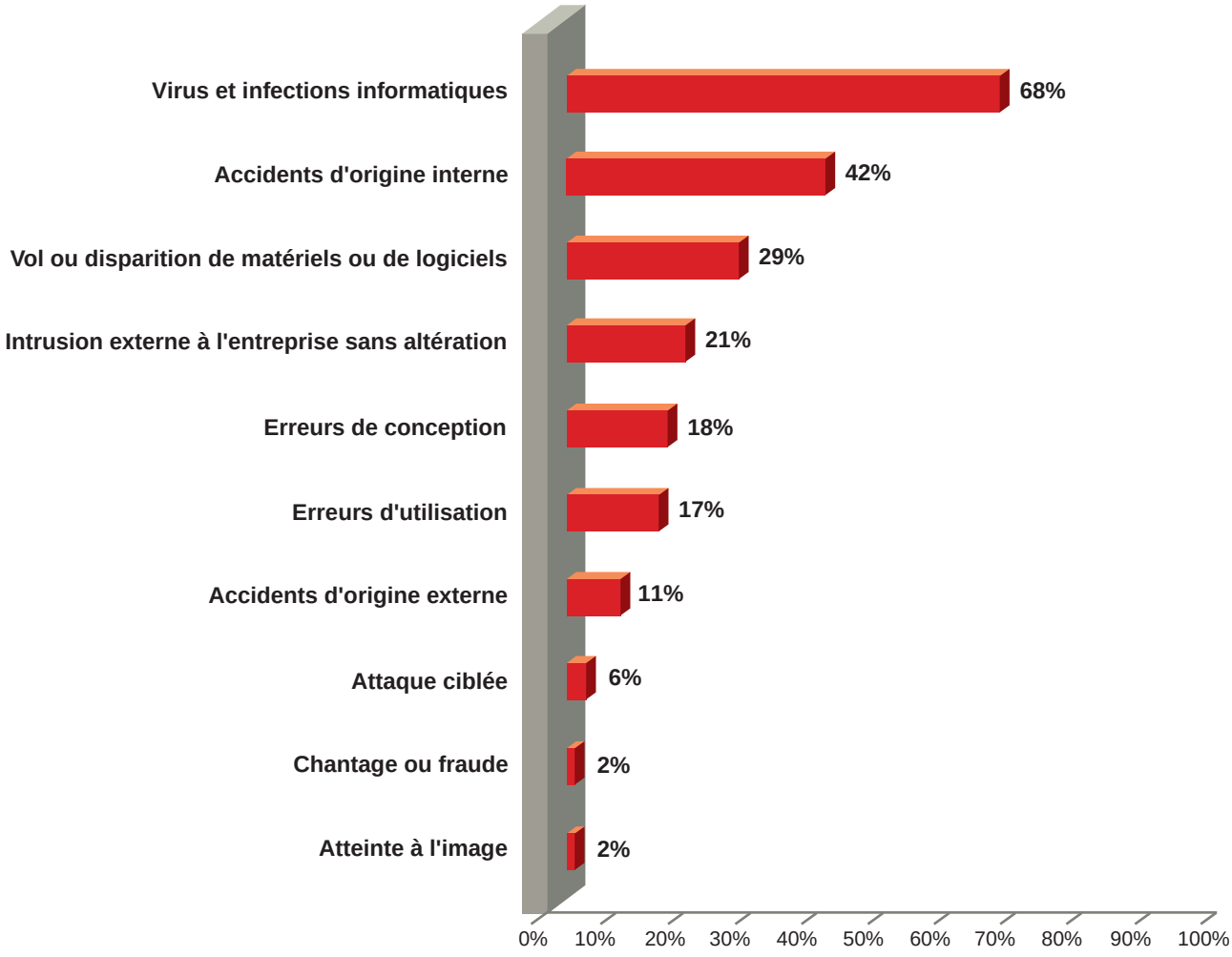
Dans les deux prochaines années, 22 % des collectivités publiques souhaiteraient se voir allouer des ressources consacrées à la sécurité.

Le renforcement des dispositifs de prévention des risques est annoncé par 49 % des organismes :



Quels risques pour l'avenir ?

Voici le classement des risques potentiels :



La répartition par secteur apporte un éclairage supplémentaire :

	ADMINISTRATIONS	COLLECTIVITÉS LOCALES, TERRITORIALES	ÉTABLISSEMENTS HOSPITALIERS
Virus et infections informatiques	**72 %**	**64 %**	**60 %**
Accidents d'origine interne	**36 %**	**50 %**	**44 %**
Erreurs de conception	**17 %**	**18 %**	**20 %**
Intrusion externe à l'entreprise sans altération	**17 %**	**25 %**	**28 %**
Erreurs d'utilisation	**14 %**	**14 %**	**28 %**
Vol ou disparition de matériels ou de logiciels	**14 %**	**54 %**	**28 %**
Accidents d'origine externe	**8 %**	**11 %**	**20 %**
Attaque ciblée	**3 %**	**7 %**	**12 %**
Atteinte à l'image	**0 %**	**4 %**	**4 %**
Chantage ou fraude	**0 %**	**4 %**	**4 %**

La comparaison entre la réalité des sinistres subis et la crainte des risques redoutés fait ressortir des perceptions très contrastées, ne serait-ce que concernant le vol ou l'intrusion.

Glossaire

Accident physique :
incident d'origine non intentionnelle ayant porté atteinte à l'intégrité du système d'information, tels que incendies, explosions, dégâts des eaux...
Les sinistres ayant une cause naturelle ne sont pas inclus dans cette catégorie.

Acte de dénigrement ou d'atteinte à l'image :
acte utilisant les technologies informatiques et visant à porter atteinte à l'image, par exemple par le piratage de pages web.

Attaque logique ciblée :
virus et autres attaques comme destruction manuelle des données, déni de service, mail bombing, bombe logique, cheval de Troie, visant une structure de façon isolée dans le but de lui faire d

Audit/conseil :
prestations externes regroupant exclusivement l'audit sécurité des SI (audit, tests d'intrusion, analyses de risque…) et le conseil en sécurité (management, schéma directeur, conseil en architecture, conseil en continuité, coaching…), à l'exclusion de toute prestation opérationnelle (intégration, administration, supervision…).

Coût de reconstitution de données, logiciels ou procédures endommagés ou perdus :
ce coût est calculé à partir du temps passé à reconstituer dans le système d'information les éléments perdus.

Coût de renforcement des protections :
Coût de l'achat et/ou de la mise en oeuvre de nouveaux dispositifs de sécurité, suite à un incident.

Coûts de réparation ou remplacement du matériel informatique :
coût direct en matériel, auquel s'ajoute éventuellement le temps passé par du personnel de l'entreprise pour procéder aux réparations.

Code NAF :
anciennement code APE, indiquant l'activité principale de l'entreprise.

Divulgation :
communication à des tiers d'informations confidentielles.

Equivalent temps plein (ETP) :
unité de mesure de la charge de travail divisant la charge totale par le nombre de personnes la réalisant :
exemple :
1 salarié à temps plein = 1ETP
3 salariés à plein temps, mais consacrant 20% de leur temps pour la tâche concernée = 0,6 ETP

Erreur de conception :
erreur dans la programmation, la réalisation, la mise en œuvre et le déploiement de logiciels, systèmes ou procédures qui engendre des dysfonctionnements.

Erreur d'utilisation :
erreur commise par les opérateurs et les utilisateurs lors de l'utilisation du système d'information, comme une erreur de saisie.

Evénement naturel :
incident d'origine naturelle, tels que tempête, inondation, glissement de terrain…

Extranet :
extension de l'Intranet aux ressources du réseau Internet afin de donner accès à des clients ou fournisseurs à certaines applications et/ou informations internes.

Fraude informatique :
fraude utilisant le système d'information. Il peut s'agir de détournement de biens, comme une sortie de matériel, de fonds, de fraude aux télécommunications comme le piratage de PABX.

Incident :
terme entendu au sens où un virus qui touche 200 micros = un incident, un incendie qui touche la salle des serveurs = un incident.

Infection par virus :
seule est prise en compte l'infection effective, ce qui exclut les virus détectés et bloqués par le système de protection. L'infection considérée ne vise pas spécifiquement une structure, qu'elle soit de type entreprise ou collectivité publique.

Intranet :
réseau interne utilisant les technologies internet pour y diffuser de l'information et /ou partager des applications. Il se distingue d'un simple réseau par l'interface web qui le caractérise.

Mise à jour automatique :
procédé permettant la mise à jour du logiciel antivirus sans intervention humaine. Le serveur où l'antivirus est installé se connecte automatiquement, selon les paramètres de configuration entrés, au site de l'éditeur pour y télécharger les mises à jour.

Origine interne / externe / inconnue :
un sinistre est d'origine interne quant il est causé par un salarié ou un ex-salarié. Il est d'origine externe dans le cas contraire. Si l'origine n'est pas identifiée, elle sera considérée comme inconnue.

Panne d'origine interne :
panne du système d'information mais qui n'est pas de la responsabilité d'un fournisseur de service.

Perte de service essentiel :
panne d'origine externe qui touche des services dont dépend le bon fonctionnement des ressources informatiques, telles que coupures d'électricité, de service de télécommunication, d'eau (induisant la climatisation)…

Perte d'exploitation :
perte de marge due à des frais supplémentaires ou à des pertes de revenus (perte d'affaires, de clients, image).

Responsabilité encourue par l'entreprise :
coût pour l'entreprise des préjudices causés à autrui, par exemple lors de la divulgation d'information.

Sabotage physique :
dégradation volontaire de matériel informatique.

Service opérationnel :
prestation de service permettant la mise en œuvre de la sécurité (supervision à distance, hébergement de sites de secours, administration de l'infrastructure de sécurité, délégation d'expertise…)

Veille :
démarche consistant à se tenir informé de l'évolution d'un secteur donné : cadre juridique, évolution des technologies… Une démarche de veille comprend : la définition du périmètre (sur quoi porte la veille), la direction de l'effort de veille (juridique, technologique, concurrentiel…), les ressources consacrées, l'analyse et la synthèse des informations récoltées, les moyens de partage et de diffusion de ces informations.

Vol ou disparition de matériel :
à comprendre sur le plan physique.

Club de la Sécurité des Systèmes d'Information Français
30, rue Pierre Sémard - 75009 Paris
TÉL.: 01 53 25 08 80
Fax.: 01 53 25 08 88
Mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr