



L'ESPRIT DE L'ÉCHANGE

# ANALYSIS AND STATISTICS ON COMPUTER SYSTEM LOSSES IN FRANCE 2002



For business and public authorities alike, 2002 was characterised by two key trends:

- acceleration of the openness of information systems
- a strong increase in virus infections

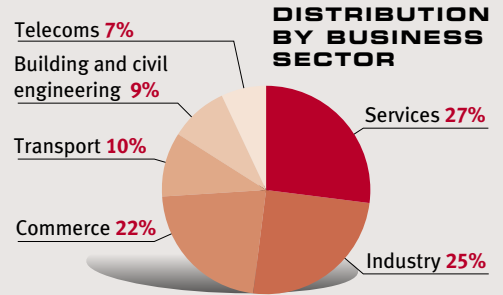
Although human, organisational and technical means are developing overall, the design and application of global security strategies remain the exception rather than the rule.

*“A comparison of the means deployed and the strong dependency [of companies on their information systems] forces the question of whether this is due to lack of management awareness, lack of time or a fully measured and voluntarily accepted risk.”*

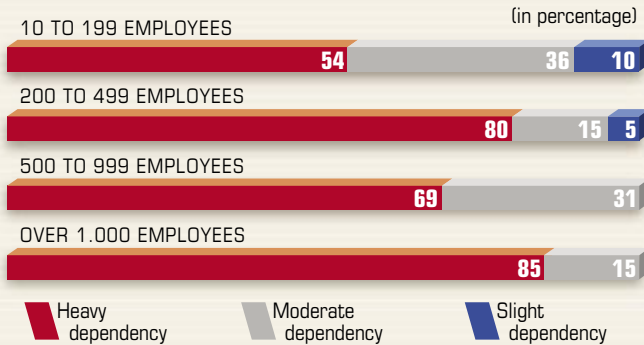
There is still a long way to go to move from a feeling of trust to a situation of controlled security.

The surge of our information exchange based society must be accompanied by strong action from all: decision makers, technical and operational managers, end users.

# PRIVATE SECTOR 600 COMPANIES ANSWERED THE SURVEY



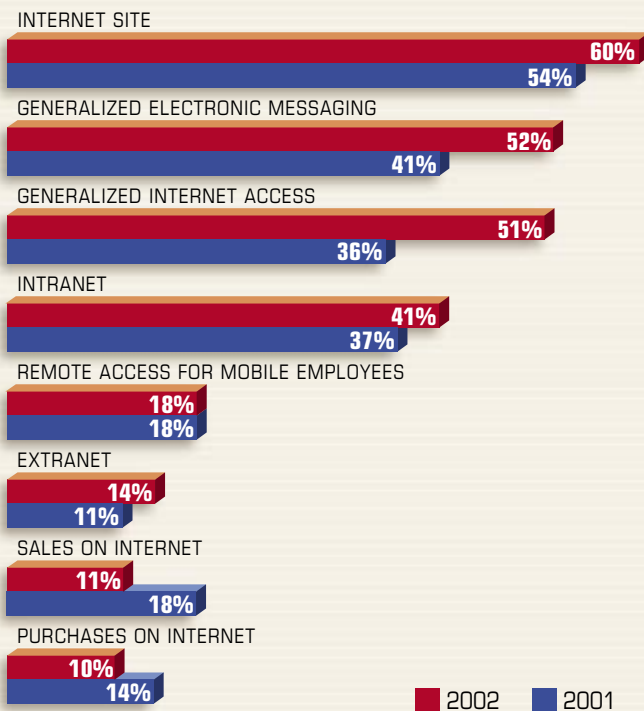
## A FEELING OF DEPENDENCY WHICH IS DECLINING



Companies announced a lower degree of dependency in 2002. *"In an increasingly digital based society, we must raise the question of what objective criteria are behind such a reduction."*

A company's dependency is perceived very differently according to the number of employees and the sector of activity. However, this change in perception is not a true reflection of reality, especially for SMEs.

## INCREASINGLY OPEN SYSTEMS



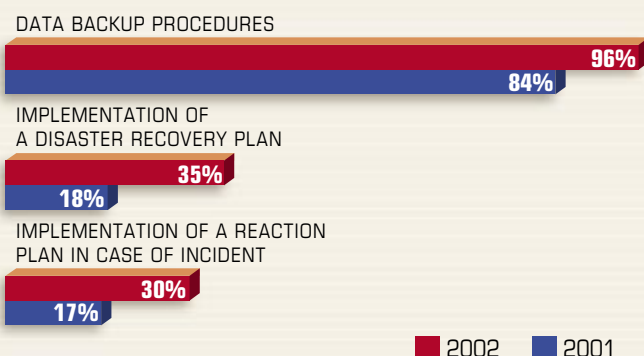
The increasingly widespread use of email and internet is behind this fast advance in the openness of information systems.

On line trading is the exception here.

*"The reduction in sales and purchases over the internet shows that our trust in the digital economy is not yet established. For purchases, only companies with over 1000 employees go against this downward trend"* (24%).

A clear divide appears at companies with 200 employees, 80% with more than this number of employees have internet sites whereas 59% of companies with less than 200 employees have sites.

## CONTINUITY OF ACTIVITY: INSUFFICIENT PROGRESS



Even though backup procedures have become generalised, whatever the company size and sector, the same is not true for disaster recovery and reaction plans.

*"The observed increase seems to be the beginning of a wider understanding that greater care needs to be taken with respect to dependency. The events in autumn 2001 in the United States and Toulouse and the fears around centennial flooding in the Parisian basin may also be factors in this development."*

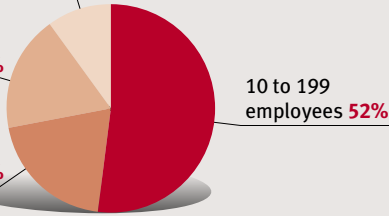
The underlying challenge is no longer simply the continuity of the computer service but the long term future of the business activity.

Over 1.000 employees **10%**

500 to 999 employees **18%**

200 to 499 employees **20%**

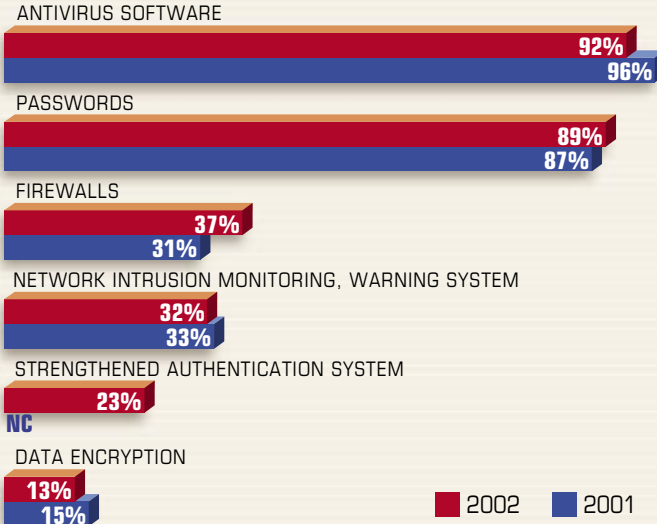
### DISTRIBUTION BY WORKFORCE



## EXPERTISE

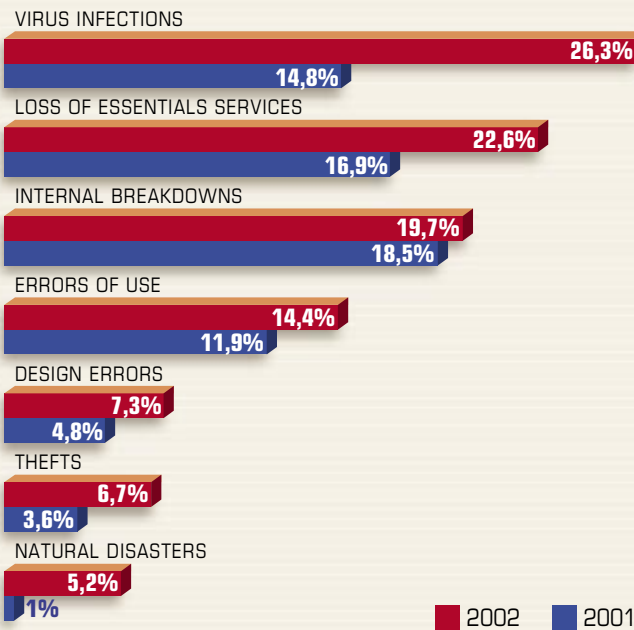
The Clusif has called upon experts from a wide range of fields to comment upon these statistics. Extracts from their comments are represented in *Italics* in this document.

## STILL TOO FEW FIREWALLS



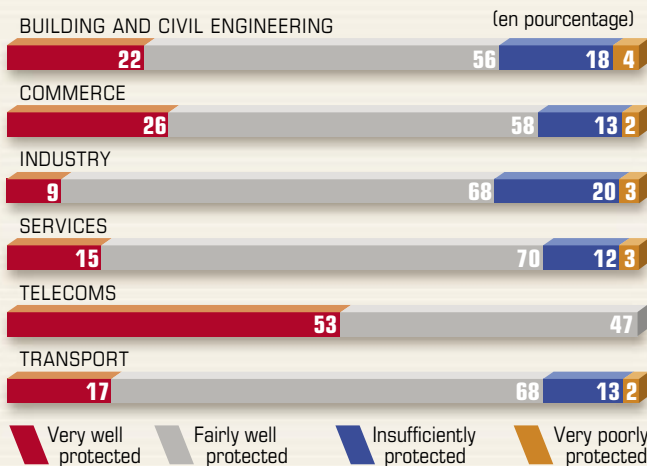
It is worrying to observe the low level of deployment of firewalls and intrusion detection systems. Analysis in terms of number of employees and sectors of activity highlights the fact that the low level of firewall deployment mainly concerns companies with fewer than 200 employees across all sectors of activity. As information systems are becoming increasingly open and companies increasingly dependent on computers, there is clearly insufficient awareness of the related risks.

## AN INCREASE IN RECORDED LOSSES



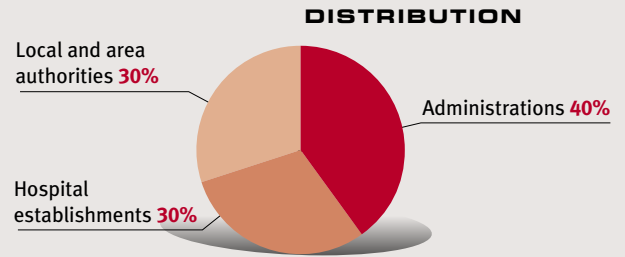
60% of companies state that they have never suffered any prejudice. It would appear that numerous incidents are not recorded because not detected. The general trend is to play down the impact of recurrent problems. Natural phenomena are mentioned in first place of problems occurring at 23%, virus impact accounts for just 15% of damage or loss. Financial evaluation of incidents remains marginal. However, *“such a calculation would be one of the means to enable justification of expenditure on security. For an Information Security Officer this would be a means to increase budget applications. Indeed, we observed that companies generally estimate the impact of accidents or losses as low but do not make any formal evaluation which in turn raises the question of what are the tangible elements upon which they have based their answer in the first place.”*

## PROTECTION PERCEIVED AT VARYING DEGREES



Wide differences appear across different sectors of activity. This is a general feeling which again is not based on concrete elements. For example, *“telecommunications companies feel 100% very well or relatively well protected with a well developed openness of their information systems and a 43% deployment of firewalls.”* Comparison with the other graphs in the study reveals a lag between the feeling of dependency and the feeling of protection. This may be explained by a certain incoherence in the procedures or deployment schedules of security policies.

# 100 PUBLIC AUTHORITIES ANSWERED THE SURVEY



Significant differences between the three categories can be explained by organisation differences. Thus, *“central and decentralized administrations manage national networks whereas local authorities and hospital establishments present a wide variety of situations... The behaviour [that of local authorities] is similar to that of SMEs where the role of a mayor could be compared to that of a company director.”*

Information systems are generally open, especially in State administrations: 84% access to an Intranet and 61% remote access for mobile employees.

Physical security is ensured by UPS equipment and fire protection systems. Technical, human and organisational resources are generally in line with the norm. However, some security solutions are still underdeveloped, notably that of strengthened authentication: *“evolution from passwords or protected access systems to other means of protection is a long winded process.”*

A noteworthy figure is the 51% deployment of firewalls when opening an internet site; this result should be considered in relative terms *“given that State employees are not always aware of the systems deployed by service providers and suppliers.”*

Nearly 2/3 of public authorities declared no incidents. Virus infections and loss of key services were the two main prejudices declared.

READ THE FULL REPORT  
FREE DOWNLOAD ON  
[www.clusif.asso.fr](http://www.clusif.asso.fr)

Equally available for free download from the Clusif site:

PANORAMA  
OF CYBERCRIME

CLUSIF  
GUIDELINES



L'ESPRIT DE L'ÉCHANGE

CLUSIF was established in 1984. It is a gateway for exchange, open to all those involved in the Security of Information Systems: from end users to security service providers and product developers. Such diversity represents CLUSIF's strength, through the development of synergies between all involved.

All sectors of the French economy, public and private, are represented within the CLUSIF which equally has regional offices - CLUSIR - and European parallel organisations in Belgium, Italy, Luxemburg and Switzerland.

Today, its services are used by over 600 members.

For more information:

Clusif  
30 rue Pierre Sémard  
75009 Paris FRANCE

Tél.: 33 1 53 25 08 80  
Fax: 33 1 53 25 08 88  
E-mail : [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr)