

# ÉTUDE ET STATISTIQUES SUR LA SINISTRALITÉ INFORMATIQUE EN FRANCE ANNÉE 2002

Pour les entreprises et les collectivités publiques, 2002 a été marquée par deux grandes tendances :

- une accélération de l'ouverture des systèmes d'information
- une forte augmentation des infections par virus

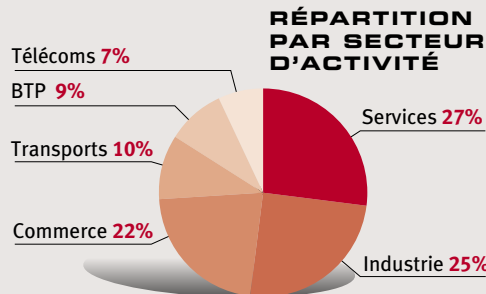
Si les moyens humains, organisationnels, techniques, sont globalement en progression, la conception et la mise en place d'une stratégie globale de sécurité restent encore trop marginales.

*“La comparaison entre les moyens développés et la dépendance forte [des entreprises vis-à-vis de leur système d'information] 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.”*

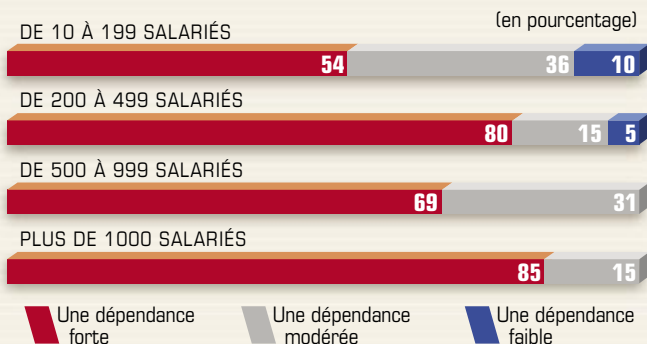
Le chemin est encore long pour passer d'un sentiment de confiance à une sécurité maîtrisée.

L'essor de la société numérique doit aller de pair avec une forte mobilisation de tous : décideurs, responsables techniques et opérationnels, utilisateurs finaux.

# SECTEUR PRIVÉ 600 ENTREPRISES ONT RÉPONDU À L'ENQUÊTE



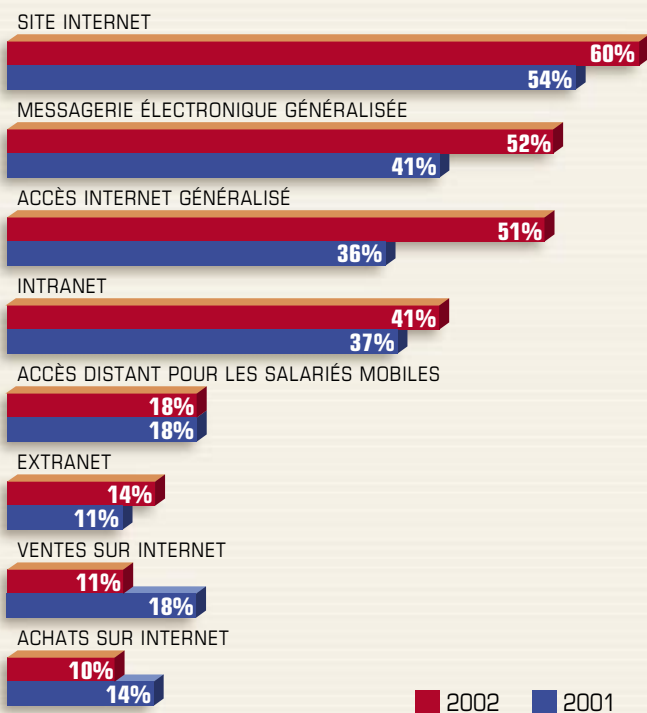
## UN SENTIMENT DE DÉPENDANCE QUI S'INFLÉCHIT



Les entreprises annoncent une dépendance moins forte en 2002. *“Dans une société de plus en plus numérique, la question se pose de savoir sur quels critères objectifs peut s'appuyer cet infléchissement”.*

Les effectifs creusent les disparités, non moins que les secteurs d'activité. Toutefois, cette rupture de perception n'est pas pour autant le reflet de la réalité, notamment pour les PME.

## UNE OUVERTURE DES SYSTÈMES EN FORTE PROGRESSION



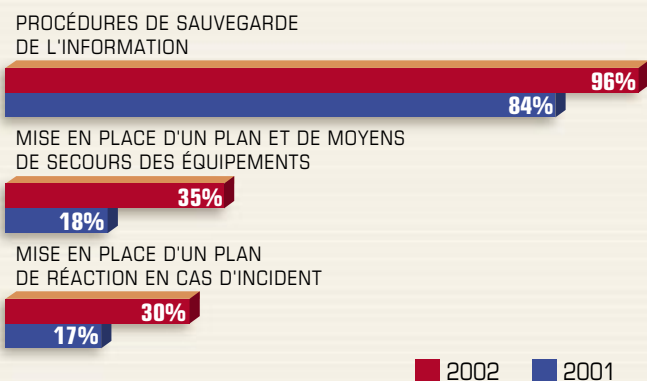
Ce sont la messagerie électronique et l'accès Internet généralisés qui enregistrent la plus grande progression dans l'ouverture des systèmes d'information.

Les opérations de commerce en ligne font exception à cette ouverture.

*“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 1 000 salariés se démarquent à 24%”.*

Une scission très nette apparaît à partir de 200 salariés, avec 59% de sites internet en deçà contre plus de 80% au-delà.

## CONTINUITÉ D'ACTIVITÉ : DES PROGRÈS INSUFFISANTS



Si les procédures de sauvegarde sont généralisées quels que soient l'effectif et le secteur, il n'en est pas de même pour les plans de secours et les plans de réaction.

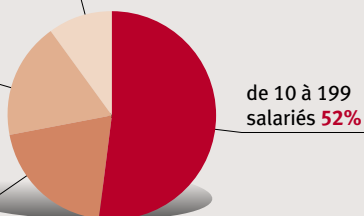
*“L'augmentation constatée semble le début d'une prise de conscience qui appelle un renforcement au regard des niveaux de dépendance. Les événements de l'automne 2001, aux Etats-Unis et à Toulouse, ainsi que les craintes liées à la crue centennale en région parisienne peuvent aussi se refléter dans ces chiffres”.* Dans cet esprit, il ne s'agit plus de la seule continuité d'un service informatique mais de la pérennité de l'activité économique.

Plus de 1000 salariés **10%**

de 500 à 999 salariés **18%**

de 200 à 499 salariés **20%**

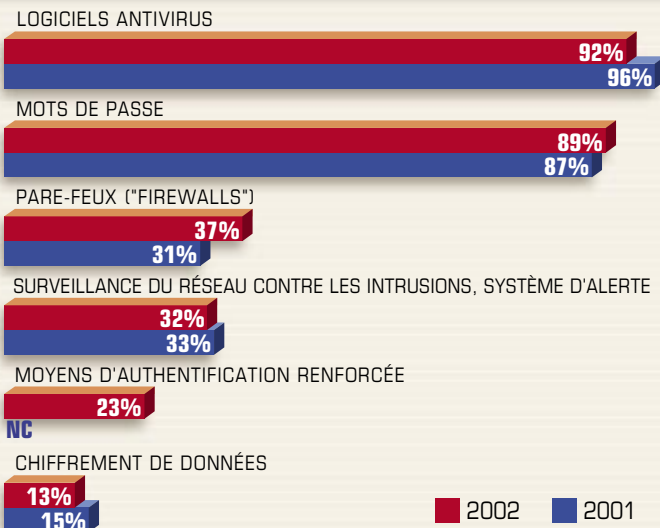
## RÉPARTITION PAR EFFECTIF



## EXPERTISE

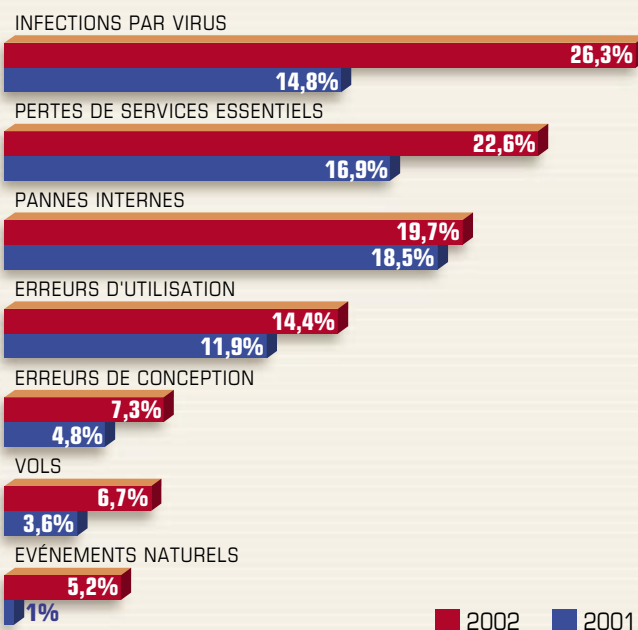
Le Clusif a fait appel à des experts d'horizons variés pour commenter les statistiques. Des extraits sont reproduits en italique dans ce document.

