



# Analysis and statistics on computer system losses in France

**Year 2002**



**National survey carried out on behalf of CLUSIF by GMV Conseil**

# Contents

■ Acknowledgements _____	4
■ Summary _____	5
■ <b>METHOD OF INVESTIGATION</b>	
■ New developments in 2002 _____	7
■ Method of investigation _____	7
■ Characteristics of the sample _____	8
■ <b>COMPANIES</b>	
■ Environment of information systems _____	12
A feeling of dependency which is declining _____	12
Increasingly open systems _____	13
■ Organisation and resources _____	14
A security policy in need of reinforcement _____	14
Security resources on the increase _____	16
Employee awareness: a priority _____	17
■ Evaluation of losses _____	22
An increase in recorded losses _____	22
■ Summary and trends _____	25
■ <b>PUBLIC AUTHORITIES</b>	
■ Environment of information systems _____	31
■ Organisation and resources _____	33
■ Evaluation of losses _____	38
■ Summary and trends _____	39
■ <b>GLOSSARY</b> _____	42

# Acknowledgements

---

## The expert committee

CLUSIF wishes to thank the companies and public bodies which gave it the benefit of the skills of their 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

## The losses committee

CLUSIF wishes to thank those active members who made possible the execution of this study

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

# Summary

---

Founded in 1984, CLUSIF 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 are represented, both public and private. Today, its services are used by over 600 members.

For the third consecutive year, CLUSIF surveys the incidence of computer system losses in France, for the year 2002.

The sample was defined on the basis of complete replies from 600 companies - 6 business sectors - and 100 public authorities - 3 categories. The comparisons between 2002 and 2001 relate to the private sector only.

2002 was marked by two major trends:

- ◆ increasingly open information systems.

The increasingly widespread use of email and internet is behind this fast advance. On line trading is the exception here.

- ◆ a strong increase in virus infections.

On the one hand, 60% of companies state that they have never suffered any loss, and it seems clear that many incidents are not detected. On the other hand, such losses are still very rarely evaluated, so that the financial costs engendered are not very visible. What, then, are the grounds for this feeling of low impact ? As regards viruses, a strong impact only affected 15% of companies.

While human, organisational and technical resources are on the increase overall, the design and application of global security strategies still remain far too rare. At a time of striking increase in the numbers of highly dependent systems, awareness of the related risks is insufficient.

*"Companies train, do not set out formal guidelines, and carry out checks even less".*

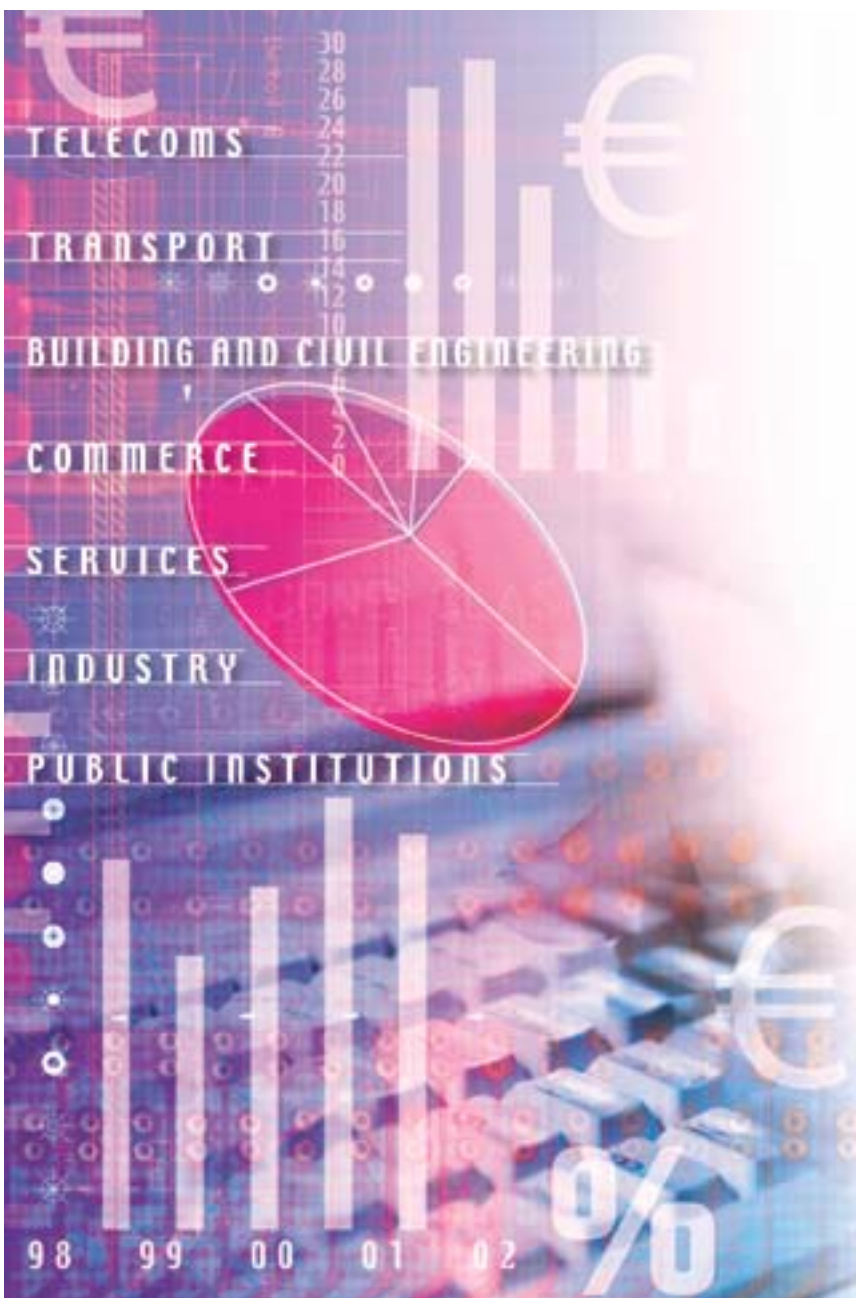
Unlike procedures for data back up, which are widespread, plans for disaster recovery and reaction lag behind. Yet in cases of serious losses, the underlying challenge is no longer simply the continuity of the computer service, but the long term future of the business activity.

The feeling of protection claimed by companies reveals a lag to their dependency and the resources brought into play. This may be explained by delays in deployment schedules of security policies, or incoherence in the procedures.

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

The surge of the digital society must be accompanied by strong action from all: decision-makers, technical and operational managers, and end users.

# METHOD OF INVESTIGATION



# Method of investigation

---

The method established by CLUSIF makes it possible to assess information system losses in France with greater refinement each successive year.

These studies enable:

- ◆ an appreciation of information system losses resulting from accidents, errors and dishonest acts, in terms of incidence, recurrence and impact,
- ◆ assessment of the resources brought to bear to counter these risks,
- ◆ a presentation of the overall picture and a view of prospects in security needs.

In order to enrich these studies, CLUSIF calls upon experts in a variety of fields, whose comments are incorporated and are indicated by a green box:

---

## *Example of expert comment*

---

These studies form an integral part of CLUSIF's mission of raising awareness of the security of information systems.

## **New developments in 2002**

The main developments concern:

- modification of the public sector and private sector questionnaires, with the introduction of new items such as the implementation of security charters and facilities management contracts,
- an increase in the number of public bodies replying, up from 31 to 100,
- removal of the geographical criterion, which was seen as irrelevant,
- removal of the general view of all the data, the samples being far too widely differentiated.

## **Mode of data collection**

The data were collected by means of a questionnaire sent by fax, after identification by telephone of the person competent to reply.

This year, responses by telephone are still in the majority, this method being perceived as providing a higher level of confidentiality than a fax reply. Also, interviewees seem to prefer to receive some assistance with their answers, in view of the complexity of some of the questions. The acceptance rate by companies in the telecommunications sector was much lower than in other areas of business. Public authorities gave a warm welcome to the study, with a very low refusal rate.

## Characteristics of the sample

The sample is made up of 600 replies from companies and 100 replies from public authorities. These figures presuppose that 3.000 companies and just under 300 public authorities were contacted.

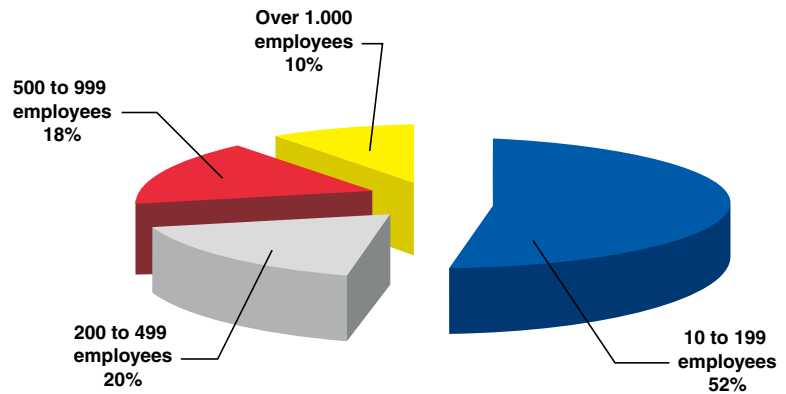
The proportion of public authorities was tripled in this study, providing us for the first time with a minimum sample amenable to adjustment.

*Data that did not exceed the threshold of 5% of responses are not taken into account, the result in such cases being insignificant. Furthermore, an annual variation of 5% or less can be explained by standard statistical deviation.*

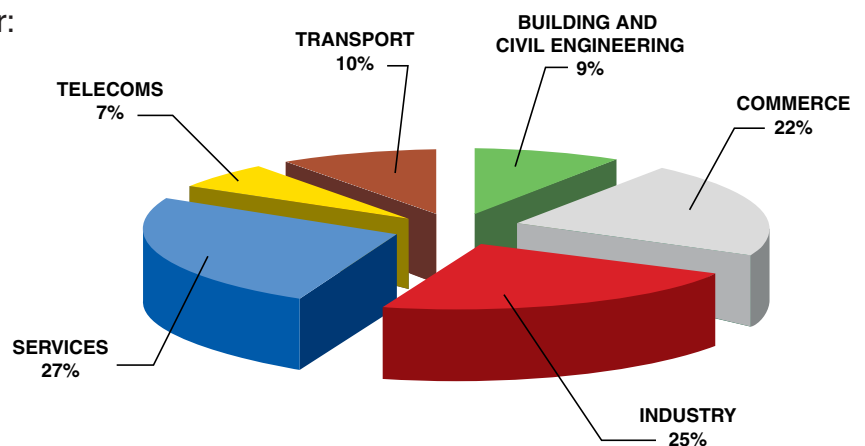
### Companies

On the basis of 600 companies with more that 10 employees, two types of analysis were adopted, workforce and business sector:

Distribution by workforce:



Distribution by business sector:



Most of these companies have a turnover figure of less than 7.6M Euros (67%)  
28% of companies with 200 to 499 employees declare a turnover of more than 150M Euros compared to more than 40% of those with 500 employees or more.

40% of companies were members of a group.

84% have only one site in France and only 16% have establishments abroad.

### A) Definition of business sectors

#### Transport

Transport by land, sea, inland waterway and air (NAF 60 to 62)

Transport auxiliary services (NAF 63)

#### Telecommunications

Postal and telecommunication services (NAF 64)

#### Industry

Mining industries (NAF 10 to 14)

Manufacturing industries (NAF 15 to 37)

Production and distribution of electricity, gas and water (NAF 40 and 41)

#### Commerce

Commercial activities, including repair of motor vehicles and domestic appliances (NAF 50 to 52)

#### Services

Hotels and restaurants (NAF 55)

Financial business (NAF 65 to 67)

Property, letting and services to companies (NAF 70 to 74)

#### Building and Civil engineering

Building (NAF 45)

### B) Adjustment of the sample of companies

The set of data on companies has been adjusted on the basis of the real distribution of the number of French companies, by workforce and business sector, registered in INSEE files.

	10 to 199 employees	200 to 499 employees	500 to 999 employees	Over 1.000 employees	Total	Total in percent		INSEE data
BUILDING AND CIVIL ENGINEERING	41	10	4	1	56	9 %	⇒	12 %
COMMERCE	70	26	22	13	131	22 %	⇒	25 %
INDUSTRY	65	39	33	15	152	25 %	⇒	25 %
SERVICES	72	28	41	20	161	27 %	⇒	27 %
TELECOMS	15	10	6	8	39	7 %	⇒	2 %
TRANSPORT	53	6	1	1	61	10 %	⇒	9 %
Total	316	119	107	58	600			
Total in percent	53 %	20 %	18 %	10 %				

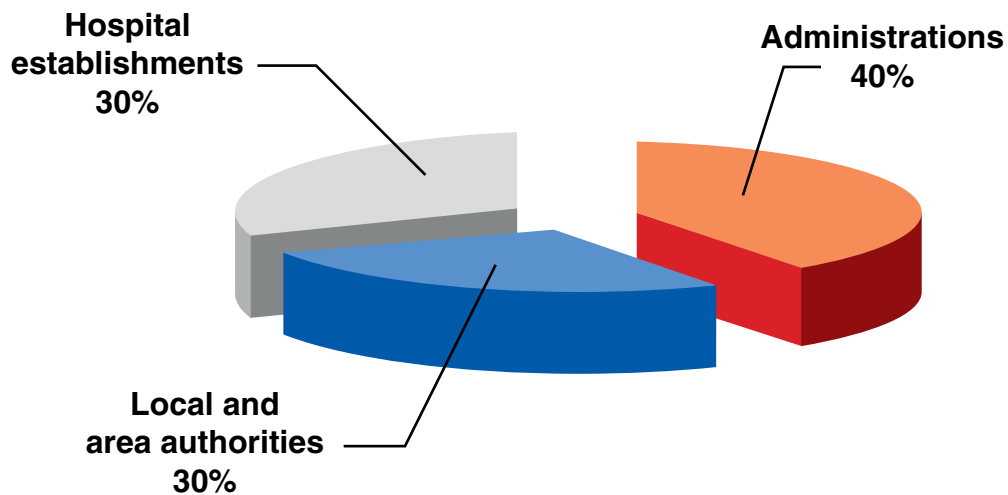
  

INSEE data	96 %	2 %	1%	1 %
------------	------	-----	----	-----

N.B. The respective proportions of small companies and business sectors in the French economy should be kept in mind for better appreciation of overall results.

### Public authorities

On the basis of 100 public authorities three categories were retained:



### C) Adjustment of the sample of public authorities

This sample has been adjusted on the basis of civil service staff numbers.

	Total	Total in percent		Civil service staff
Administrations	40	40 %	→	51 %
Local and area authorities	30	30 %	→	30 %
Hospital establishments	30	30 %	→	19 %
	100	100 %		100 %

# COMPANIES

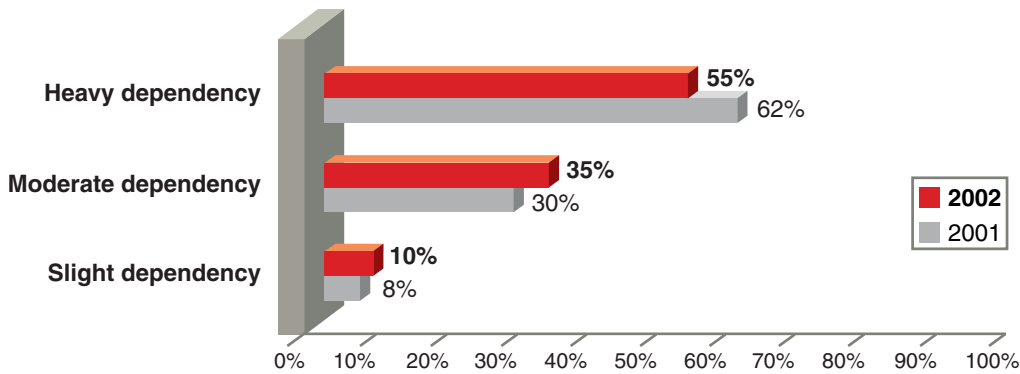


# Environment of information systems

## A feeling of dependency which is declining

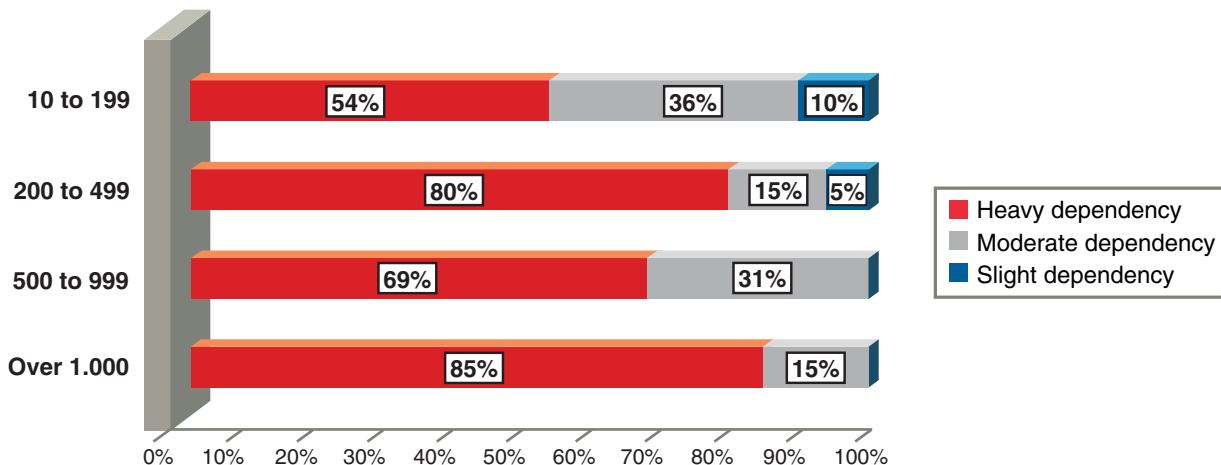
While the low level of dependency declared is still in the minority, it is interesting to note that companies declared a weaker degree of dependency in 2002.

They have a feeling of:



*In an increasingly digital society, the question arises on what objective criteria this growing confidence is based.*

Analysis by workforce reveals considerable disparities:

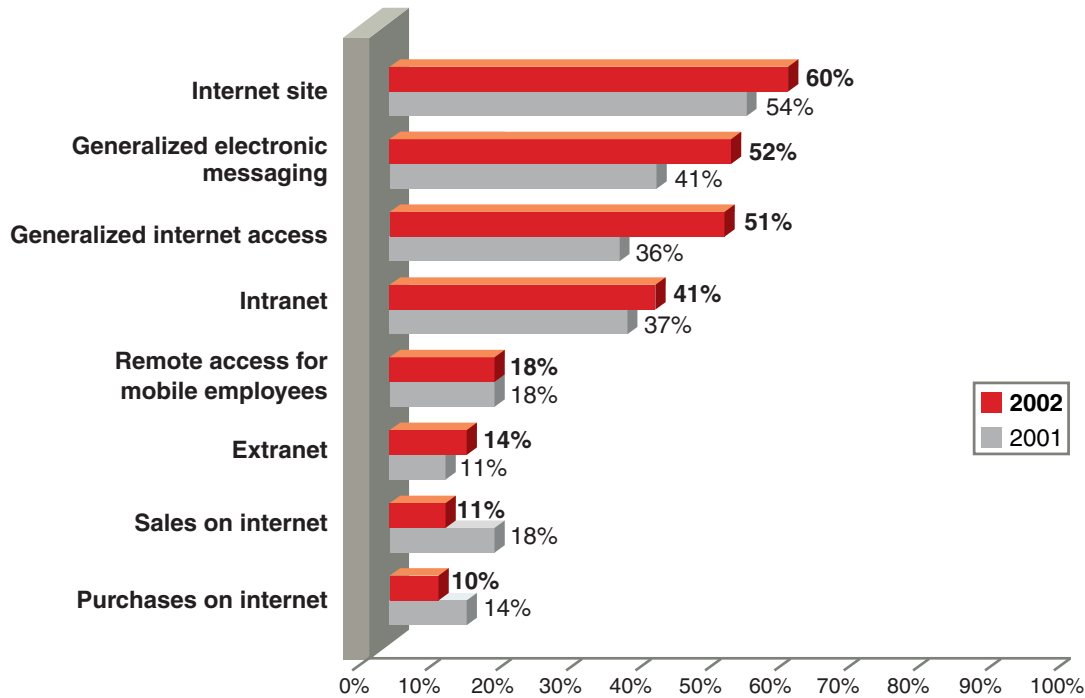


The different sectors reveal great diversity in strong dependency:

Building and Civil engineering, 33%; Transport, 49%; Industry and Services, 53%; Commerce, 67%; Telecommunications, 83%.

## Increasingly open systems

With the exception of on-line commerce operations, the openness of information systems made strong progress in 2002:



The drop in purchases and sales on the Internet shows that confidence in the digital economy is not yet established. As regards purchases, only the companies with more than 1.000 employees stand out at 24%. This figure is explained by mass orders and the transfer to Internet of EDI solutions.

Opening up of systems varies as a function of workforce and sector. A sharp division can be observed from 200 employees upward, with 59% of internet sites below this threshold, compared with 80% above it. Telecommunications, logically enough, stand out by the number of open systems; building and civil engineering lags behind as regards general electronic messaging (35%) and intranet (23%).

# Organisation and resources

---

## A security policy in need of reinforcement

64% of companies have still not defined a policy of information system security. Just 36% of companies, then, have taken this step, which is low in proportion to the 55% which declare themselves heavily dependent. Despite a slight increase compared with 2001 (30%), this observation highlights the substantial ground yet to be covered in this respect.

---

*Some companies, although they know themselves to be dependent, have not taken on board continuity of service.*

*There are several possible reasons to explain this failure to react:*

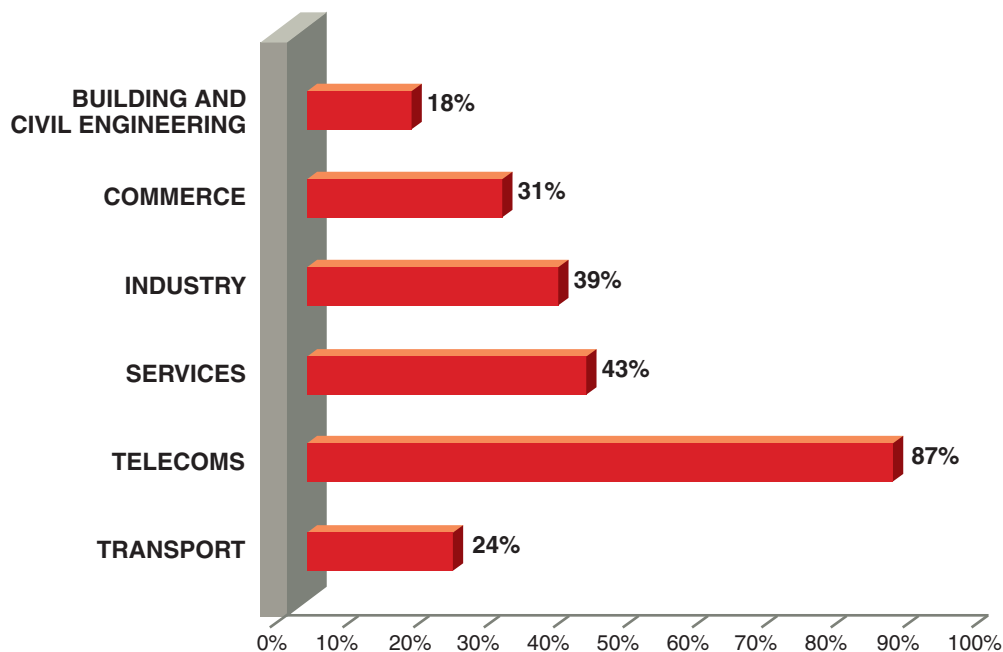
- *an IT security policy is, or appears to be, expensive to set up,*
- *companies are "hanging fire",*
- *they are becoming aware of the situation, and the procedure is getting under way,*
- *policy is in course of preparation.*

*The comparison with heavy dependency prompts the question of whether this is a matter of managerial negligence, lack of time or of taking a carefully calculated risk.*

*Looking forward, the increase in security audits (see below), which are often useful for consistency and setting up security plans, gives grounds to predict an improvement.*

---

Among these 36%, breakdown by business sectors reveals disparities:



It is with 200 employees or more that such a policy is defined, at 68%, and even more so with 500 employees or more, at 85%.

31% of companies carry out sector intelligence watch, a drop of 6 points with respect to 2001. This practice is in force particularly with 500 employees or more and in the telecommunications sector.

---

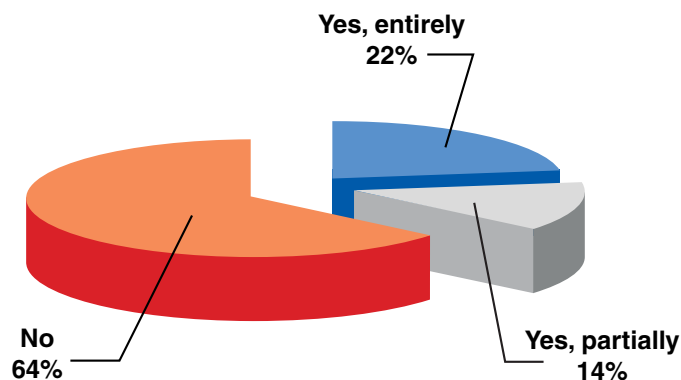
*It appears to be a legal and regulatory rather than a technical intelligence approach: indeed, examples of virus infections taking advantage of weaknesses that are known but not remedied testify to the absence, still all too frequent, of this type of intelligence gathering.*

*In addition, the reduction in the practice of internal intelligence monitoring can be partly explained by the growth in recent years of external intelligence services, especially on the vulnerability of products.*

---

### External facilities management and services

One company in three has placed all or part of its IT and telecom system under a facilities management contract.



The size of a company does not appear to be a crucial factor in taking this decision. Commerce is in the lead 51% (whole or partial), followed by Telecom businesses at 46%.

40% of companies have recourse to external suppliers of specialist services. The latter are evenly divided between audit/consulting<sup>1</sup> and operational services.

All workforce sizes are concerned to a similar extent, from 32% for companies with over 1.000 employees to 47% for the 500 to 999 band. It is surprising to note a proportion of 40% of smaller companies.

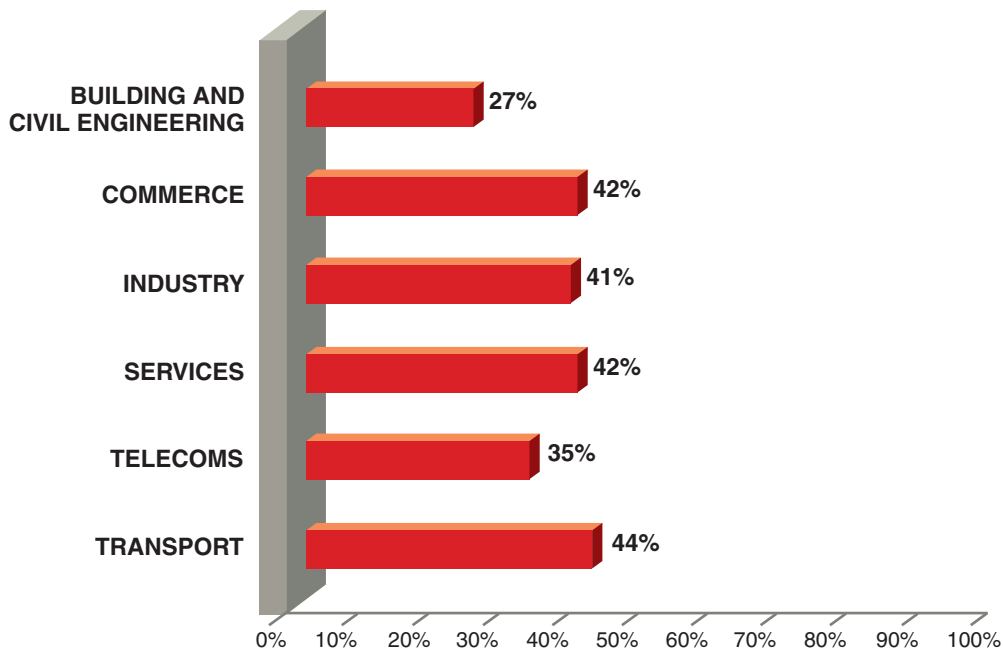
We observe that this recourse concerns:

- almost half of those companies that have set up a policy of security,
- 37% of those who have no-one in charge of IT security.

---

<sup>1</sup> The questionnaire specifies that it refers to audits of security and not to verification or operational audits.

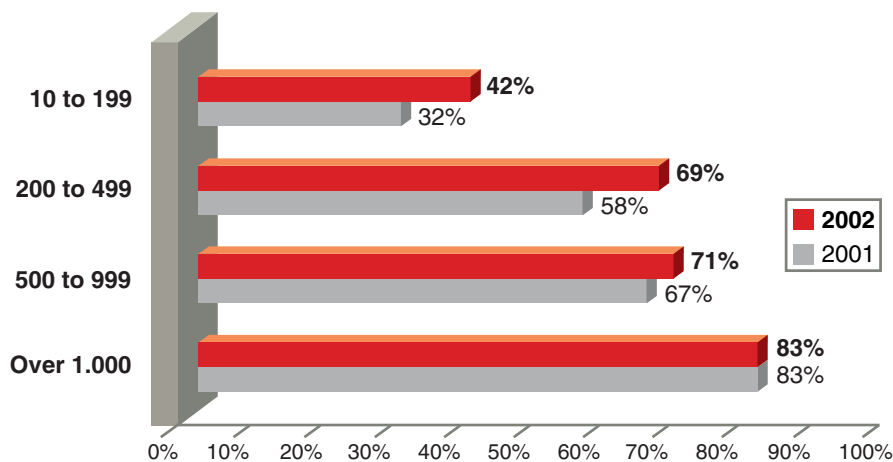
Distribution by sectors is as follows:



### Security resources on the increase

44% of companies have at least one person in charge of IT security, compared to 34% in 2001.

Proportion by size of workforce:



The greatest increases are observed in building and civil engineering, up from 15% to 33%, and in services, from 34% to 55%.

---

*Does this increase in human resources indicate an increase in the power of IT security managers in companies ?*

---

In 2002, companies had an average of 1.9 full time equivalent (FTE) posts compared to 1.4 in 2001. Even companies with less than 200 employees declared 1.6 FTE allocated to security. Nevertheless, considerable disparities are observed:

in an SME, the function of IT security manager is often an extra duty, while in larger companies it becomes a company resource in its own right.

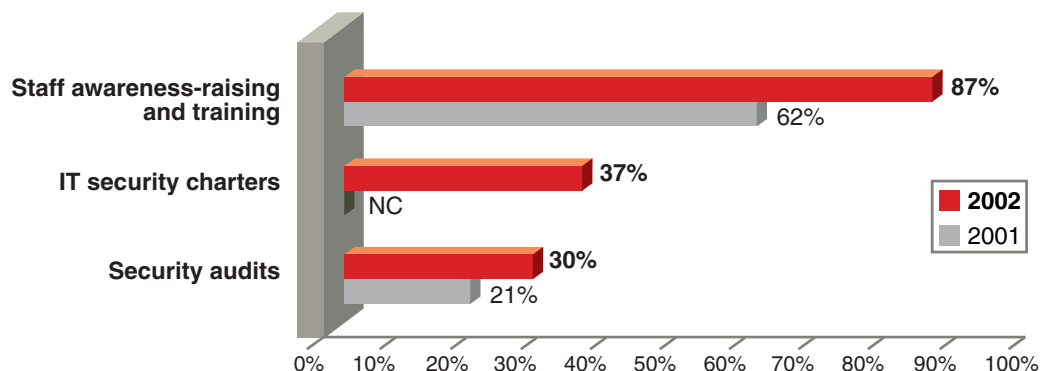
All sectors are concerned by this development with the exception of Telecom companies, which show a change from 8.3 posts to 5.

Visibility of this function in the IT budget is always uncertain : only one company in two is capable of putting a figure on it. As a function of replies received, it can be calculated at 58K euros on average. For the 2/3 of companies that replied, it is this budget that finances action relating to security, very few companies having a specific dedicated budget.

## Employee awareness: a priority

### Managing security

The determination of companies to develop an internal culture of security is patently clear:



The human factor, which is and will always remain dominant, whatever the technical resources brought to bear, is genuinely taken into account.

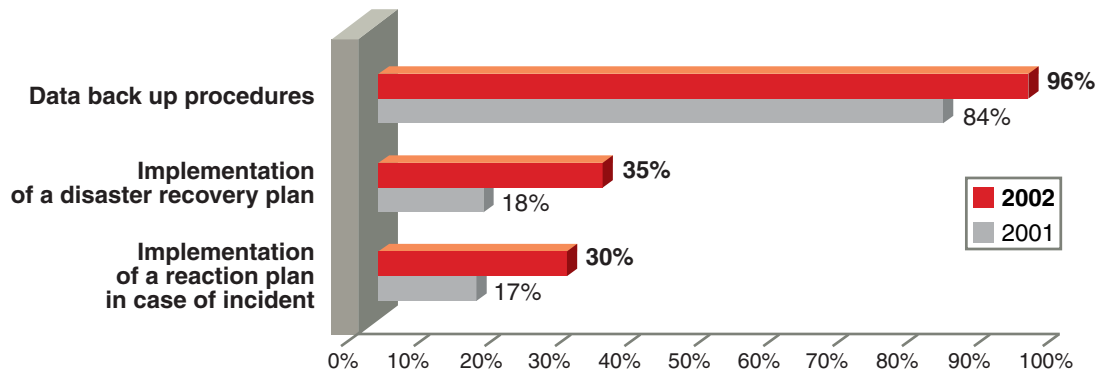
*From this graph, the following conclusion can be drawn : companies give training, but do not set out formal guidelines and carry out even fewer checks. The repercussions on company life of the problems raised by the generalized use of internet and intranet resources are experienced to the full. Yet the number of security charters introduced is relatively low, if we consider the responsibility, and even criminal liability, of both employees and their managers, in cases where these resources are abused<sup>2</sup>.*

Awareness raising applies, to more than 85%, to all business sectors and company sizes.

<sup>2</sup> In 2002, CLUSIF published a "Guide to the preparation of a charter for the use of Intranet and Internet resources", describing in detail the current context in the world of work, the risks and consequences, and the constituent elements of a charter.

## Continuity of business

While data back up procedures are in general use, disparities can be seen in the implementation of disaster recovery and reaction plans:



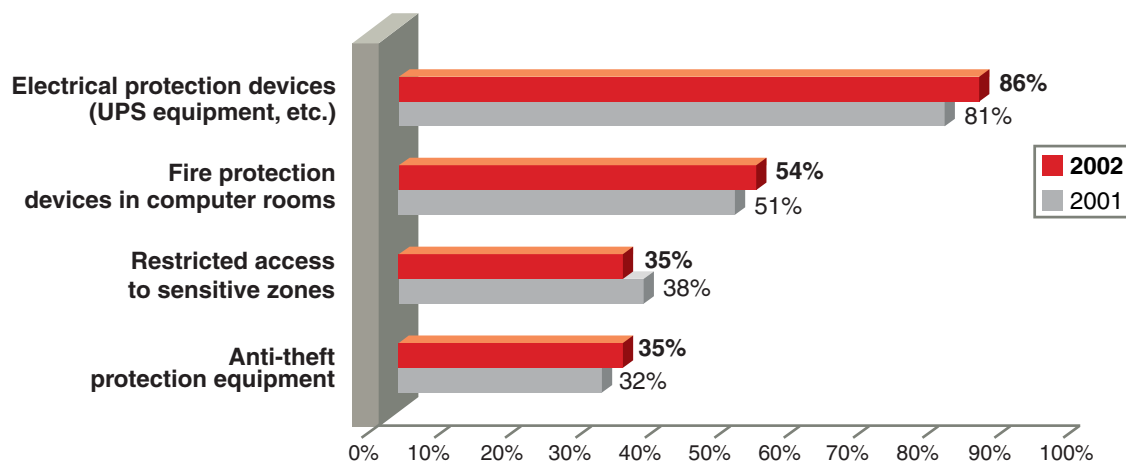
By way of example, here are the percentages of companies that have set up a plan for reaction in the event of an incident:

Building and Civil engineering	Commerce	Industry	Services	Telecoms	Transport
13 %	34 %	32 %	31 %	60 %	26 %
From 10 to 199	From 200 to 499	From 500 to 999	Over 1.000		
29 %	55 %	74 %	65 %		

*Last year, we wondered whether there would be heightened awareness as regards implementation of these plans during 2003. The increase observed seems to indicate an awakening awareness leading to closer attention being paid to levels of dependency. The events of autumn 2001, in the United States and in Toulouse, as well as fears around centennial flooding in the Parisian basin, may also be reflected in these figures.*

## Physical security

After the boom of 2001, the trend seems to indicate stability of resources put into operation:

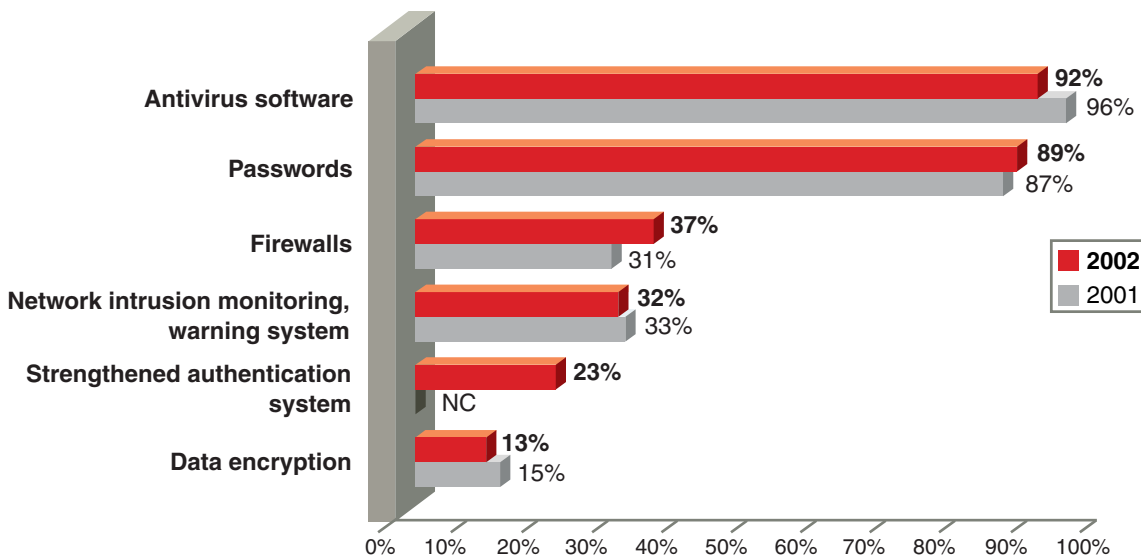


Electrical protection devices are very widespread in all company sizes, at over 85%, and whatever the sector, at over 75%.

Devices to prevent theft of equipment are mainly installed by companies of over 1.000 employees, at 71%, and Telecoms, at 60%, compared to 35% for all other sectors.

Software security

The resources put into operation are also stable, with a slight lead by firewalls:



*This stability, in parallel with the marked opening up of information systems, shows how insufficient is the development of policies of security and appropriate tools. Many companies do not seem to have realized the extent of the risks that they are running.*

The tables below give a more detailed picture of the distribution of firewalls, by company size and sector.

Installation of firewalls :

	Commerce	Industry	Services	Telecoms	Transport
Building and Civil engineering	15 %	40 %	45 %	42 %	43 %
	18 %				
From 10 to 199	35 %	80 %	83 %	89 %	

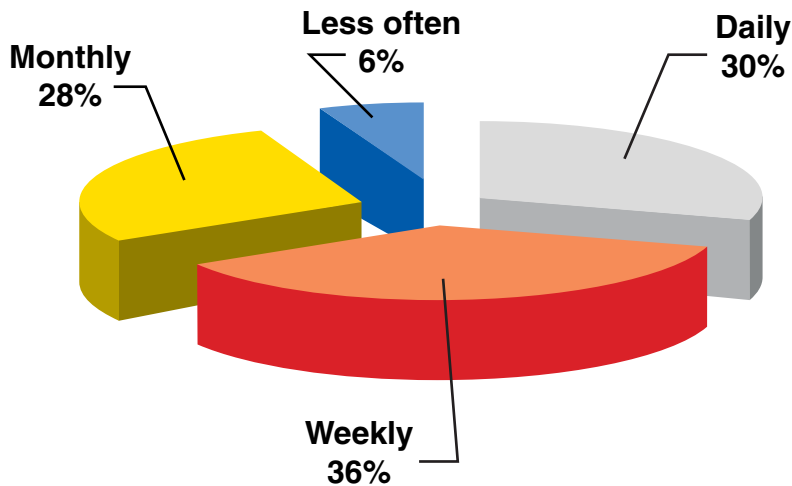
The correlation between the opening up of information systems and level of software security gives the following result:

	Internet site	Generalized electronic messaging	Generalized internet access
Antivirus software	96%	95%	95%
Passwords	93%	92%	91%
Firewalls	45%	49%	45%
Network intrusion monitoring, warning system	38%	42%	34%
Strengthened authentication system	27%	28%	24%
Data encryption	17%	19%	15%

Antivirus software

90% of companies that have installed antivirus software keep it updated. Only 30% of them carry out daily updates.

Frequency of updates:



These updates are automatic in 74% of cases, compared to 61% in 2001. They become more frequent with the size of the company, rising from 73% for those with 10 to 199 employees, to 89% for those with over 1.000.

Four sectors are positioned around the 70% mark: civil engineering, industry, services and transport. Commerce reaches 85% and telecoms 92%.

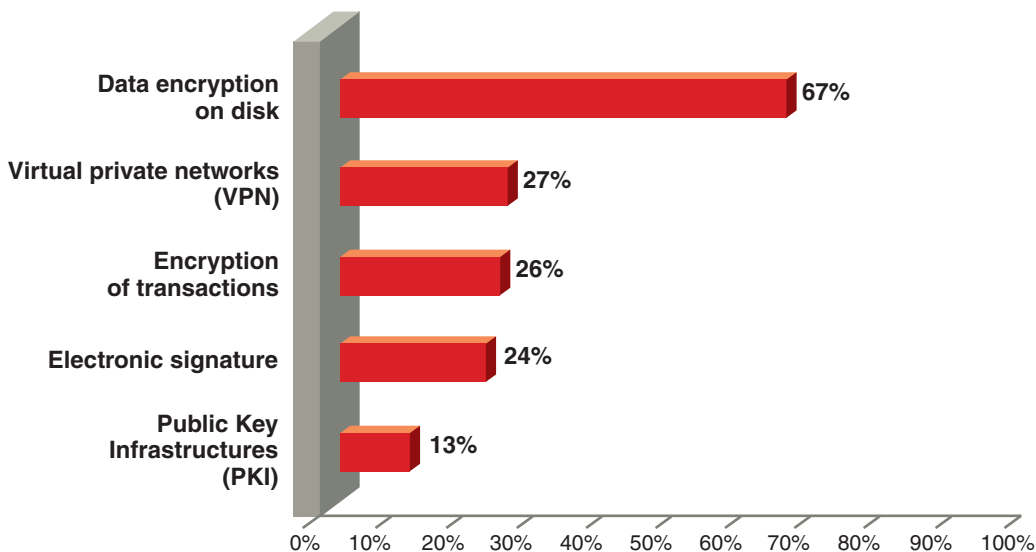
*It should be noted that about a third of companies state that they update their anti-virus software only once a month, or even less frequently, although infection by virus is strongly on the increase (+ 12 points). This frequency is far too low when we consider that some viruses propagate extremely rapidly<sup>3</sup>. Automatic daily consultation of publishers' sites to see whether any updates are available is strongly recommended.*

*We should however remark that generic antivirus technologies are available which do not seek to put a name to viruses but which simply detect virus behaviour. These are not dependent on updates based on signatures.*

### Data encryption

Only 13% of companies practise data encryption, most of which is done to secure workstation content. Encryption of transactions and PKI have not yet succeeded in making a breakthrough.

Encryption techniques used:



<sup>3</sup> The inquiry that CLUSIF carried out among its members on the Lirva virus showed that even daily antivirus updates are not always sufficient: several companies have decided to perform several updates daily.

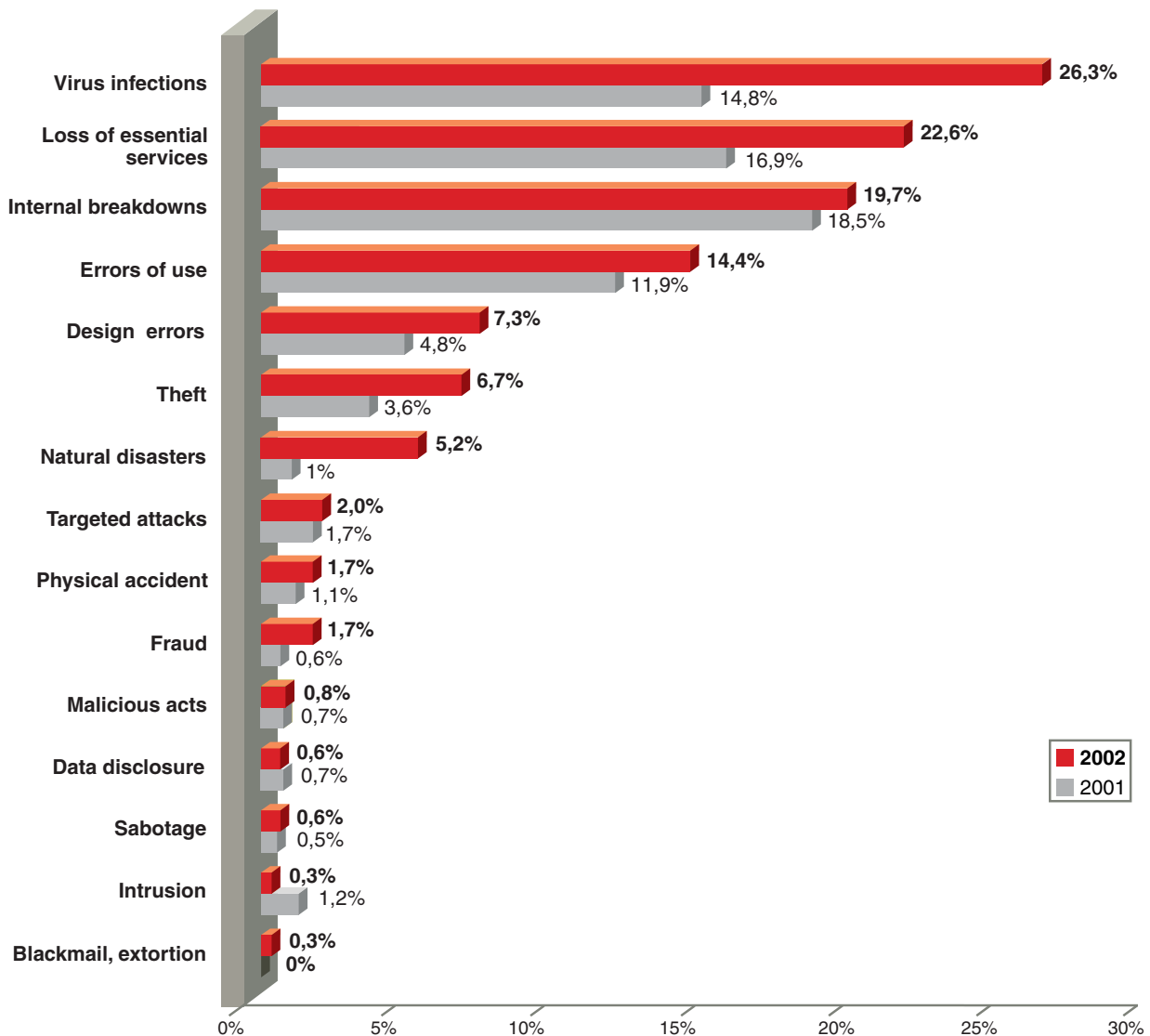
# Evaluation of losses

## An increase in recorded losses

60% of companies state that they have suffered no damage: is this ignorance or lack of transparency? It seems clear that many incidents are not taken into account because they remain undetected.

Among the 40% who declare damage, the rate is less than 10 incidents for 36% of companies. The breakdown of this 36% yields information regarding the populations affected: companies of 200 to 999 employees are affected to 49%. The two extreme bands lie close to the 36% mark. Commerce is affected to 40%, industry, services and transport to 35%, building and civil engineering to 32% and telecoms to 27%.

Certain types of incident show a marked increase in frequency:



This is the analysis by sector of the main items in percentage:

	Sector most affected		Sector least affected	
Virus infections	Services	35%	Telecoms	13.5%
Loss of essential services	Industry	28%	Public works	16%
Internal breakdowns	Telecoms	33%	Public works	12%
Errors of use	Commerce	24%	Public works	6%
Theft	Industry	12%	Transport	0.4%

Theft is significantly more frequent in large companies, at 54%, while it only affects 5% of structures with less than 200 employees.

### Impact of incidents

The general tendency is to underplay the impact of recurrent incidents, of whatever type.

Declared degree of impact:

	Low impact	Average impact	Strong impact
Virus infections	60 %	25 %	15 %
Loss of essential services	68 %	20 %	12 %
Internal breakdowns	58%	32 %	10 %
Errors of use	77 %	18 %	5 %
Design errors	50 %	35 %	15 %
Theft	54 %	24 %	22 %
Natural disasters	52 %	25 %	23 %

Only 14% of companies that have suffered an incident proceed to an assessment of the financial cost, still a rare undertaking. Although the figures obtained are low, it is possible to say that the theft or disappearance of equipment or software does lead to the initiation of such assessments.

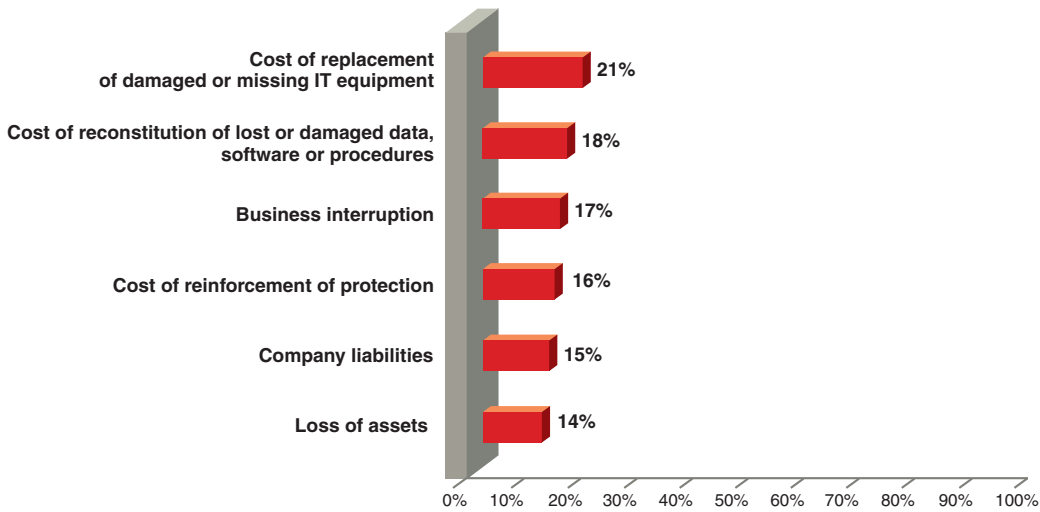
---

*At a time of widespread cuts in budgets, with much emphasis on return on investment, and considering the key strategic challenge that IT security represents for a company, it is extraordinary that such impact calculations are not carried out as a matter of course. Yet it is one of the resources that justify expenditure in the matter of security. For a CISO<sup>4</sup> it is a lever for extracting budgets. We observe that in general companies estimate the impacts of losses as low, but do not proceed to evaluate them, which prompts the question of what tangible criteria their confidence is based on.*

---

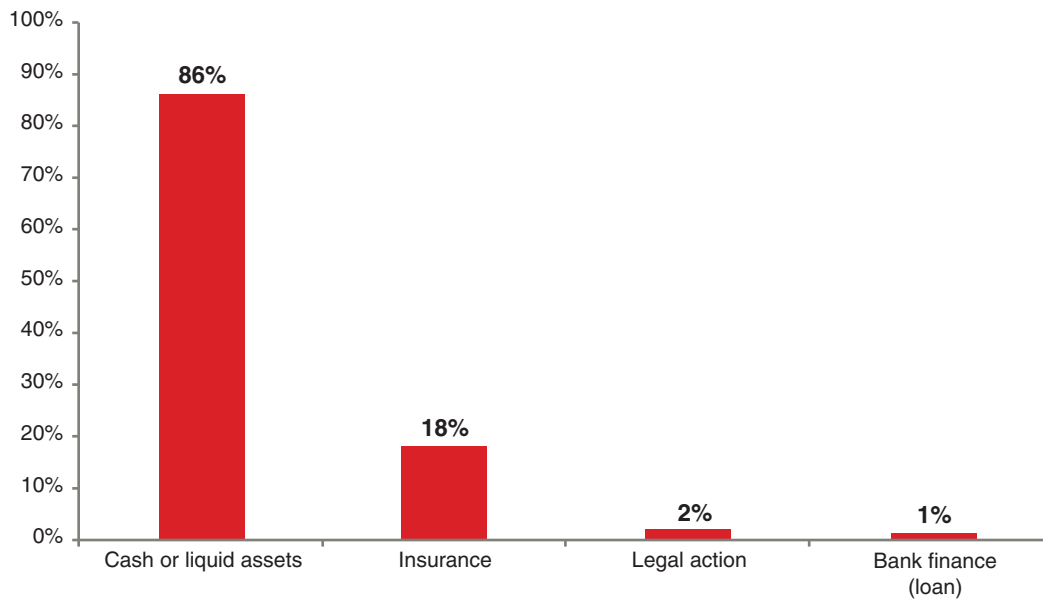
<sup>4</sup> Chief Information Security Officer

The graph below shows the approximate distribution of the financial impact between possible different consequences:



*As regards business interruption, we would remark that we live in a society dependent on digital information, since either material or immaterial damage leads to this type of loss; in the context of insurance, it is advisable to take out appropriate contracts. It should not be forgotten that while this graph shows relatively even distribution between the different types of expense, the cost of equipment is often vastly less than the daily operational loss.*

In 86% of cases, the financial impact of losses is absorbed from cash or liquid assets:



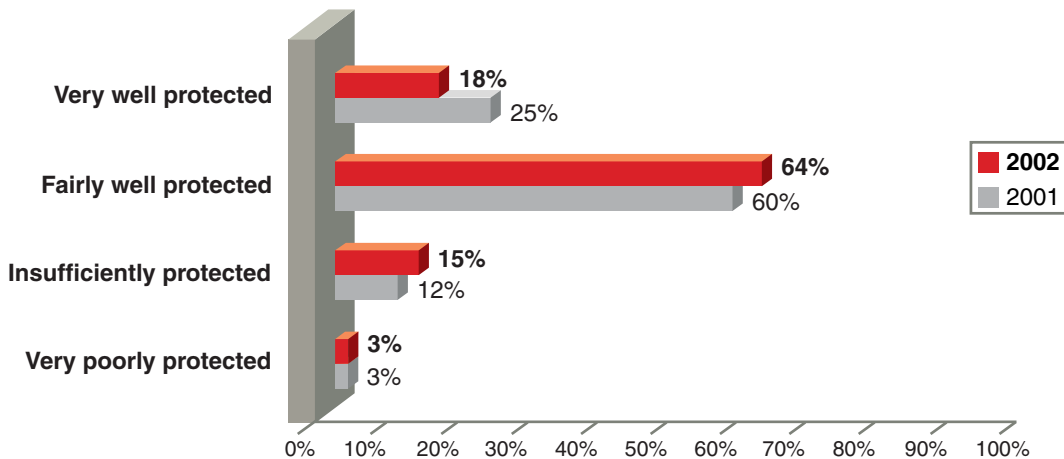
*This high level of recourse to cash or liquid assets may reflect the low cost of impacts, less than the amount of the excess, or by lack of proper insurance.*

## Summary and trends

Most companies, 82% of them, consider that their information system is well or very well protected. Only 3% of companies consider themselves very poorly protected. This figure has remained unchanged for three years.

Developments between 2002 and 2001 reveal divergences.

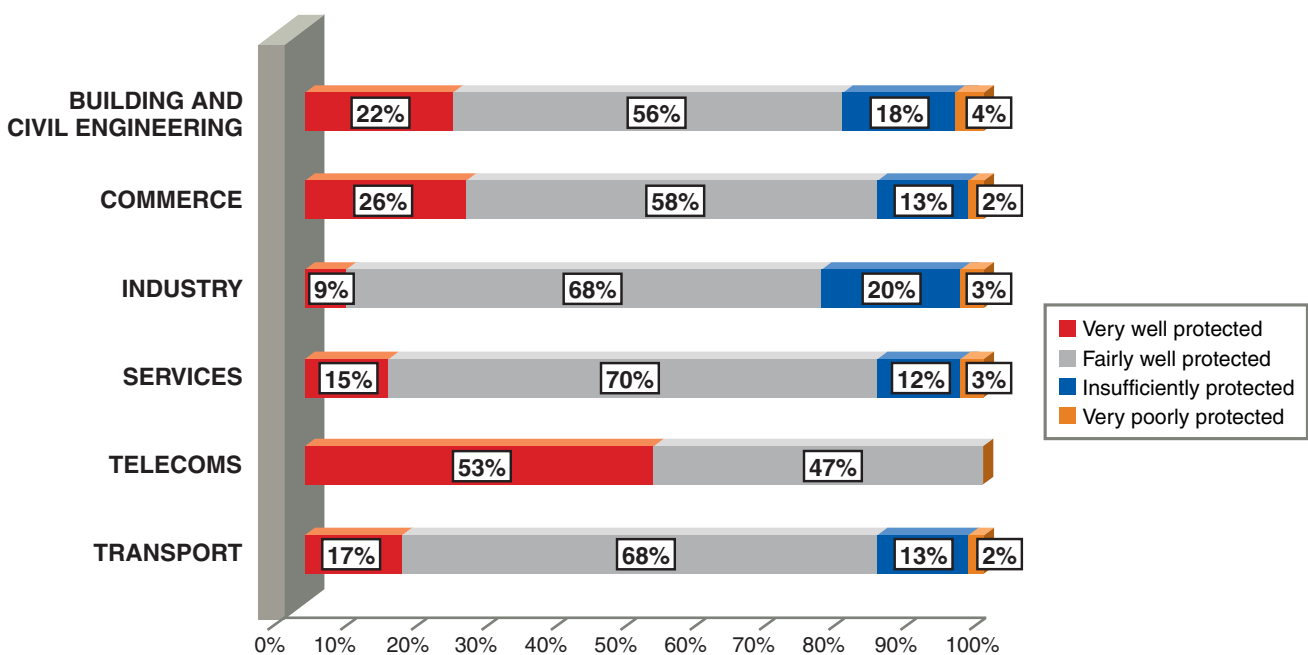
The feeling of confidence of companies with regard to risks:



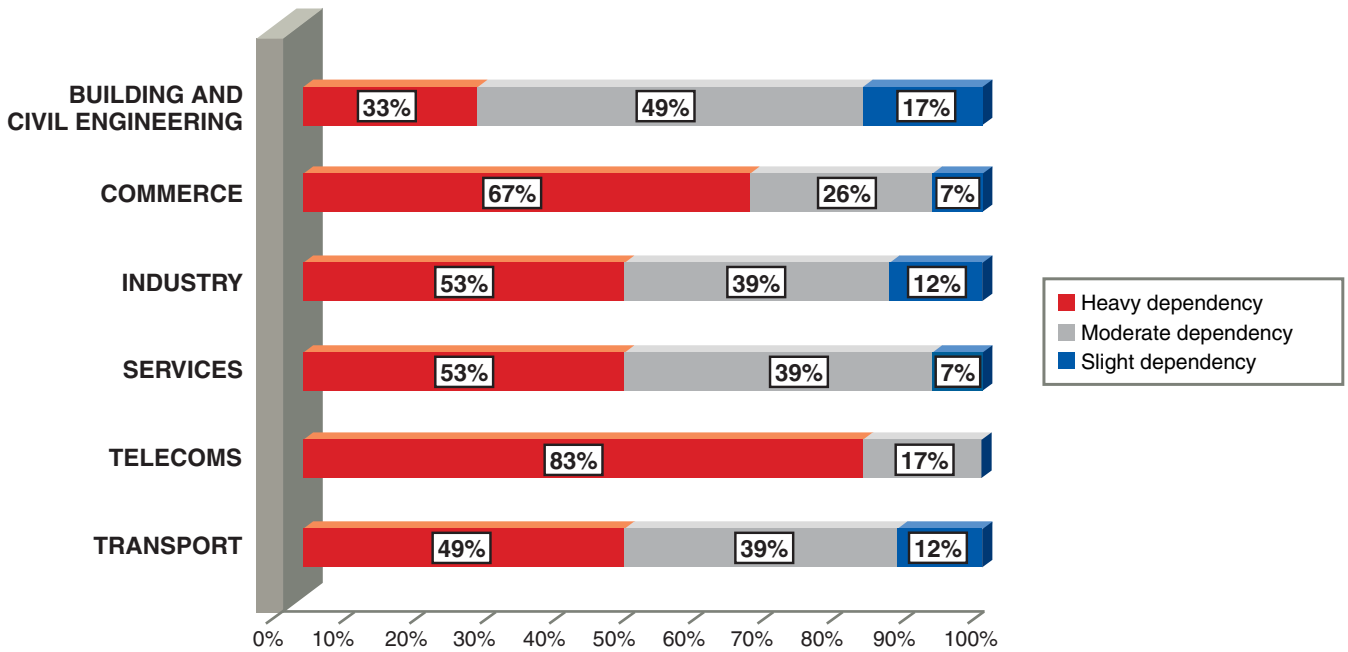
The disparities between company size ranges are very large in comparison to 2001. The fall in the "very well protected" category is highly significant: thus from 500 to 999 employees, the percentage is now 17% compared to 41% the previous year.

Overall, confidence is greatest in the 200 to 499 employee band : 13% "very well protected" and 80% "fairly well protected".

The sectors are distinguished as follows:



It is interesting to compare these data with the feeling of dependency declared by companies.

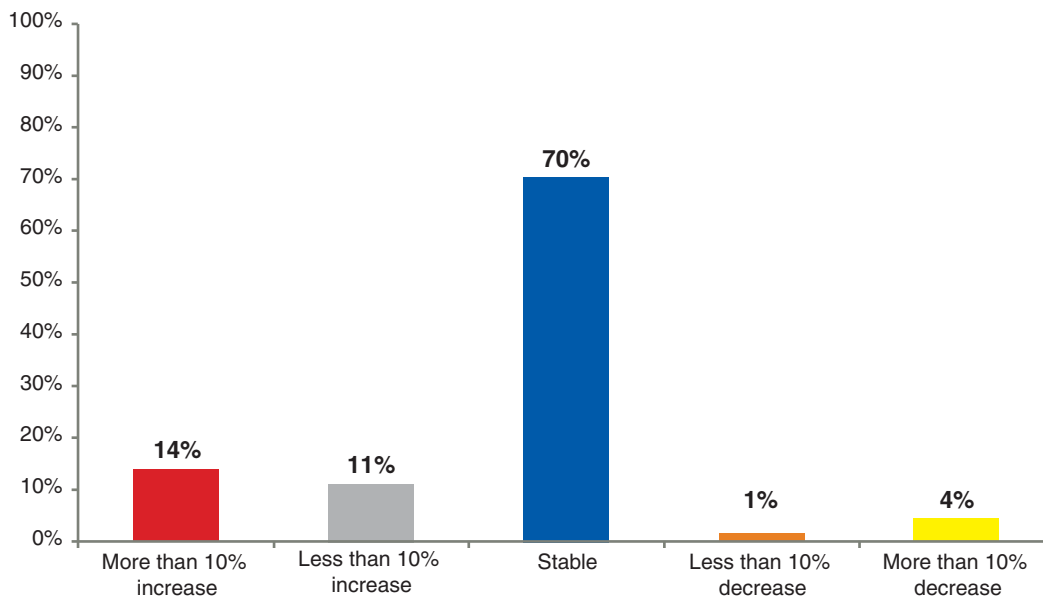


*100% of telecoms companies feel "very well" or "fairly well" protected, despite opening up of systems and a high level of dependency, with 43% use of firewalls.*

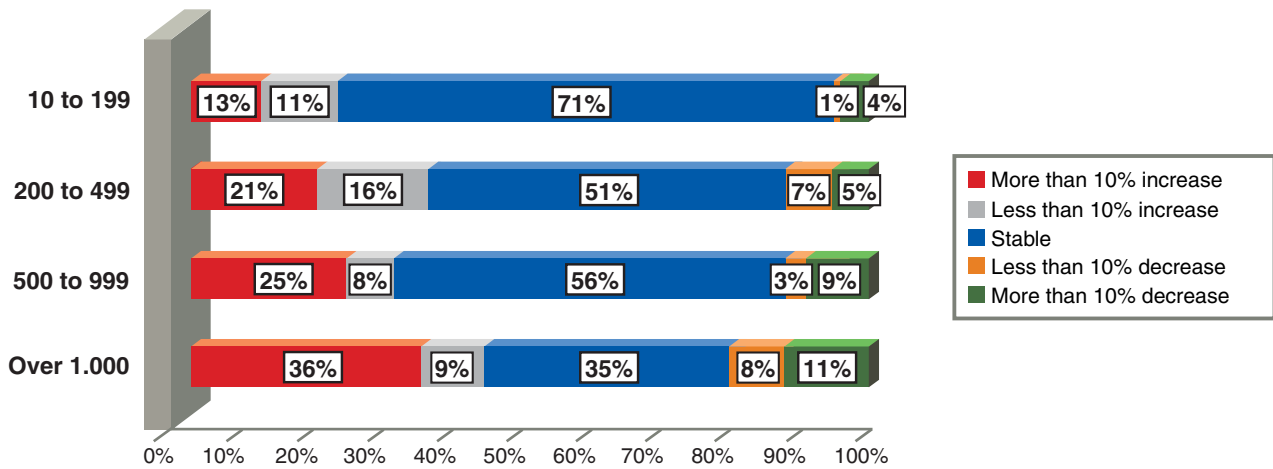
Budgetary and technical prospects over the next two years

It is perhaps this feeling of relative security that induces the stability over two years of the budget allocated to security.

Security budget forecasts:



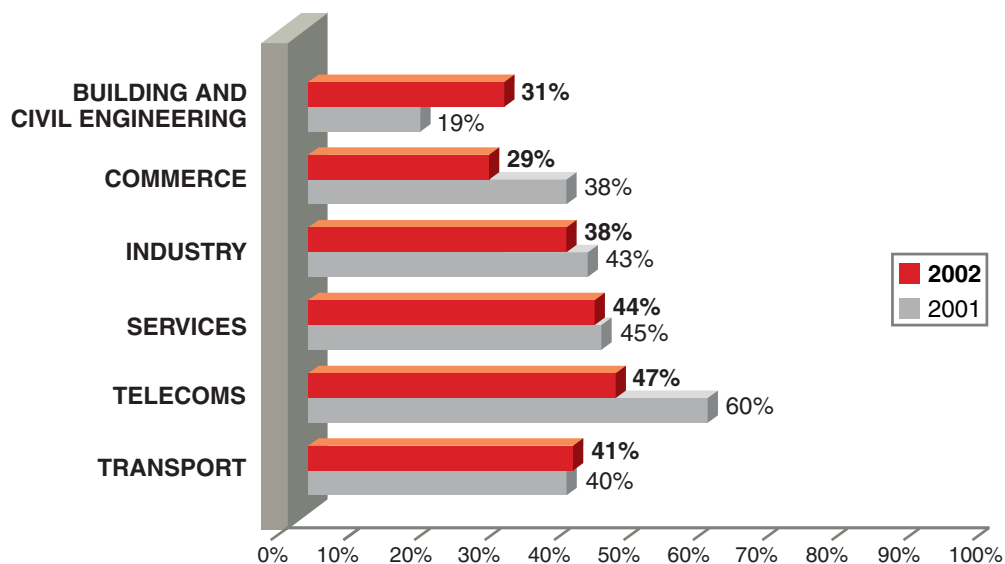
The correlation between the feeling of dependency and the increase of this budget is not significant; company size would seem to be the dominant factor:



While 54% of the telecoms companies, the exception, plan an increase, all the other sectors lie between 20% and 26%.

As regards the reinforcing of security devices, 37% of companies announce this intention. Here again, company size is the decisive factor. There is a widening gap between organizations with less than 200 employees, 36% of which intend an increase, and the other size categories, which are spread out between 62% and 72%.

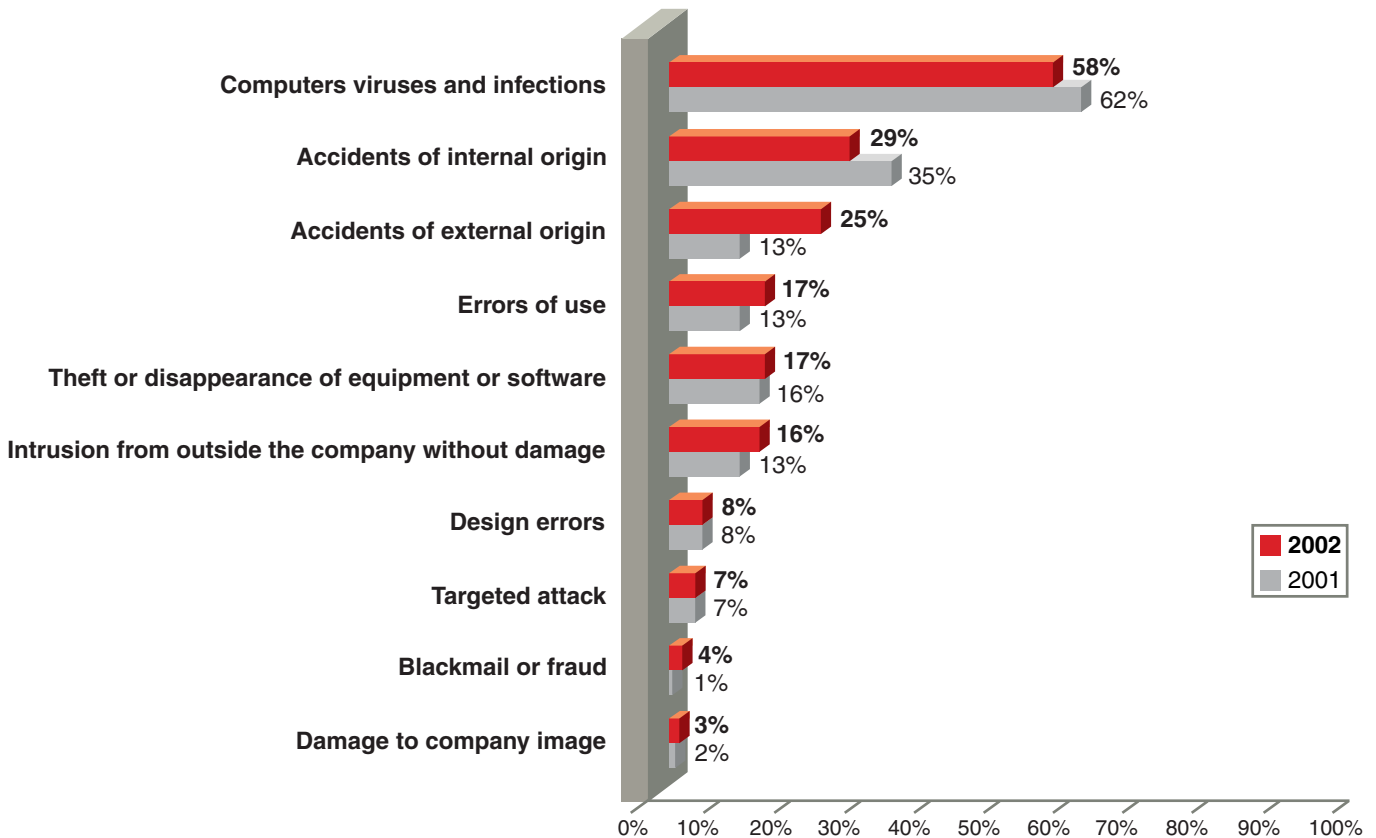
The sector comparison between 2002 and 2001 gives certain indications:



What are the risks for the future ?

The risks apprehended show distinct growth since last year. Accidents of external origin have jumped furthest.

Perceived risks Top Ten:

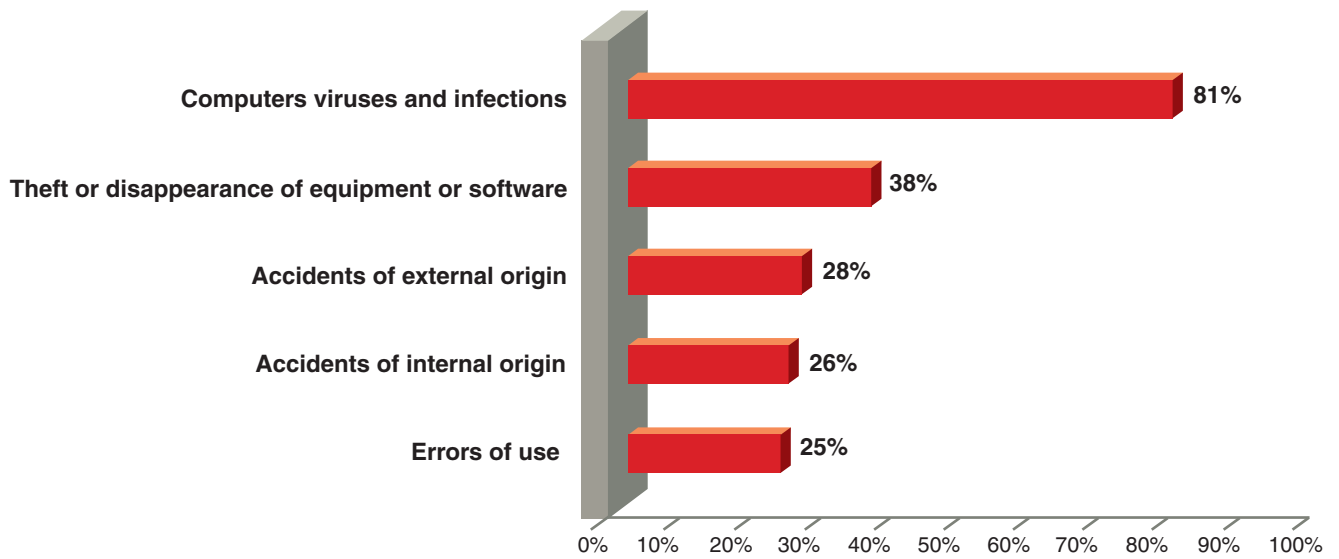


Despite a regression of insignificant magnitude, viruses head the list of this classification for the third year in succession.

*The myth of the virus persists. While it is seen as the most alarming risk, its impact is considered low in the hierarchy of incidents that really occur. How can this predominance be explained? There are several possible reasons: the latest viruses, which hit the headlines as usual; the easily identifiable aspect of the virus and its analogy with health; and lastly, the fact that this misfortune directly affects a large number of users.*

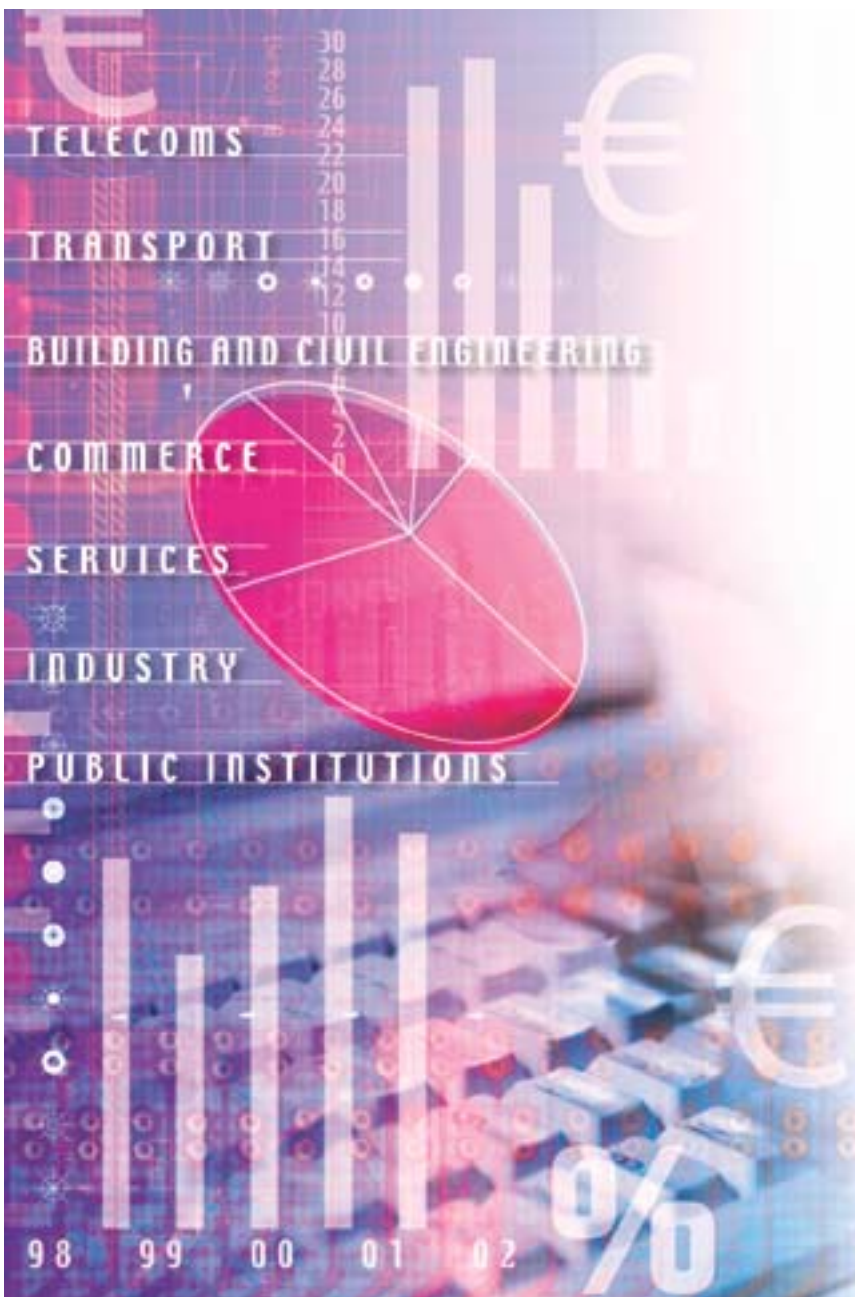
Company size has little influence on the perception of risks in general.

The correlation between incidents that occurred during the year and the potential risks is apparent in the following diagram:



N.B. This graph should be read as follows: 81% of companies which were victims of a virus infection in 2002 fear this type of incident in the future.

# PUBLIC AUTHORITIES



# Environment of information systems

---

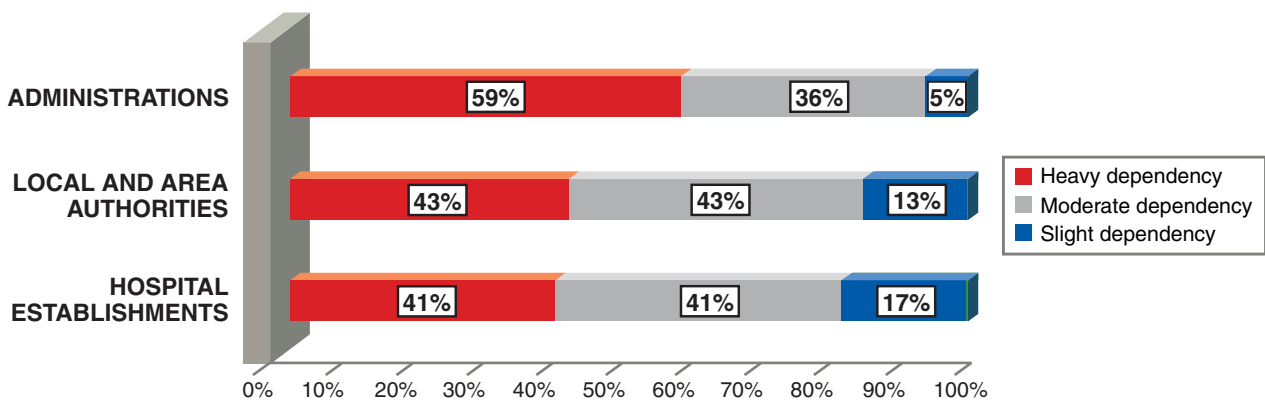
## Note

We remind the reader that major modifications were made to the 2002 sample, in terms of both size and adjustment <sup>5</sup>. In consequence, no comparison is attempted between the data shown in this study and those from last year.

\*\*\*\*

Half (51%) of public authorities consider themselves heavily dependent on their information systems. This dependency is moderate for 39% of them and low for 10%.

Distribution by sector:



Administrations <sup>6</sup> are significantly more aware of their dependency.

---

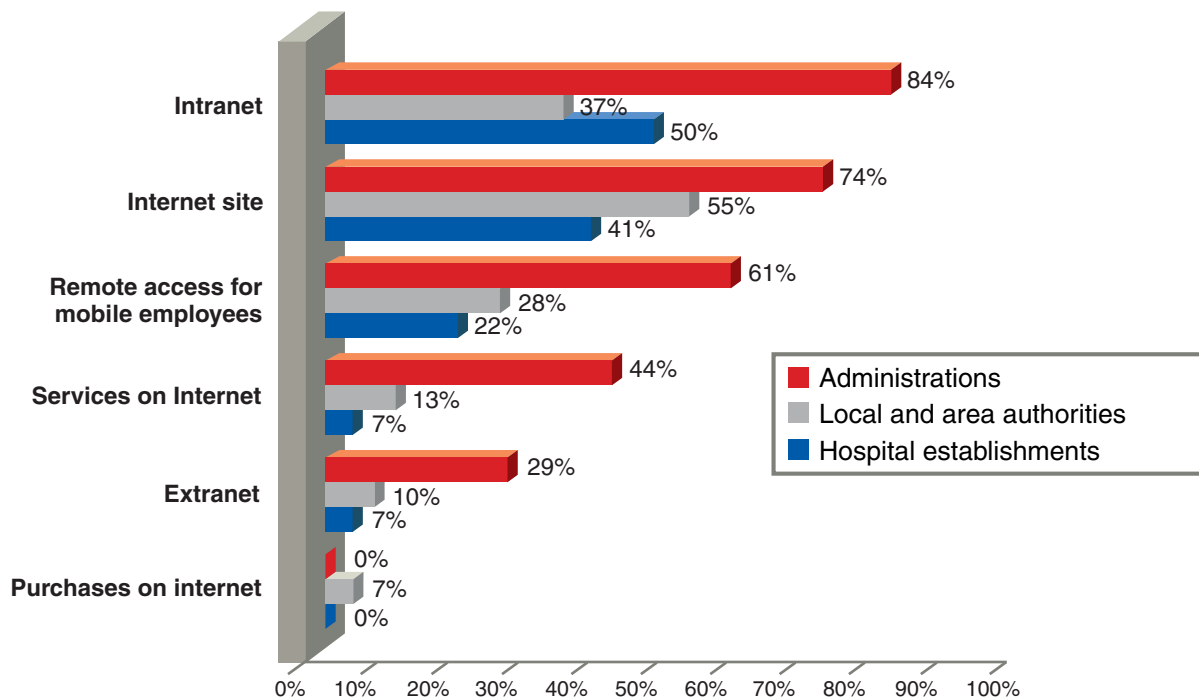
*The differences observed in the feeling of dependency with respect to the information system are explained by the differences of organisation in the three categories. Centralized and decentralized administrations manage national networks, while local authorities and hospital establishments display widely differing situations.*

---

<sup>5</sup> See chapter "Method of investigation".

<sup>6</sup> Administrations include central administrations and decentralized departments.

The opening up of information systems is significant for all the categories:



The importance of remote access for administrations should be noted.

---

*The programmes developed by the administration aiming to promote the internet channel to facilitate relations between the user and the administration (marital status procedures, miscellaneous on-line declarations, etc.) undoubtedly account for a significant proportion of these figures.*

---

# Organisation and resources

---

36% of public authorities state that they have defined a comprehensive security policy. This is true of 41% of administrations, 30% of local authorities and 31% of hospital establishments.

Intelligence is kept by 36% of them: 41% of administrations and hospital establishments and 23% of local authorities do this.

---

*As regards intelligence, the administrations all adopt a similar procedure, which is not the case for local authorities. The latter behave in a manner more closely resembling that of an SME, in which the role of the mayor can be compared to that of the director of a company.*

---

Where public authorities actually have set up a security policy, 38% of them make have recourse to an external service provider.

## External facilities management and services

Over a third of public authorities have signed a contract of facilities management for their information system, either partial, 7%, or in totality, 30%.

Distribution by sectors of recourse to facilities management:



The study shows that the local authorities have a stronger tendency to make use of facilities management.

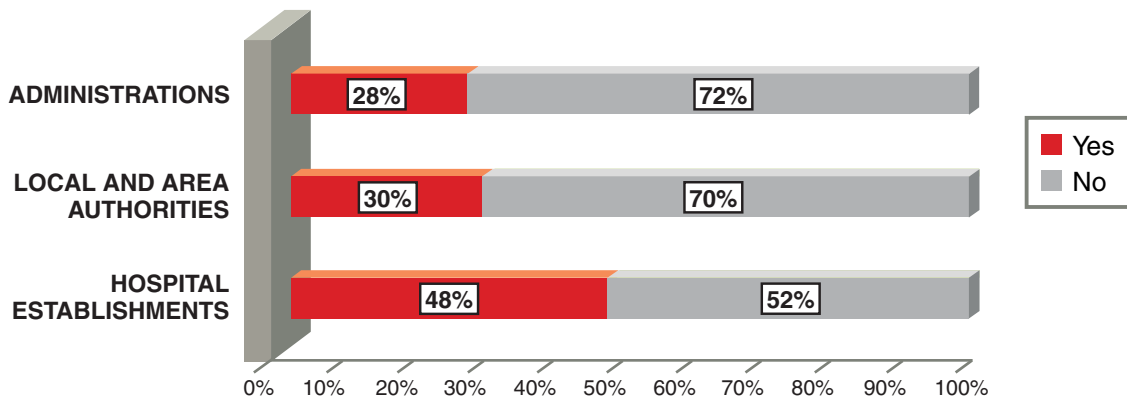
---

*The local authorities differ in their income, especially from local income tax. This number prompts certain questions: in budgetary terms, is it advantageous to externalize information systems ? Is this difference is a consequence of decentralization ?*

---

33% of public authorities call upon specialist external service providers. Hospital establishments stand out for this procedure.

Distribution by sectors of recourse to external service providers:



### Security resources

40% of public authorities have at least one person in charge of the security of information systems:

- administrations: 46%,
- hospital establishments: 41%,
- local authorities: 30%.

On average, this corresponds to one full-time equivalent post.

Of those who have no specific person in charge, 39% have recourse to external service providers.

31% allocate specific budgetary resources to security of information systems.

In the absence of a specific budget, security actions are almost exclusively financed from the IT budget.

---

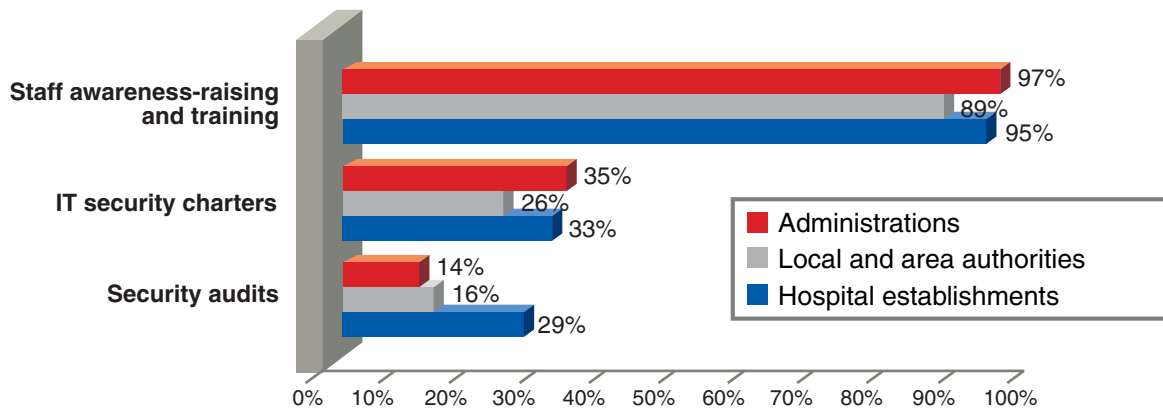
*We would point out that where public authorities are concerned, the IT and telecom budgets are one and the same. There are only two ministries with a dedicated security budget; in general, public authorities do not show this line visibly under a corresponding accounts heading; the budget is simply estimated.*

---

### Management of security

Among the resources used in terms of management, raising employee awareness heads the list. This almost unanimous result shows clearly that the message is getting across in operational terms.

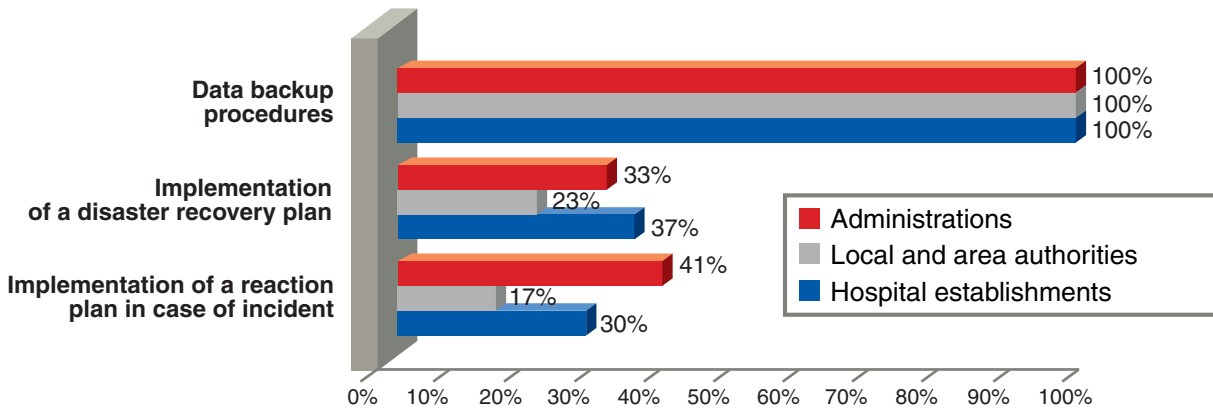
Resources deployed:



*The average figure relating to security charters is explained by the fact that there is a moral contract, with rules to be obeyed, but no internal regulations. The low percentage of audits can be put into perspective; organizational procedures with identical objectives may well be undertaken under another name.*

Continuity of activity

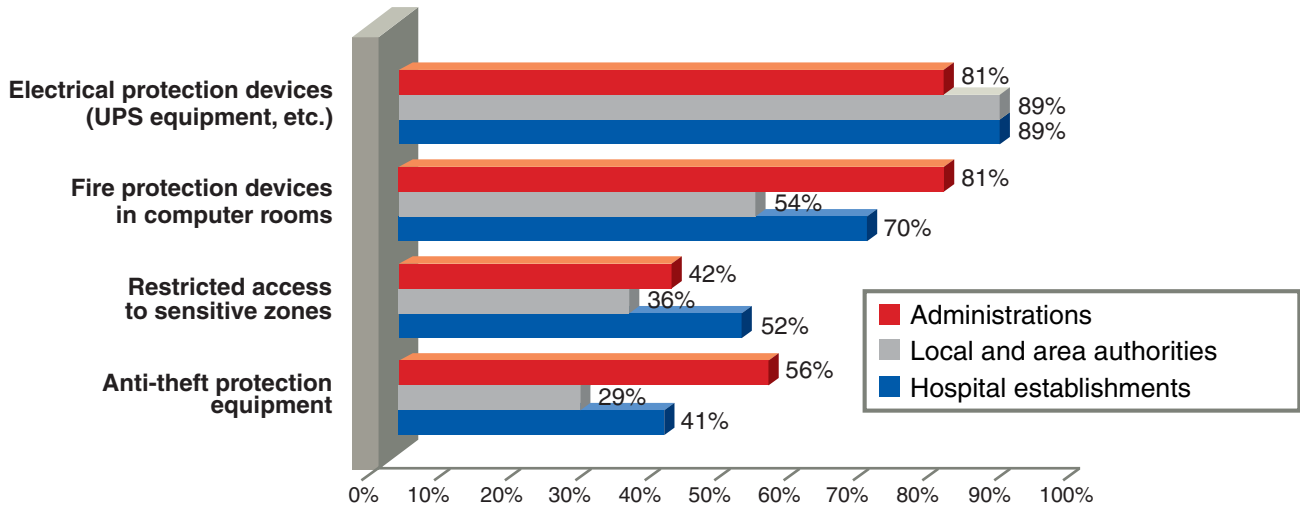
Continuity of activity does not appear to be employed at high level, except as regards data back up procedures.



*For hospital establishments, the absence of differentiation between medical and management IT undoubtedly brings down the figure for setting up reaction plans. Medical IT is subject to specific plans, which is not always true in other cases.*

Physical security

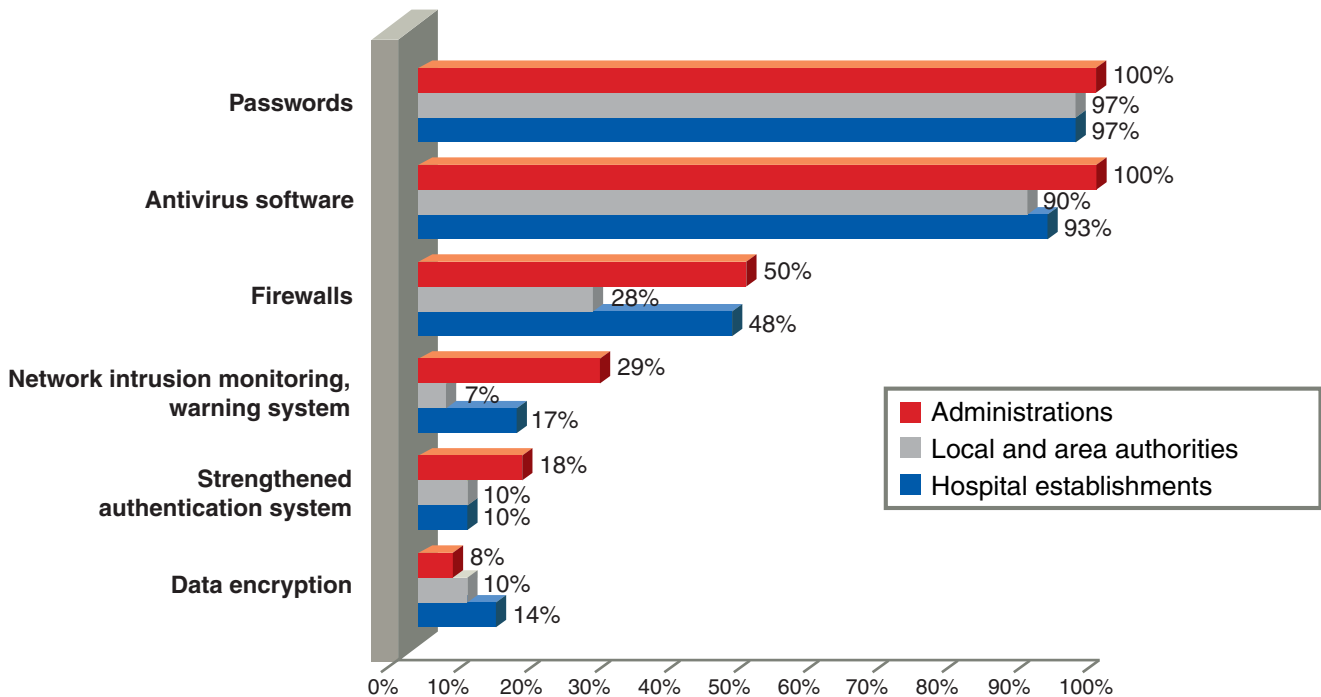
Physical security is well developed in all sectors, with particular emphasis on electrical and fire protection:



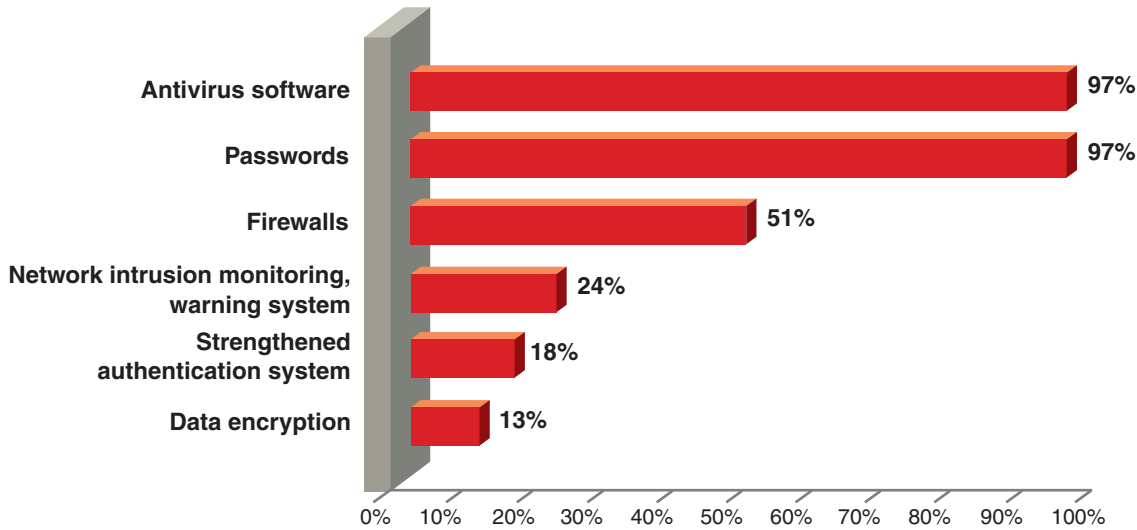
Software security

Passwords and antivirus software are in general use.

Local authorities do not seem to make direct use of firewalls or network surveillance:



If we look at the correlation between the opening of an internet site and the software security resources installed, the results are as follows:

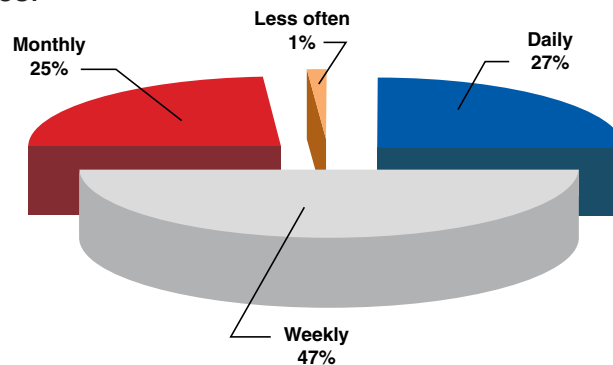


*These results should be put in perspective, as the agents of the administration are not always aware of the resources brought to bear by hosts or service providers. The low rate of intensified authentication is a reflection of the fact that the change-over from the use of passwords or protected access to other means of protection is a long-term process.*

### Antivirus software

91% of public authorities that use it carry out update. These are carried out at least once a week for 74% of them.

Frequency of updates:



*It is necessary to make a distinction between the email gateway antivirus and the workstation antivirus. The recommendation generally applied in administration is the use of two different antivirus software packages.*

The updates are automatic in 77% of cases.

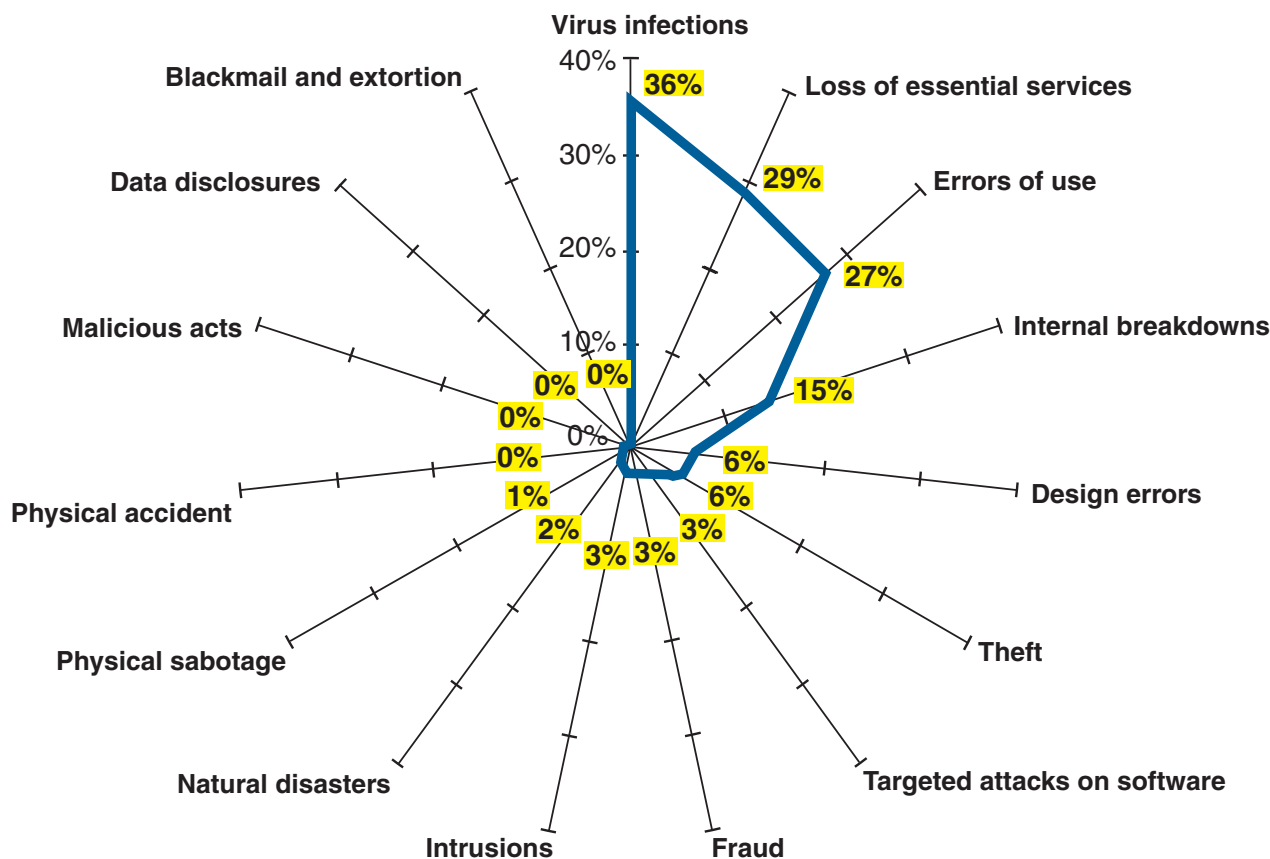
Administrations are the most highly automated, at 94%, compared to 64% for local authorities and 46% for hospital establishments.

# Evaluation of losses

---

Nearly 2/3 of public authorities declare no incident and 27% less than ten. In this case, distribution by sectors is fairly uniform, between 24% and 29%.

The causes of incidents declared are as follows:



---

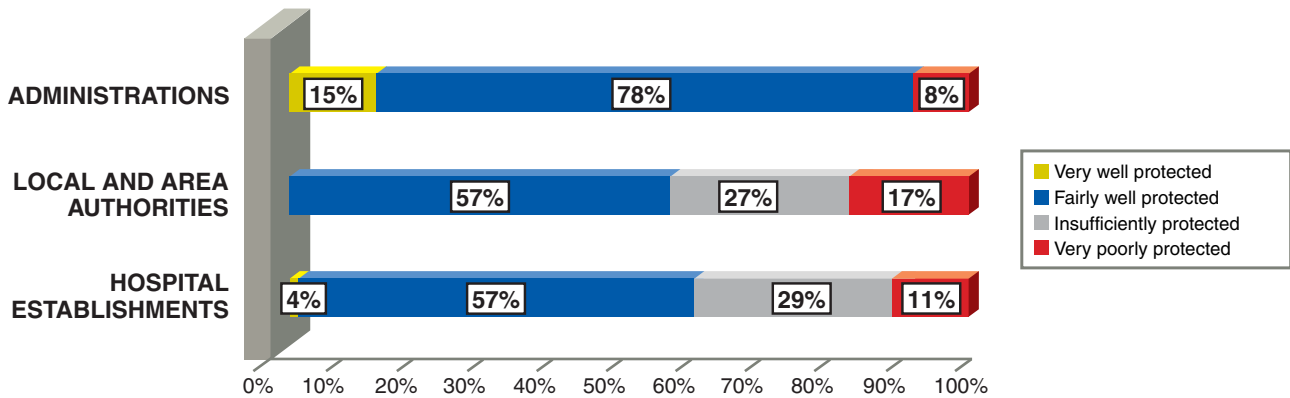
*The percentage of errors of use corresponds to operational reality. On the right-hand side of this graph, damage ranging from virus infection to targeted attacks on software are an accurate representation of the real situation. The other part shows the difficulty of processing incident declarations and of building up a relationship of confidence between the investigator and the persons investigated.*

---

## Summary and trends

The positive feeling of protection of public authorities is 76%, split between 8% "very well protected" and 68% "fairly well protected".

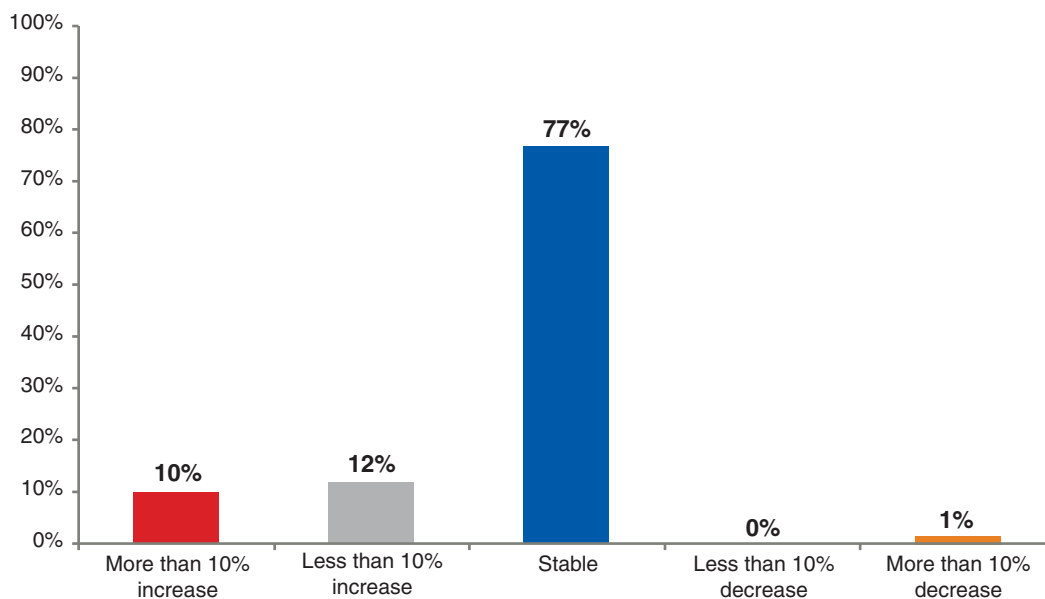
Distribution by sectors:



The hospital establishments, although they have committed considerable resources to protection, have not developed a corresponding level of confidence. The local authorities express a stronger feeling of anxiety.

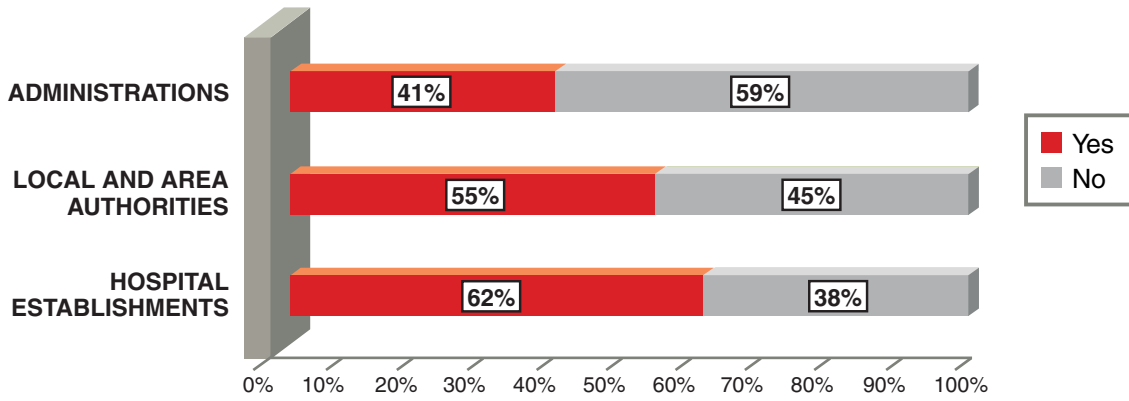
### Financial and technical prospects over the next two years

In the majority of cases, an increase in security resources is not envisaged:



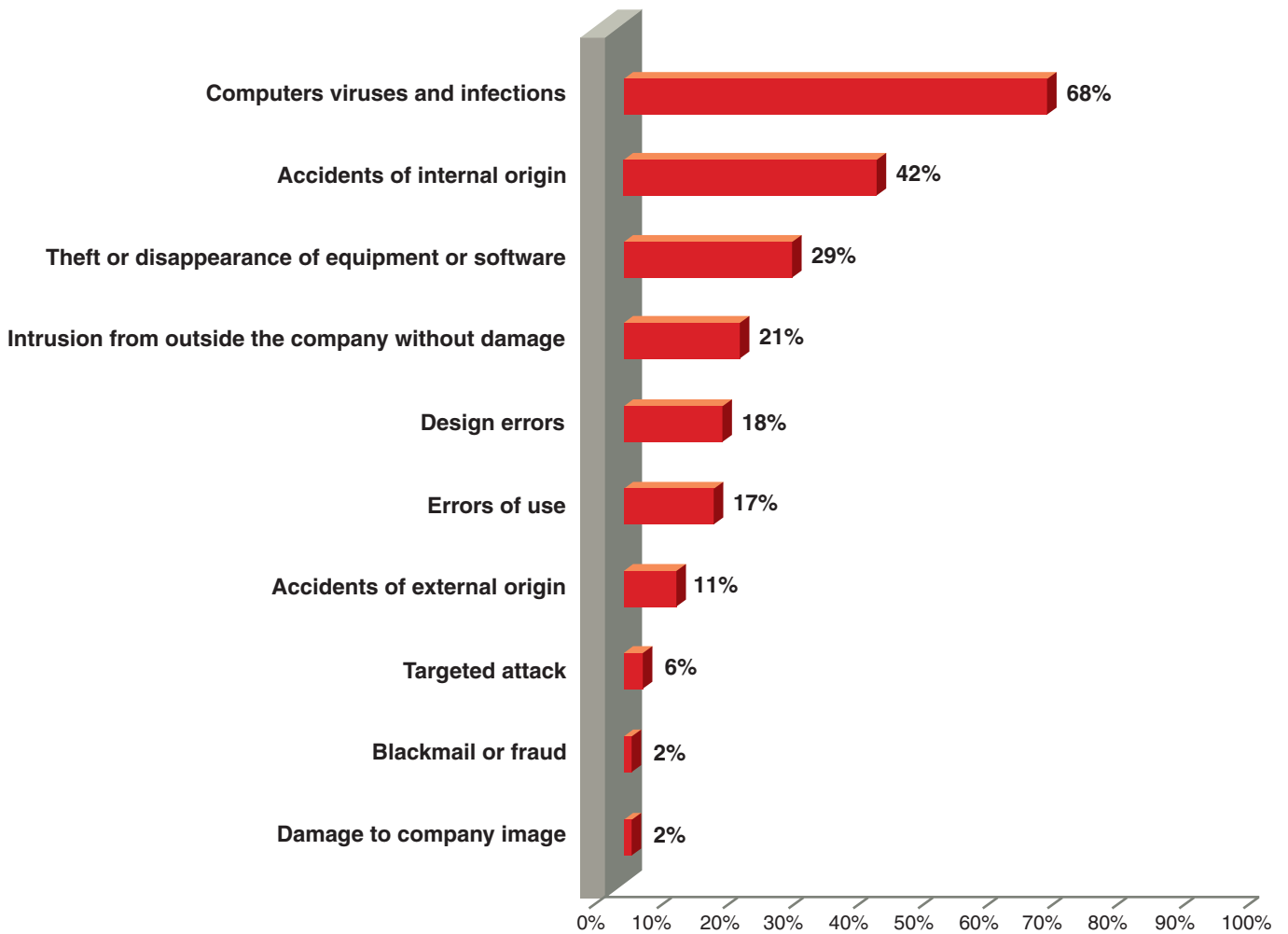
Over the next two years, 22% of public institutions would like to see resources dedicated to security.

The strengthening of risk prevention measures is announced by 49% of organisations:



What are the risks for the future?

Below is the classification of potential risks:



Distribution by sectors sheds further light:

	ADMINISTRATIONS	LOCAL AND AREA AUTHORITIES	HOSPITAL ESTABLISHMENTS
Computers viruses and infections	72 %	64 %	60 %
Accidents of internal origin	36 %	50 %	44 %
Design errors	17 %	18 %	20 %
Intrusion from outside the company without damage	17 %	25 %	28 %
Errors of use	14 %	14 %	28 %
Theft or disappearance of equipment or software	14 %	54 %	28 %
Accidents of external origin	8 %	11 %	20 %
Targeted attack	3 %	7 %	12 %
Damage to company image	0 %	4 %	4 %
Blackmail or fraud	0 %	4 %	4 %

Comparison between the reality of damage suffered and the fear of the risks that threaten reveals strongly contrasting perceptions, theft or intrusion being just one example.

# Glossary

---

**Audit/consulting:**

external services covering the security audit of an IT system only (audit, tests of intrusion, risk analyses, etc.) and security consulting (management, master plan, architecture consulting, continuity consulting, coaching, etc.), but excluding all operational services (incorporation, administration, supervision, etc.).

**Automatic update:**

procedure by which the antivirus software can be updated without human intervention. The server on which the antivirus is installed connects itself automatically, according to the configuration parameters entered, to the site of the software publisher to download the updates.

**Breakdown of internal origin:**

breakdown of the information system which is not the responsibility of a service provider.

**Business interruption:**

loss of margin due to additional costs or loss of income (loss of orders, customers or image).

**Company liability:**

cost to the company of losses caused to others, for example by disclosure of information.

**Computer fraud:**

fraud exploiting the information system. It may consist in misappropriation of equipment or funds, or of telecommunication fraud such as PABX abuse.

**Cost of reconstitution of data, software or procedures lost or damaged:**

this cost is calculated on the basis of the time spent reconstituting the lost elements in the information system.

**Cost of reinforcement of protection:**

Cost of the purchase and/or of putting into service of new security measures following an incident.

**Cost of repair or replacement of IT equipment:**

direct cost of equipment, to which may be added the time spent by company staff on carrying out repairs.

**Design error:**

error in the programming, construction or deployment of software, systems or procedures which engenders malfunctions.

**Disclosure:**

communication of confidential information to a third party.

**Error of use:**

error made by operators or users while using the information system, such as a typing error during input.

**Extranet:**

extension of the Intranet to resources of the Internet network for the purpose of giving customers or suppliers access to certain internal applications and/or information.

**Full time equivalent (FTE):**

unit of measurement of workload obtained by dividing the total workload by the number of persons carrying it out : example :

1 employee on full time = 1 FTE

3 employees on full time, but devoting 20% of their time to the task in question = 0.6 FTE

**Incident:**

a broad term in that a virus affecting 200 microcomputers = an incident; a fire that damages the server room = an incident."

**Intelligence:**

procedure of keeping oneself informed of developments in a given sector legal framework, advances in technologies, etc.. An intelligence procedure includes definition of scope (what the intelligence is covering), direction of the intelligence effort (legal, technological, competitive, etc.), the resources allocated, the analysis and compilation of information collected, the resources for the sharing and distribution of this information.

**Internal/external/unknown origin:**

damage is of internal origin when it is caused by an employee or an ex-employee. Otherwise it is of external origin. If the origin is unidentified, it is considered to be unknown.

**Intranet:**

internal network using internet technologies to communicate information and/or share applications. It is distinguished from a simple network by the web interface that characterizes it.

**Loss of essential services:**

breakdown of external origin affecting services upon which the proper operation of the IT system depends, such as electric power cuts, interruptions of telecommunication services, water supply cuts (affecting air conditioning), etc.

**Malicious act or damage to company image:**

act employing computer technologies and intended to cause injury to the image, for example by defacing web pages.

**NAF code:**

formerly APE code, indicating the principal business of the company.

**Natural disaster:**

incident of natural origin, such as storm, flood, landslide, etc.

**Operational service:**

provision of service to ensure security (remote supervision, hosting of back-up sites, administration of the security infrastructure, delegation of experts, etc.)

**Physical accident:**

incident of unintentional origin that causes damage to the information system, such as fire, explosion, water damage, etc. Damage attributable to natural causes is not included in this category.

**Physical sabotage:**

intentional damage to IT equipment.

**Targeted attack on software:**

virus and other attacks such as manual destruction of data, denial of service, mail bombing, software bomb, Trojan horse, aimed at an organization in isolation with intent to harm it.

**Theft or disappearance of equipment:**

to be understood in the physical sense.

**Virus infection:**

this concerns only effective infection, and excludes any viruses detected and neutralized by the protection system. The infection under consideration is not specifically aimed at an organisation, either of the nature of a company or of a public institution.



**Club de la Sécurité des Systèmes d'Information Français**

30, rue Pierre Sémard - 75009 Paris

Tél.: 33 1 53 25 08 80

Fax.: 33 1 53 25 08 88

Mail : [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr)

Web : <http://www.clusif.asso.fr>