## ENCORE TROP PEU DE PARE-FEUX



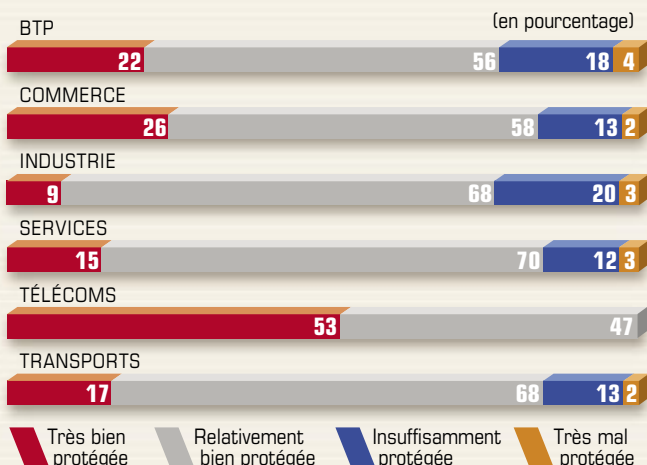
Il est inquiétant de constater le faible niveau de déploiement de pare-feux et de système de détection d'intrusion. Le rapprochement avec l'effectif et le secteur d'activité permet de constater que cette carence est largement imputable aux entreprises de moins de 200 salariés et que tous les secteurs sont concernés. A l'heure d'une ouverture marquante des systèmes d'information et d'une dépendance forte des entreprises, la prise de conscience des risques liés est insuffisante.

## DES SINISTRES DÉCLARÉS EN PROGRESSION



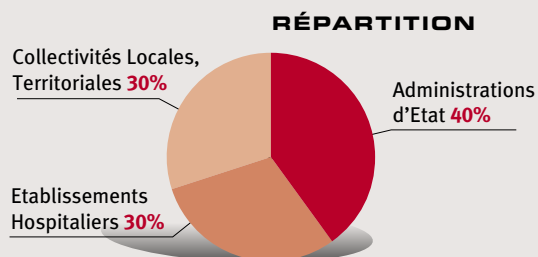
60% des entreprises déclarent n'avoir subi aucun sinistre. Il semble évident que de nombreux incidents ne sont pas comptabilisés, car non détectés. La tendance générale est de relativiser l'impact des sinistres récurrents. Les événements naturels sont cités, à 23%, en première position d'impact fort, le virus ne se situant qu'à 15%. L'évaluation financière des incidents reste encore très marginale. Pourtant "ce calcul est l'un des moyens permettant de justifier les dépenses en matière de sécurité. Pour un RSSI, il s'agit d'un levier pour dégager des budgets. D'autre part, 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."

## UNE PROTECTION RESSENTIE À DEGRÉ VARIABLE



Des différences notables apparaissent selon les secteurs d'activité. Il s'agit bien là d'un sentiment, qui ne repose pas toujours sur des éléments concrets. Ainsi, "les Télécoms se sentent, à 100%, très bien ou relativement bien protégés, avec une ouverture très forte de leurs systèmes d'information et la mise en œuvre à 43% de pare-feux." Le rapprochement avec les autres graphes de l'étude fait état d'un décalage entre sentiment de dépendance et sentiment de protection. Celui-ci peut s'expliquer par une incohérence de démarche ou des délais de déploiement d'une politique de sécurité.

# 100 COLLECTIVITÉS PUBLIQUES ONT RÉPONDU À L'ENQUÊTE



Les écarts souvent significatifs entre les trois catégories s'expliquent par des différences d'organisation. Ainsi, *“les administrations centrales et déconcentrées gèrent des réseaux nationaux alors que les collectivités territoriales et les établissements hospitaliers présentent des situations très disparates... Leur comportement [des collectivités territoriales] est assez proche de celui des PME où le rôle d'un maire peut être comparé à celui d'un chef d'entreprise.”*

Les systèmes d'information sont largement ouverts, particulièrement dans les administrations d'Etat : 84 % d'accès à un Intranet et 61 % d'accès distant pour les salariés mobiles.

La sécurité physique est assurée en priorité par les onduleurs et dispositifs anti-incendie. La plupart des moyens techniques, humains et organisationnels sont au diapason. Cependant, certains sont encore peu développés, notamment les moyens d'authentification renforcée : *“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.”* L'attention est attirée par la mise en œuvre à 51 % de pare-feux en cas d'ouverture de site internet ; ce résultat demande à être relativisé *“du fait que les agents de l'Etat n'ont pas toujours conscience des équipements qui sont mis en œuvre par les hébergeurs ou les prestataires.”*

Près de 2/3 des collectivités publiques ne déclarent aucun incident. Les infections par virus et les pertes de services essentiels sont les deux causes les plus déclarées de sinistres.

RETROUVEZ L'INTÉGRALITÉ  
DE L'ÉTUDE EN LIBRE TÉLÉCHARGEMENT  
SUR [www.clusif.asso.fr](http://www.clusif.asso.fr)

Egalement disponibles en libre téléchargement sur le site du Clusif :

LES PANORAMAS  
DE LA CYBERCRIMINALITÉ

LES SYNTHÈSES  
DU CLUSIF



L'ESPRIT DE L'ÉCHANGE

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 produits et services en SSI. Cette diversité fait sa force en favorisant le développement de synergies.

Tous les secteurs de l'économie française, public et privé, sont représentés au sein du CLUSIF qui dispose de relais régionaux, - les CLUSIR -, et d'homologues européens en Belgique, Italie, Luxembourg, Suisse.

Il compte aujourd'hui plus de 600 membres qui bénéficient de ses services.

Pour plus d'informations :  
CLUSIF  
30 rue Pierre Sémard  
75009 Paris

Tél. : 01 53 25 08 80  
Fax : 01 53 25 08 88  
E-mail : [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr)