Information Systems Threats and Security Practices
in France

2008 Edition

- COMPANIES WITH OVER 200 EMPLOYEES
- LOCAL AUTHORITIES
- INTERNET USERS

CLUSIF (*Club de la Sécurité de l'Information Français*)

Acknowledgments

CLUSIF would like to express its gratitude to the following participants of this survey:

NAME	COMPANY
Mr. Laurent BELLEFIN	SOLUCOM GROUP
Mr. Thierry CHIOFALO	SDV
Mr. Paul CONSTANT	CONSULTANT
Ms. Perrine DILIGENT	BYWARD LIMITED
Mr. Marc-Noël FAUVEL	TOWN HALL OF RUEIL MALMAISON
Mr. Eric FREYSSINET	NATIONAL GENDARMERIE
Mr. Pierre GOJAT	ORANGE BUSINESS SERVICES
Mr. Paul GRASSART	AGERIS CONSULTING
Mr. Olivier GUERIN	CLUSIF
Mr. Bruno HAMON	GROUPE LEXSI
Mr. Jean-Philippe JOUAS	CLUSIF
Mr. Pascal LOINTIER	AIG EUROPE
Mr. Lionel MOURER	BULL
Mr. François PAGET	MCAFEE
Mr. Patrice RENAUDINEAU	NANTES METROPOLIS
Mr. Philippe ROSE	BEST PRACTICES INFORMATION SYSTEMS
Mr. Jean-Louis ROULE	CLUSIF

CLUSIF would also like to thank the representatives of the companies and local authorities as well as the Internet users who took part in this study.

The statistical survey was conducted on behalf of CLUSIF by GMV Conseil and Harris Interactive.

Editorial

For the 2008 edition of its investigation on information systems threats and security practices, CLUSIF has once more conducted an in-depth evaluation of information security in France. This study is intended to serve as a reference on the grounds of its representative sample sizes comprising companies and local authorities. It should also be considered to be comprehensive insofar as it reviews a vast range of issues dealing with information systems security.

This year, the scope has been broadened and now includes an entire section on the practices of individual Internet users at home. Today, the use of computers and Internet in the home has become commonplace and the behavior of users in companies is increasingly influenced by their private practices. Our study has proven that the boundaries between the two contexts are becoming blurrier. According to our results, a third of Internet users also use the family computer for professional purposes, which raises several questions concerning the protection of company data. And while Internet users are generally cautious when making online purchases and seem to be aware of the utility of protection tools (antivirus, personal firewalls, etc.), only a minority of them feel genuinely "unsafe" on the Internet.

As for companies, this 2008 edition highlights a troubling feeling of stagnation. Remarkable progress had been made between 2004 and 2006, particularly in the formalization of policies and security dashboards. Yet since then, it seems that these policies are still waiting to be concretely applied. Currently, 40% of companies still lack a business continuity plan to handle major crises, compared to 42% in 2006. Furthermore, 30% of them state that they are still not in compliance with the Data Processing, Data Files and Individual Liberties Act….

Regardless, threats are ever present and our study has once again revealed that malicious acts and security incidents are very real, with frequent occurrences of viral attacks, equipment theft and a growing number of data disclosure problems and targeted logical attacks. Recent events continue to demonstrate the serious consequences of security flaws (bank fraud, personal data disclosure, etc.).

Abandoning "empty" security policies drafted merely for show and instead adopting concrete practices firmly anchored in data management processes – that is the true challenge for the years to come…

Laurent BELLEFIN
For the "Study on Information Systems Threats and Security Practices" Working Group

Table of Contents

COMPANIES **12**
Presentation of the sample 12
Dependence on IT in companies with over 200 employees 13
Resources invested in information security 13
Clause 5: Security Policy 16
Clause 6: Organization of Information Security and Means 18
Clause 7: Risk Assessment and Treatment 20
Clause 8: Human Resources and Security 22
Clause 10: Communications and Operations Management 24
Clause 11: Access Control 28
Clause 12: Acquisition, Development and Maintenance 30
Clause 13: Incident Management - Disasters 31
Clause 14: Business Continuity Management 34
Clause 15: Compliance 36

LOCAL AUTHORITIES **40**
Presentation of the sample 40
Dependence on IT in local authorities 41
Resources invested in information security 41
Clause 5: Security Policy 44
Clause 6: Organization of Information Security 46
Clause 7: Risk Assessment and Treatment 48
Clause 8: Human Resources and Security 50
Clause 10: Communications and Operations Management 51
Clause 11: Access Control 53
Clause 12: Acquisition, Development and Maintenance 56
Clause 13: Incident Management - Disasters 56
Clause 14: Business Continuity Management 61
Clause 15: Compliance 64

INTERNET USERS **68**
Part 1: Profile of Internet Users 68
Part 2: Internet Uses 71
Part 3: Perception of Threats and Risks 74
Part 4: Security Means and Behavior 79
Conclusion 80

APPENDIX **82**

Diagrams and Charts

Figure 1: Dependence on IT in companies 13
Figure 2: Portion of the IT budget earmarked for security in companies 14
Figure 3: Evolution of the security budget according to industry 14
Figure 4: Existence of a security policy by company size 16
Figure 5: Reliance on a security standard for the ISP 17
Figure 6: Hierarchical association of the CISO in companies 18
Figure 7: Distribution of the CISO's responsibilities 19
Figure 8: Risk analysis conducted in companies 20
Figure 9: ISS improvement process 20
Figure 10: Consideration of risks in projects 20
Figure 11: Participants in risk analysis 21
Figure 12: Existence of security charters, a function of size 22
Figure 13: Security awareness tools 23
Figure 14: Mobility and IS access control in companies 24
Figure 15: Technologies for securing IS access in controlled mobile equipment 25
Figure 16: Security technologies/antivirus, anti-intrusion combat, management of vulnerabilities 26
Figure 17: Logical access control technologies deployed in companies 28
Figure 18: Surveillance of vulnerabilities in companies 30
Figure 19: Time frame for patch deployment in companies 30
Figure 20: Units for collecting and treating malicious incidents 31
Figure 21: Complaints filed by companies 32
Figure 22: Number of security incidents inventoried in 2007 by companies 32
Figure 23: Types of security incidents in companies 33
Figure 24: Existence of a formalized process for IS continuity management 34
Figure 25: Testing frequency of business continuity plans 35
Figure 26: Disaster recovery solutions 35
Figure 27: Data Protection Officers in companies by branch of industry 36
Figure 28: Number of security audits conducted a year in companies 37
Figure 29: Reasons for security audits 37
Figure 30: Implementation of dashboards in companies 38
Figure 31: Recipients of the dashboard 38
Figure 32: Indicators monitored in the dashboard 38
Figure 33: Adjusted sample of local authorities surveyed 40
Figure 34: Dependence on IT in local authorities 41
Figure 35: Average IT budget by category of local authority 41
Figure 36: Portion of IT budget earmarked for security in local authorities 42
Figure 37: Evolution of the IT budget by category of local authority 42
Figure 38: Obstacles to security tasks 43
Figure 39: Existence of a security policy by category of local authority 44
Figure 40: Reliance on a security standard for the ISP 45
Figure 41: Identification of the CISO duty 46
Figure 42: Hierarchical association of the CISO in local authorities 46
Figure 43: Distribution of the CISO's responsibilities 47
Figure 44: Risk analysis conducted in local authorities 48
Figure 45: ISS improvement process in local authorities 48
Figure 46: Consideration of risks in projects 48
Figure 47: Existence of security charters in local authorities 50

Figure 48: Mobility and IS access control in local authorities 51
Figure 49: Technologies for securing mobile IS access on controlled equipment 52
Figure 50: Security technologies used in local authorities 52
Figure 51: Logical access control technologies deployed in local authorities 53
Figure 52: Logical access control technologies deployed in town halls, 2008 and 2006 54
Figure 53: Constant surveillance of vulnerabilities in local authorities 56
Figure 54: Time frame for patch deployment in local authorities 56
Figure 55: Types of security incidents in local authorities 58
Figure 56: Rate of viral infections in local authorities 58
Figure 57: Source of viral infections in local authorities 59
Figure 58: Impact of viral infections on local authorities 59
Figure 59: Number of security incidents inventoried in 2007 by local authorities 60
Figure 60: Existence of a formalized process for IS continuity management 61
Figure 61: BCP in town halls with over 30,000 inhabitants, 2008 and 2006 61
Figure 62: Testing frequency of business continuity plans 62
Figure 63: Disaster recovery solutions 63
Figure 64: Number of security audits conducted a year in local authorities 64
Figure 65: Types of security audits 65
Figure 66: Reasons for security audits 65
Figure 67: Example of sample adjustment 68
Figure 68: Number of computers per household 69
Figure 69: Types of use of the family computer 70
Figure 70: Internet connection time 71
Figure 71: Market share of ISPs 71
Figure 72: Downloading habits for music and movies 73
Figure 73: Security incidents encountered by Internet users in the past 18 months 74
Figure 74: Threats by order of importance for Internet users 76
Figure 75: Differences in risk perception by gender 77
Figure 76: Practices and situations considered risky by Internet users 78
Figure 77: Protection methods employed by Internet users 79

Methodology

The CLUSIF study on information systems threats and security practices in France in 2008 was conducted from January through March 2008 in collaboration with the specialized firm GMV Conseil, using survey questionnaires developed by CLUSIF. Three target populations were selected for this study:

- companies with over 200 employees: 354 companies in this category agreed to respond to the questionnaire;
- local authorities: 194 participants responded from town halls in cities with over 30,000 inhabitants, intermunicipal administrative structures such as communities of communes ("*communautés des communes*") and metropolitan communities ("*communautés d'agglomérations*"), as well as regional and departmental councils;
- private individual Internet users: 1139 individuals from a panel of Internet users from the specialized institute Harris Interactive completed this study online.

The questionnaire used for the first two target groups was developed on the basis of clauses from the ISO 27002 standard which establishes a general code of practice for information systems management. The objective was to thoroughly measure the current level of best practices implemented by these groups. The clauses, numbered from 5 to 15, are as follows:

- Clause 5: Security Policy;
- Clause 6: Organization of Information Security;
- Clause 7: Risk Assessment and Treatment;
- Clause 8: Human Resources and Security (charter, awareness);
- Clause 10: Communications and Operations Management;
- Clause 11: Access Control;
- Clause 12: Acquisition, Development and Maintenance;
- Clause 13: Security Incident Management;
- Clause 14: Business Continuity;
- Clause 15: Compliance (Data Protection Act, audits, dashboards).

Only Clause 9 which concerns physical security was excluded.

Private individual Internet users were questioned on the following topics:

- socioprofessionnal status and computer equipment;
- computers and Internet use at home;
- perception of Internet threats, awareness of security risks, incidents encountered;
- security practices (behavior and technical solutions).

The responses were compiled in complete anonymity by GMV Conseil, then analyzed by a group of CLUSIF experts specialized in information security.

Companies

- Presentation of the sample
- Dependence on IT in companies with over 200 employees
- Resources invested in information security
- Clause 5: Security Policy
- Clause 6: Organization of Information Security
- Clause 7: Risk Assessment and Treatment
- Clause 8: Human Resources and Security
- Clause 10: Communications and Operations Management
- Clause 11: Access Control
- Clause 12: Acquisition, Development and Maintenance
- Clause 13: Incident Management-Disasters
- Clause 14: Business Continuity Management
- Clause 15: Compliance

Companies

Presentation of the sample

For the 2008 edition of this study, CLUSIF intended to observe the same sample of companies as in 2006 in order to compare any progress or decline. The target group thus comprises companies with over 200 employees in the following industries:

- construction and public works (BTP);
- trade;
- manufacture;
- services, banks, insurance;
- transportation;
- telecommunications.

CLUSIF received a positive response from 354 companies, with a lower acceptance rate than in 2006 (approximately 6%). This means that only six out of every one hundred companies contacted agreed to respond to our questions, which implied calling nearly 6,000 companies! While 307 companies responded by telephone (with average interview time of 32 minutes), the others preferred to complete the survey directly over the Internet on a dedicated and secured Website.

To ensure that the sample would be representative of the total population of enterprises within a given industry, two criteria were used to derive the sample weights: total workforce in the company and the company's industry. This sample was adjusted according to these criteria to attain consistency with the reality of French companies, in accordance with data provided by INSEE (National Institute for Statistics and Economic Studies).

	200-499 employees	500-999 employees	Over 1000 employees	Total	Total in %		INSEE Data
CONSTRUCTION AND PUBLIC WORKS	2		3	5	1%	→	**6%**
TRADE	27	4	12	43	12%	→	**17%**
MANUFACTURE	96	32	35	163	46%	→	**43%**
SERVICES	51	16	48	115	32%	→	**25%**
TRANSPORTATION— TELECOMS	9	9	8	26	7%	→	**9%**
Total	185	61	106	352[1]	100%		
Total in %	52%	17%	30%				

Adjustment →

INSEE Data	**66%**	**19%**	**15%**

Adjustment →

In each company, our first priority was to question the **Chief Information Security Officer**, or CISO (21% in total responded with 43% in companies with over 1,000 employees). If this was not possible, which was often the case for the smallest companies in our sample, we questioned the IT manager (50%). Of all the participants surveyed, regardless of size or industry, 66% were CIOs[2], IT Managers or CISOs.

[1] Attentive readers will notice that we originally stated 354 participants and this figure is indeed accurate. This chart, which only mentions 352, is an intermediary compilation but does not affect the ratios.

[2] See glossary.

Dependence on IT in companies with over 200 employees

IT systems are strategic for all companies

The survey confirmed again this year that IT systems are perceived as strategic tools by a large majority of companies. Regardless of size or industry, 73% of these companies considered that unavailability of their information tools for even less than 24 hours would result in serious consequences (maximum of 83% for the trade industry).

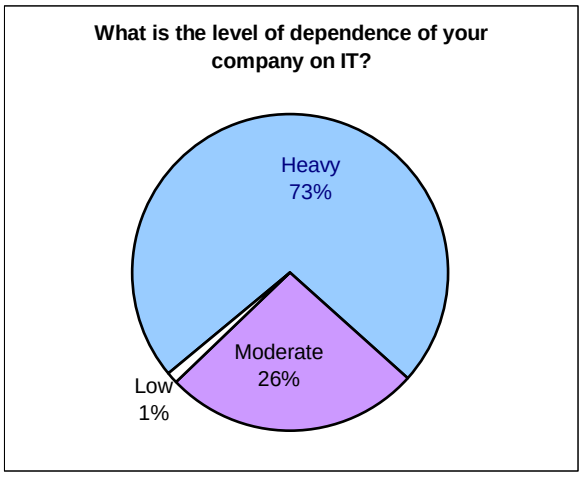

Figure 1: Dependence on IT in companies

Resources invested in information security

Average IT budget of €1.9 million

When asked about their IT budget, only 25% of companies responded. Their responses revealed that one-third of companies have a budget of between 1 and 2 million euros and 10% of budgets are higher than 5 million euros with a maximum budget of 100 millions euros.

A security budget that continues to be poorly targeted

Rather than questioning CISOs on their budget in absolute value (which is insignificant unless it is precisely correlated with each participant's size and business activity), we asked them about the portion of the IT budget allotted for information security.

There was little difference between the results of previous years and those of today. The sole exception perhaps is that security managers still have some difficulty in providing a figure, as 30% of them admitted to not knowing the weight of their budget within the overall IT budget. Reference guidelines to identify ISS costs would make it possible to establish clearer outlines. In cases where this budget is clearly set out in relation to the IT budget, a major discrepancy becomes obvious.

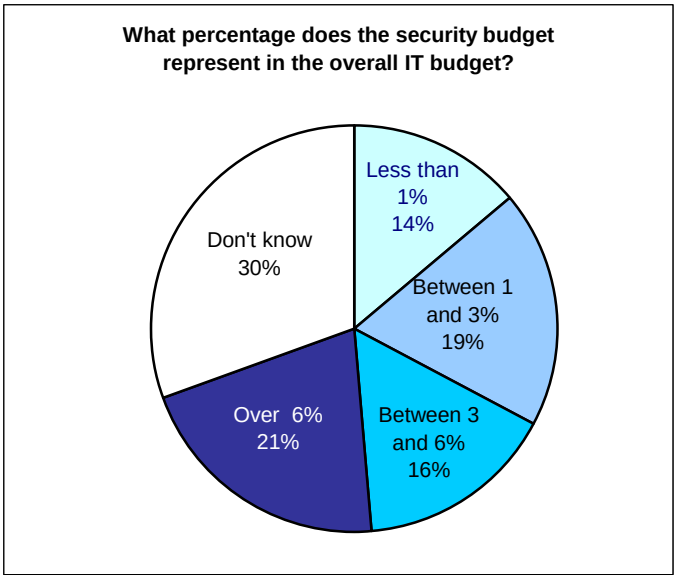

Figure 2: Portion of the IT budget earmarked for security in companies

A troubling stagnation in security budgets

It is interesting to note that budgets have not substantially changed since 2006 in the majority of companies. Fortunately, this impression of stagnation is relative: half of the companies in the services, banking and insurance industry increased their budget this year, and at times by a very large margin (28% of these companies reported a budget hike of over 10%).

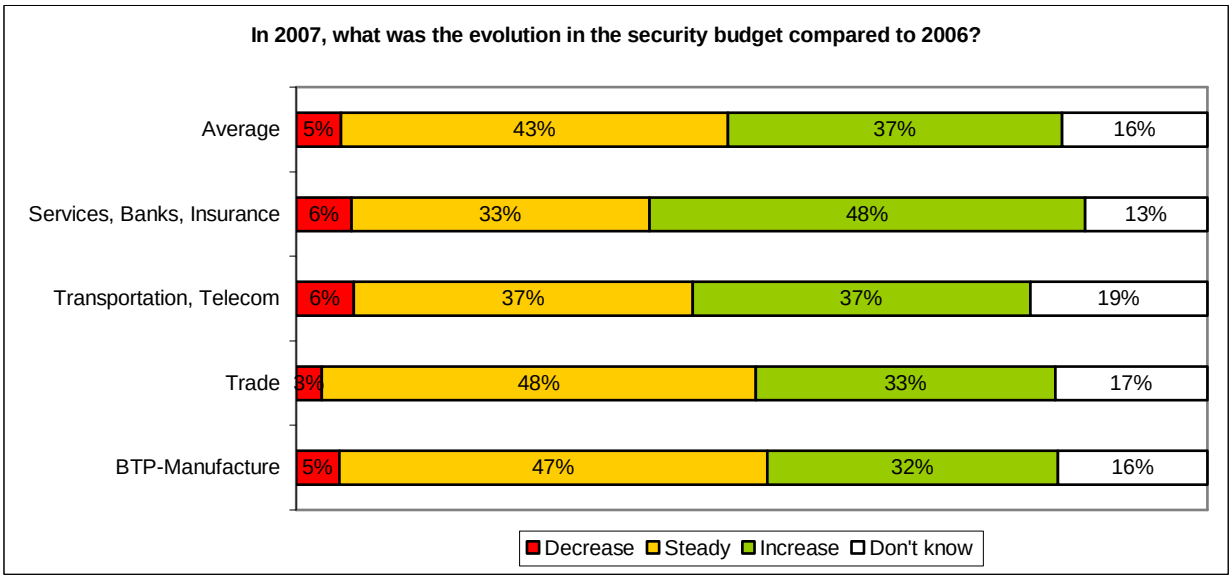

Figure 3: Evolution of the security budget according to industry

Organizational restrictions and budget: obstacles for CISOs

Lastly, when asked about obstacles preventing them from accomplishing their tasks, CISOs cited, by order of decreasing importance:

- organizational restrictions (36%);
- lack of budget (35%);
- reluctance of the hierarchy, services or users (27%);
- lack of qualified personnel (23%);
- reluctance of the Information Systems Department (8%).

The two primary obstacles were organizational restrictions (which emerge as a greater obstacle than two years ago) and the lack of budgetary means, which still continues to be as alarming.

The good news however, is that information systems users do not seem to be systematically perceived as a hindrance by CISOs. We hope that the user would even be considered an ally in accomplishing their objectives. Likewise, the CIO also appears to be a solid asset for the CISO.

The lack of qualified personnel was the second-leading obstacle in 2006 but fell to fourth position this year. An analysis of the responses nevertheless revealed a more negative outcome than what the figures would lead us to think, since one out of two CISOs (53%) blamed this lack of personnel as a major barrier (cited first or second). Moreover, frenetic activity on the ISS job market and the rise in the number of offers testify to this ongoing dissatisfaction.

Clause 5: Security Policy

Stagnation in the formalization of information security policies…

Implementing an Information Security Policy (ISP) is a precursor to enforcing good IS governance rules in companies. An ISP exists in 55% of companies and overall, figures only slightly differ compared to 2006 (less than 1%). While large companies still remain in the lead, their figures did however decrease (-6% compared to 2006).

Results clearly show that there is a better understanding of the ISP which no longer only refers to a simplistic document but rather a "full framework" that takes into consideration business risks, includes "head" and "implementation" documents, introduces complete procedures to make the transition to an ISMS[3], etc.. In light of this, it is safe to say that the work of CISOs as well as professional associations is far from over…

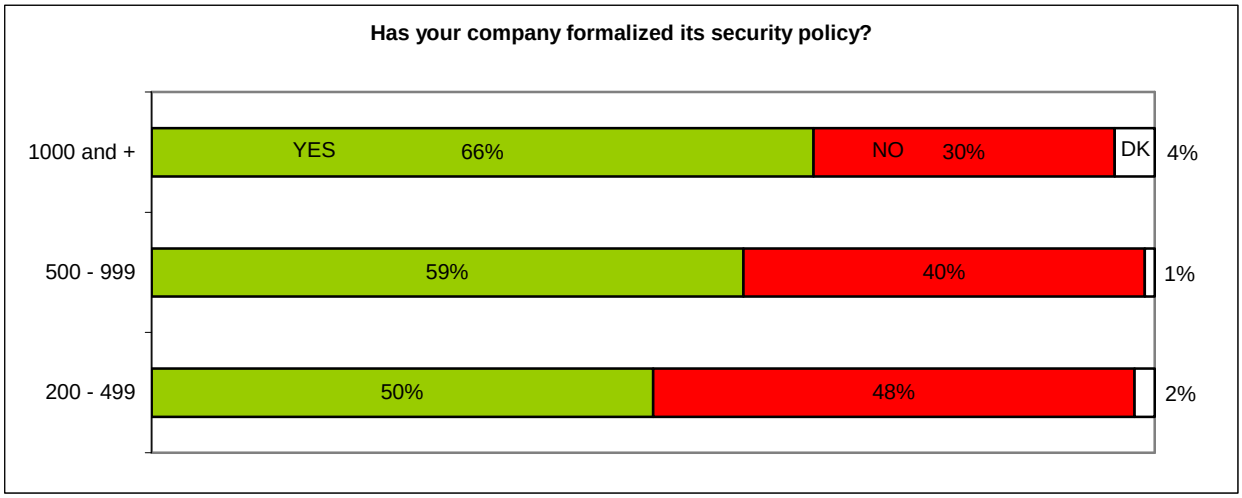

Figure 4: Existence of a security policy by company size

…but a slip in the use of standards

Today, 47% of companies rely on an official standard to formalize their ISP (-1% from 2006). ISO 2700x standards (formerly ISO 17799) are the most widely used. This is especially true in large companies (32%), enabling them to clearly position themselves as the authority in the matter regardless of the –1% compared to 2006!

[3] See glossary.

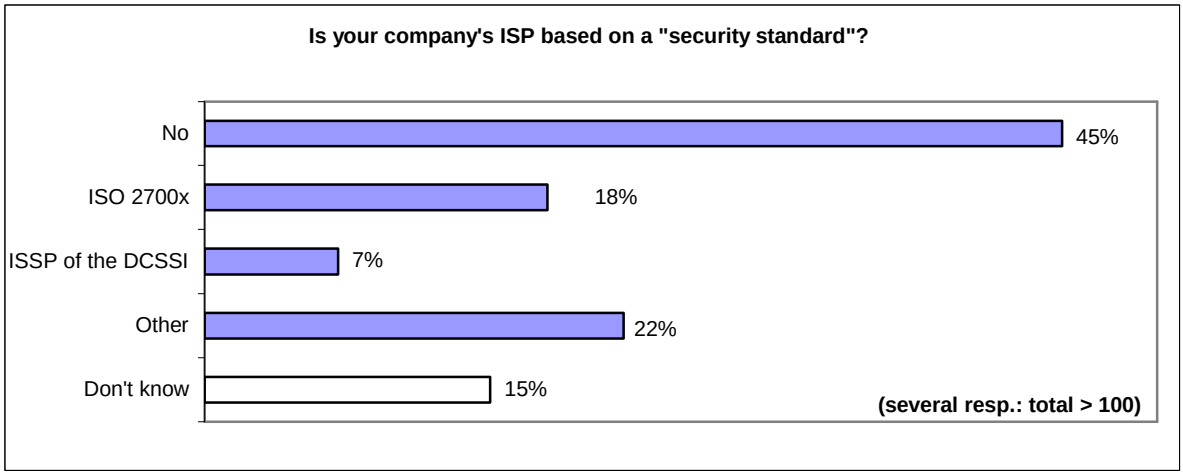

Figure 5: Reliance on a security standard for the ISP

However, standards are not the only bases that can serve as a foundation for developing a formal and consistent IS security process. There are also industry-specific “business frames” (health, certain manufacture industries, etc.) that enable best practices to be formalized without necessarily referring to a standard, used by 22% of companies.

Even so, these standards do act as an interesting guide for ensuring adequate coverage of security issues that CISOs must address. They also provide the advantage of guaranteeing comprehensive treatment of the topics included in the ISP and, as some market players believe, can facilitate the process of obtaining certification for the company, as is already done in the quality domain.

A process supported by executive management?

In 95% of cases, the ISP is explicitly supported by the company’s executive management (59% fully, 36% partially). This demonstrates the willingness of management to provide their company with a formal framework, a genuine culture of IS security and also a desire to involve employees in implementing this policy. As regulatory pressure toughens in response to corporate scandals caused by poor management, and as the number of highly publicized information disclosure incidents (especially personal data) continues to grow, companies will increasingly be forced to put in place stricter IS governance rules.

Unfortunately, as the other figures of this study show, executive management all too often has an inaccurate view of the scope of work that is required to launch such policies and therefore does not invest the necessary means and energy. And yet, once the policy is drafted and validated, the work has only just begun…

Clause 6: Organization of Information Security and Means

The CISO, a poorly identified and assigned duty

Thirty-seven percent of companies reported having a clearly identified CISO position: 16% full time (sole duty) and 21% part time (several duties).

The number of specific CISO positions grows steadily according to the size of the company:

- 31% in companies with 200-499 employees;
- 39% with 500-999 employees;
- 61% with over 1000 employees.

The formal assignment of information security tasks to a CISO has been in visible decline since the 2006 study (42% of CISOs in 2006). Oftentimes, IT managers seem to directly assume this role themselves. When there is no full-time CISO, this duty is indeed handled directly by the CIO or the IT manager over 50% of the time. This role can also be filled by high-level managers (up to executive management) or department managers (finance, internal control, etc.), or even by an external consultant (6.5%).

The CISO, more commonly associated with executive management (at last!)

The shift is obvious: today, the CISO (when such a position exists) reports to executive management in 45% of cases (+6% from 2006) and 32% to the CIO (-9% from 2006). The trend towards the CISO's relative independence from IT duties is becoming more distinct and 68% of CISOs are no longer associated with the CIO.

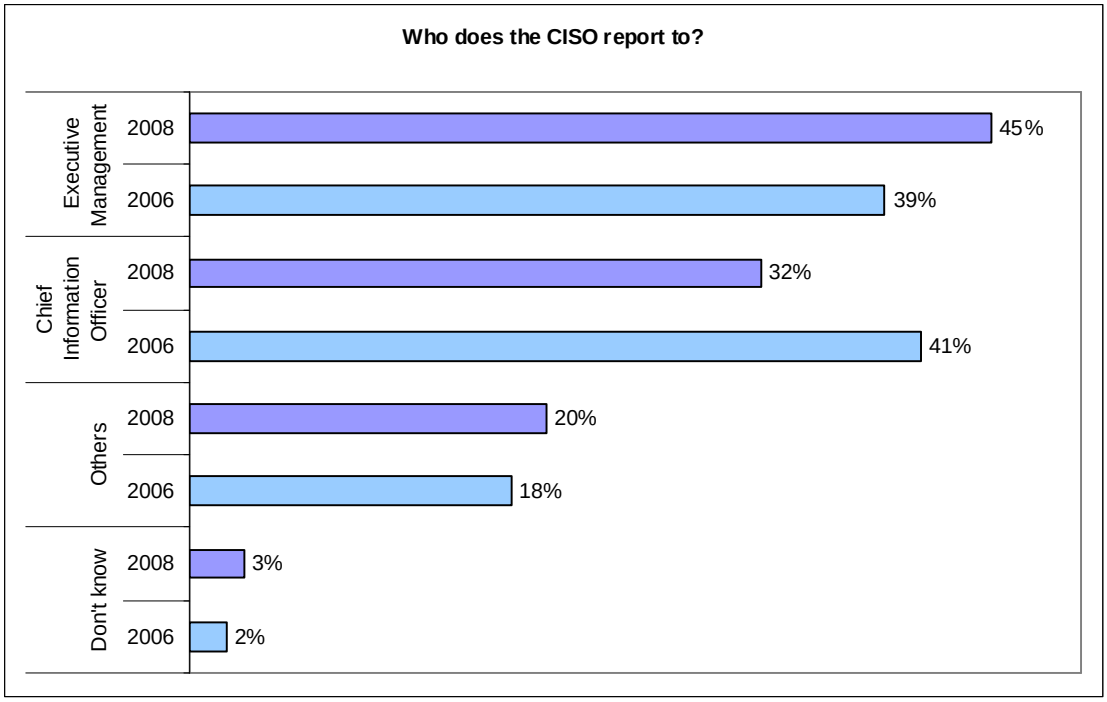

Figure 6: Hierarchical association of the CISO in companies

The CISO: a balance of operational, technical and functional duties

The role of the CISO is divided almost evenly into three areas where an “ideal” distribution is put to the test.

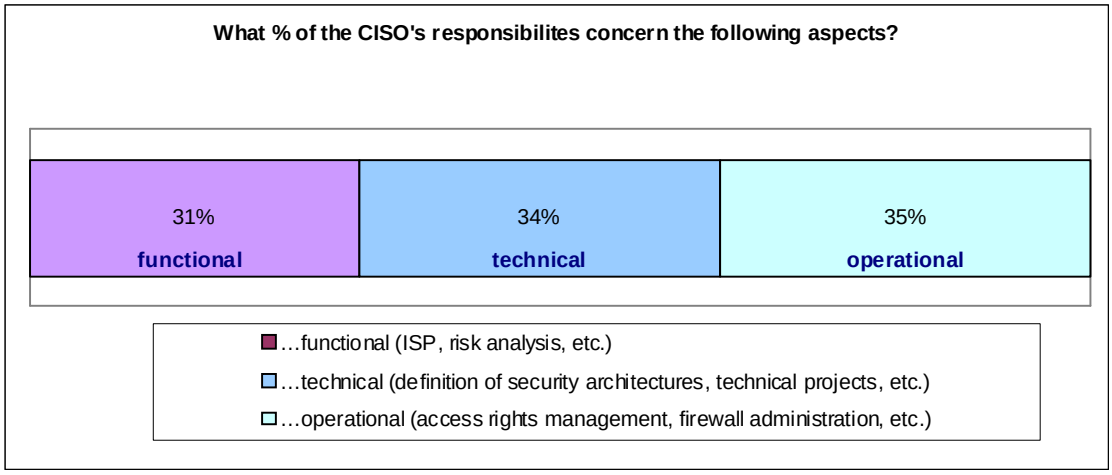

Figure 7: Distribution of the CISO’s responsibilities

The CISO is often a lone figure

On average, 43% of companies do not have permanent teams assigned to information security. When there is a permanent team, 41% have teams of one to two people, 12% have teams of three to five people and only 2% have teams comprised of more than five people.

The human means invested in the management of information security issues seem inadequate in relation to the IT dependence expressed by companies, particularly in the event of heavy constraints (24/7 for example).

Clause 7: Risk Assessment and Treatment

A developing practice of risk analysis

Only 30% of companies surveyed reported that they conduct overall IS security risk analyses, but this figure rises to 60% when including companies that conduct partial risk analyses. The results of the analysis are used in 41% of cases to define IS security priorities.

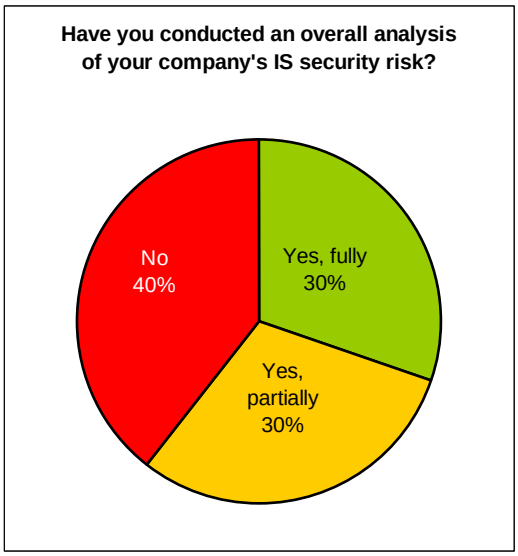

Figure 8: Risk analysis conducted in companies

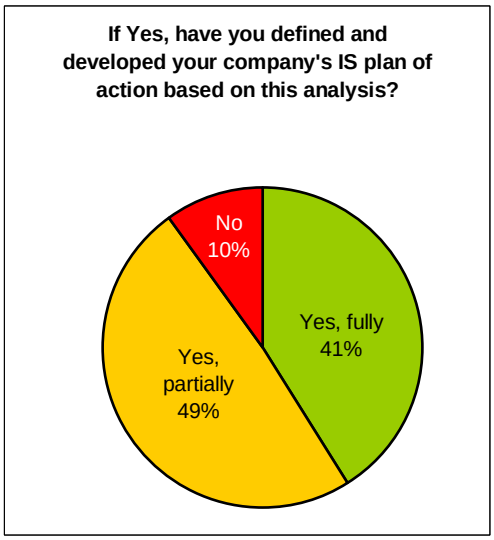

Figure 9: ISS improvement process

A large majority of companies now recognize and take into account the notion of IS security risk when developing security improvement plans. This is excellent news, even if these figures seem optimistic for CLUSIF experts. All too often, the notion of risk analysis remains informal considering that rigorous analysis methods such as MEHARI[4] are still rarely used.

Only 36% of companies systematically take into account risk factors for new IT projects, while 37% perform risk analyses from time to time and 24% never do. The number of companies that always or sometimes conduct analyses (73%) nevertheless remains stable compared to 2006.

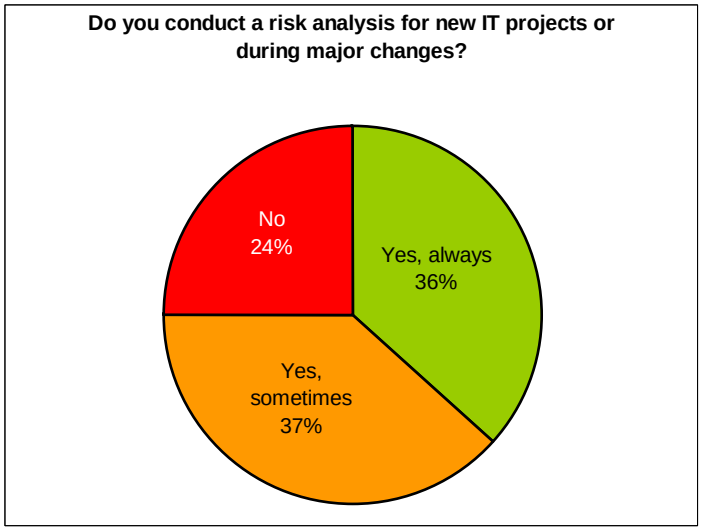

Figure 10: Consideration of risks in projects

[4] See glossary.

The CISO, still the leader in risk analysis

In 35% of cases, the CISO is in charge of risk analysis. Only 12% of companies entrust this task to department managers who create the IT projects. This proportion is slightly higher in larger companies of over 1,000 employees (14% of cases) but nevertheless seems to be in marked decline since 2006.

This proportion is however expected to increase gradually in the future. It is logical that department managers are responsible for deciding on the acceptable risks for the company, even if these risks will likely affect IS. The role of the CISO is to act as the link between the needs of these department managers and IT managers.

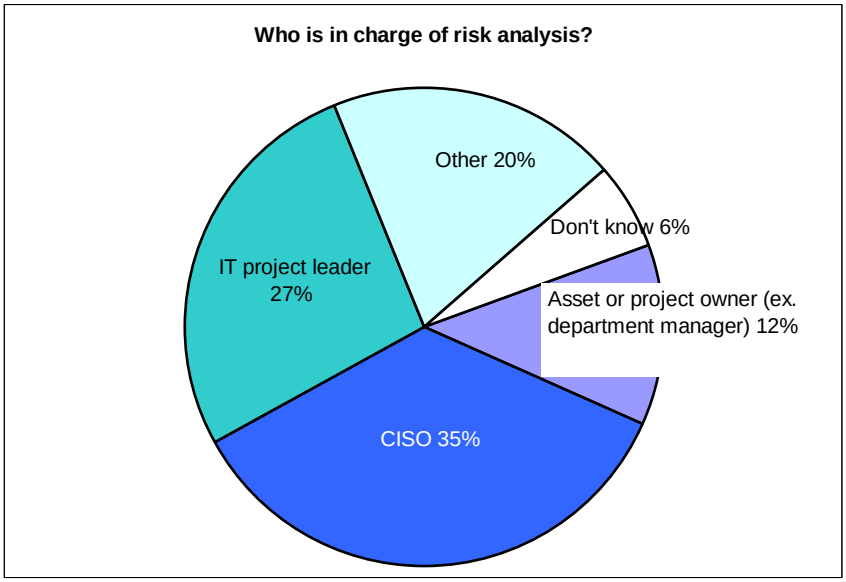

Figure 11: Participants in risk analysis

Clause 8: Human Resources and Security

Security charters level off

The proportion of companies with a security charter has not risen between 2006 and 2008. A slight decline can even be observed (50% of companies in 2008, compared to 55% in 2006). Although this ratio may already seem high (one out of two companies has established a security charter), this document is far from being generalized even though it significantly contributes to raising awareness among users and regulating their practices. Companies with over 1,000 employees (with nearly 60%) as well as those in the service industry (62%) are far ahead, which is proof of a certain maturity in security policies and more substantial means.

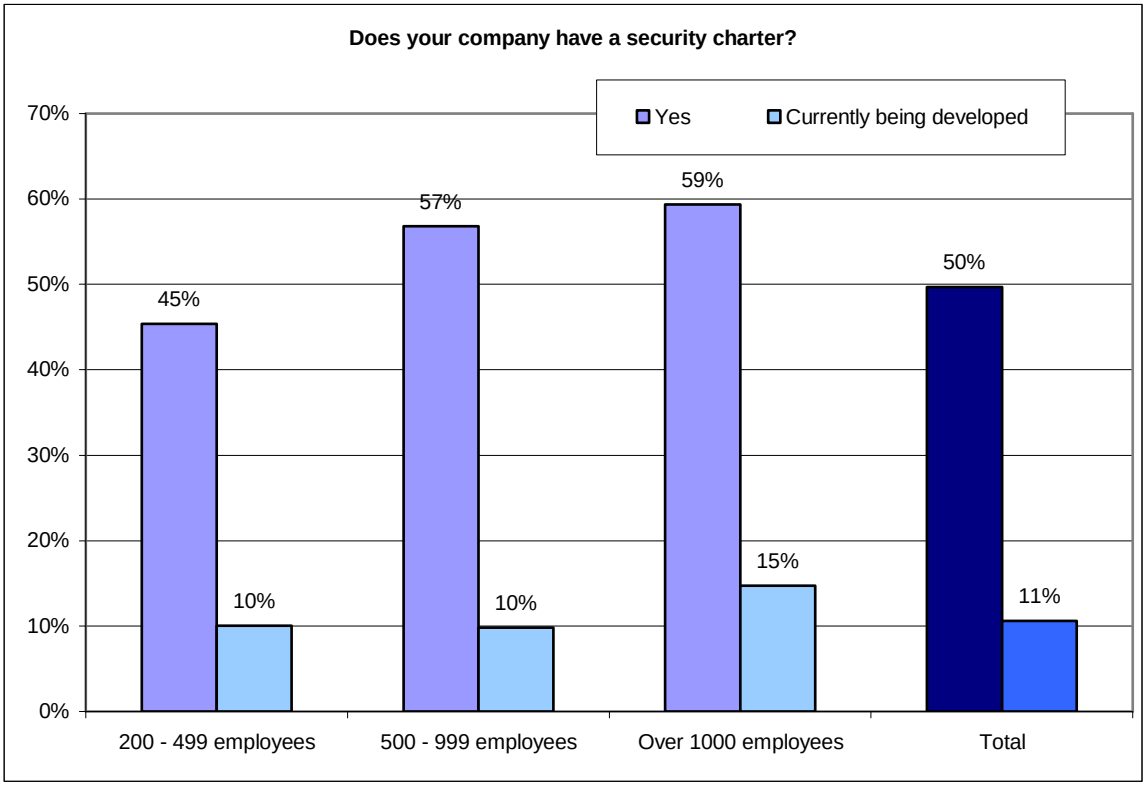

Figure 12: Existence of security charters, a function of size

Eight out of ten companies with a security charter distribute this charter to all their employees (who sign it in one out of two cases) and in 56% of cases, its content specifies the applicable disciplinary measures in the event of non-compliance. The size of the company has an influence on this latter point: seven out of ten companies with over 1,000 employees have incorporated penalties into company rules and regulations, whereas 51% of companies with 200 to 499 employees have done so.

Raising awareness among employees: an underdeveloped practice

A security charter is not always completed with actions to raise awareness among employees about best practices. Only one-third of companies (35%) have instituted information security awareness programs (53% of companies with over 1,000 employees). The range of security awareness tools and their order of preference have not changed since our last survey. Thus, the simplest means such as publishing articles on Intranet or internal newsletters remain the most preferred. Nonetheless, eight out of ten companies do not measure their effectiveness.

During the previous survey, two-thirds of companies had cited publication on different media as one of the preferred awareness tools whereas in 2008, only 42% cited these tools. One would have expected this decrease to be offset by a sharp increase in other methods, but this was not the case. Training sessions in particular did not generate a better score. If we were to be optimistic, we could deduce from these figures that users have internalized best practices, security mechanisms are more efficient and the security culture has become more generalized.

But in our opinion, awareness actions still remain too scarce considering the stakes: only 18% of personnel are trained/informed on a regular basis. For the time being, we prefer to settle with standardized communication methods using articles and/or signs, even if they are clearly less effective.

In the same vein, we would also like to emphasize that the rate of awareness among new employees is rather low (36%) despite that fact that the human factor is always, and rightly so, presented as one of the major weak points concerning security in the company.

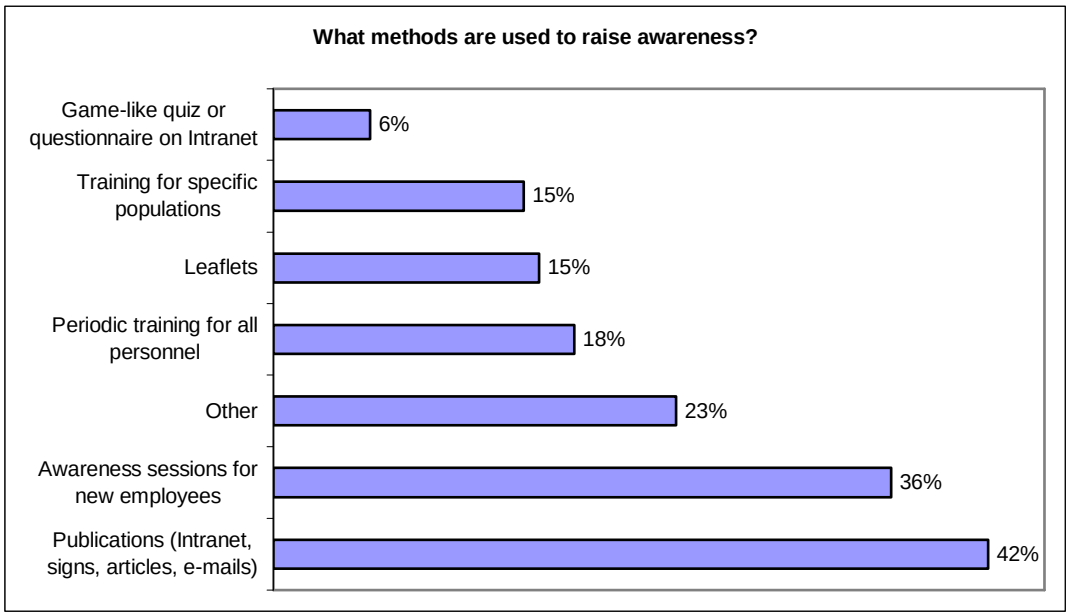

Figure 13: Security awareness tools

Clause 10: Communications and Operations Management

Securing new technologies

Despite decreased use since the 2006 survey (except for PDA/smartphones that are subject to significantly revised conditions), new technologies that invite security risks are most often prohibited by companies to protect themselves against these risks.

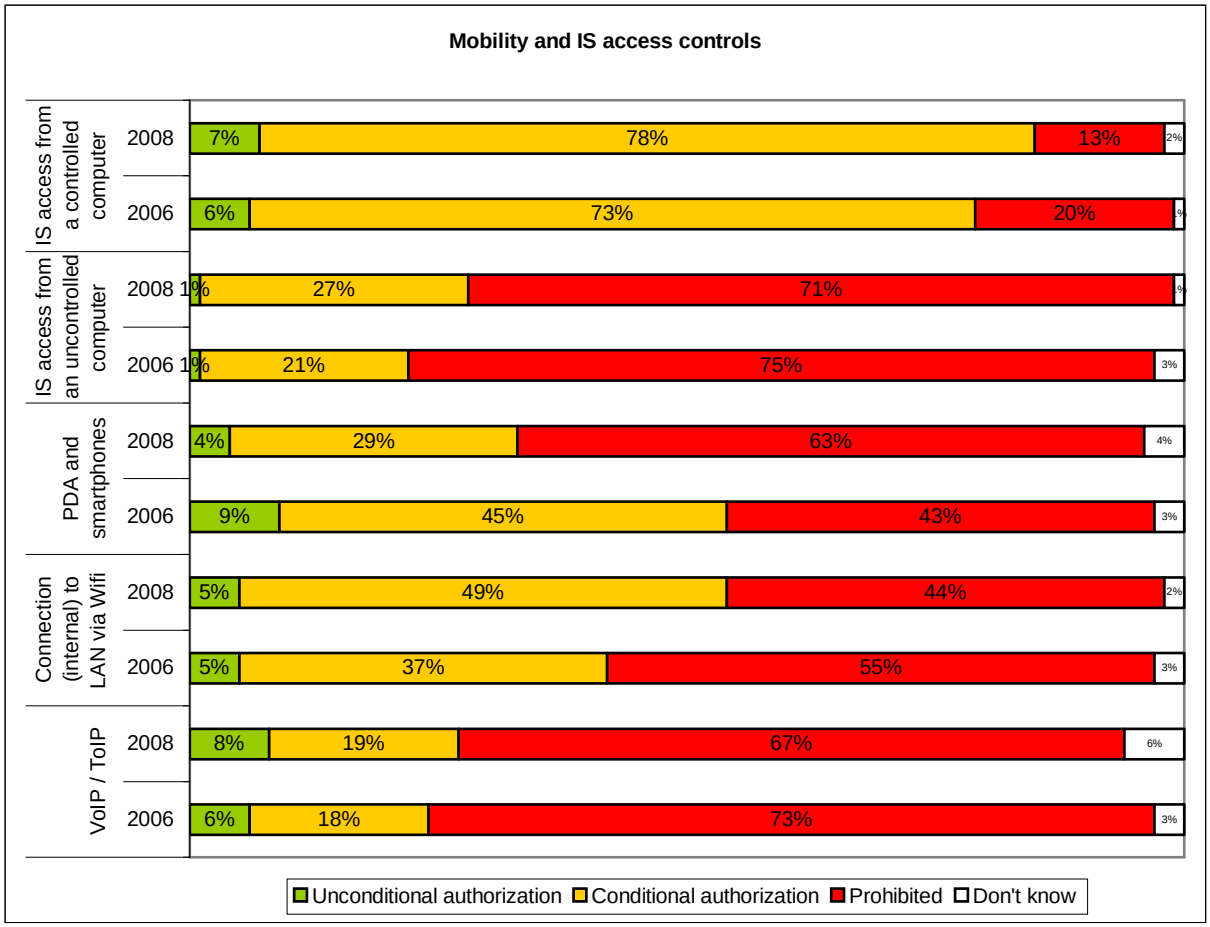

Figure 14: Mobility and IS access control in companies

Mobile devices under control

Mobility is an issue that will remain at the heart of current events as a result of new work methods in companies (staying connected all the time with access at least to e-mail and in certain cases, to software such as Customer Relationship Management for commercial fleets). It is therefore logical that companies have begun to accept these new technologies at the risk of exposing themselves to new vulnerabilities. Today, the company's information system can be accessed:

- with the laptop computer supplied by the company, up slightly compared to 2006. In 78% of companies, the provision of laptops includes means to connect to the company;
- with any computer, such as a PC in a cybercafé or the home computer (27% of companies, up slightly);
- with a PDA/smartphone (33%, down this time). The situation with smartphones is interesting because despite their growing number, their use is prohibited by companies more often than in 2006. This can undoubtedly be accounted to companies' determination

to regain control of equipment that was once split between the two worlds of professional and personal telephony.

When they are implemented, security measures substantially provide protection from perimeter security control problems through now commonplace technologies such as strong authentication or encryption (SSL, IPSec, etc.). Unfortunately, the percentage of companies using these technologies remains rather low.

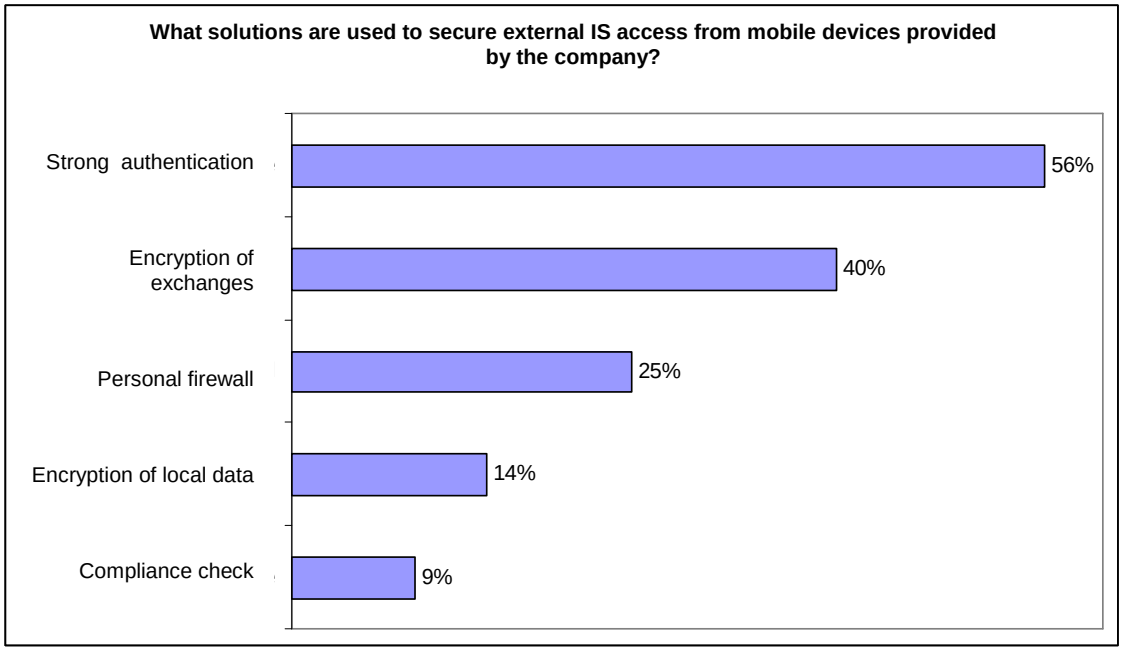

Figure 15: Technologies for securing IS access in controlled mobile equipment

The problem of terminal protection seems to be covered less exhaustively. In spite of regular thefts or losses (in fourth place of incidents cited in this survey), 14% of companies only encrypt local data, which is largely insufficient for the volume of important information that is stored in local files and e-mails of managers.

If we examine the specific case of smartphones, it appears that security solutions are very rarely deployed: only 19% of smartphones are equipped with an antivirus. Although the number of viruses inventoried on these platforms has remained low, it is important to remember that smartphones must be considered as full and complete computers connected to the Internet and their increasingly popular use will, in all logic, be drawing greater attention from malware writers.

Internal mobility (WiFi) on the rise

The use of WiFi in companies is rising: it was prohibited in 55% of companies in 2006, compared to 44% in 2008. Mobility within the company has become a real necessity. Although past experiences have shown security weaknesses in technology, changes in standards now allow for sufficiently secured access points to be put in place with solid verification and encryption systems, even if they require diligent architecture and deployment. In fact, these are the very mechanisms that companies rely on to gradually deploy these solutions (70% and 43% use strengthened authentication and encryption of exchanges, respectively).

VoIP[5] and ToIP[5]: inevitable deployment

Immediate attention was drawn to VoIP and ToIP for showing the greatest stability between 2006 and 2008 (nearly identical figures). Furthermore, 21% of non-equipped companies are considering their procurement, representing the highest rate of equipment purchase plans for 2008.

ToIP is an altogether separate case since it is generally a new responsibility assigned to CIOs, whereas telephony is historically managed by general services. Along with this new field come high "availability" expectations from users as well as its share of security constraints.

Protection technologies and vulnerabilities management

New security technologies struggle to establish themselves

Figure 16: Security technologies/antivirus, anti-intrusion combat, management of vulnerabilities

Antiviruses and firewalls are already used systematically and are therefore a grounded fact; both are necessary everywhere, like locks on doors. Nevertheless, viral attacks remain steady (30% of companies were victims of such attacks in 2007), likely due in part to updating problems on certain installations.

Antispam software use steadily rose to rapidly become nearly systematic which is logical considering the need for this type of tool (in 2007, over 96% of e-mail traffic was spam[6]).

[5] See glossary.
[6] Source: *Panorama des menaces emails (Overview of e-mail threats)- France 2007*, SECUSERVE (January 4, 2008)

The use of intrusion detection systems (IDS) and intrusion protection systems (IPS) remained stable, even falling slightly. Given that IDS require expertise and time to be used properly, and IPS functions are increasingly incorporated into new generations of firewalls, there is a much lesser need to purchase specific packages.

The implementation of a SIM[7] solution remains complex due to multiple event and log sources. Yet these tools are pivotal for properly monitoring systems and also serve as the basis for possible alert systems (ex., if abnormal activity is detected on a particular type of event). The fact that the largest companies envisage the most projects for 2008 (10%) is telling evidence that this issue remains a real concern.

Safeguarding computers is a topic that is gaining momentum as can be seen in the "product strategies" of software editors, most of which now offer complete suites in their company range including antivirus, firewall, port management, etc.. It is also apparent from the results of the survey that the use of personnel firewalls is on the rise overall. They are more systematically used today with laptop computers on which they are obviously essential when connecting to open networks.

On the other hand, data encryption has not increased. Although encryption tools are fairly easy to apply on laptops to prevent loss or theft, they are much more complicated to put in place when dealing with shared data. This scenario would require a process for classifying information and formalizing organizational processes to manage encryption keys and access rights to the encrypted data.

[7] See glossary.

Clause 11: Access Control

Logical access control is considered from three aspects:

- heavy authentication means that may be used;
- means of managing and implementing user access rights;
- systems of centralized access control and unique authentication (Single Sign-On).

Responses revealed that these technologies are still rarely deployed and above all that the situation does not seem to have changed over the past two years with 2008 results nearly mimicking those of 2006. Although the opening of systems and mobile uses in particular, has substantially increased since 2006, access control unfortunately has not followed suite.

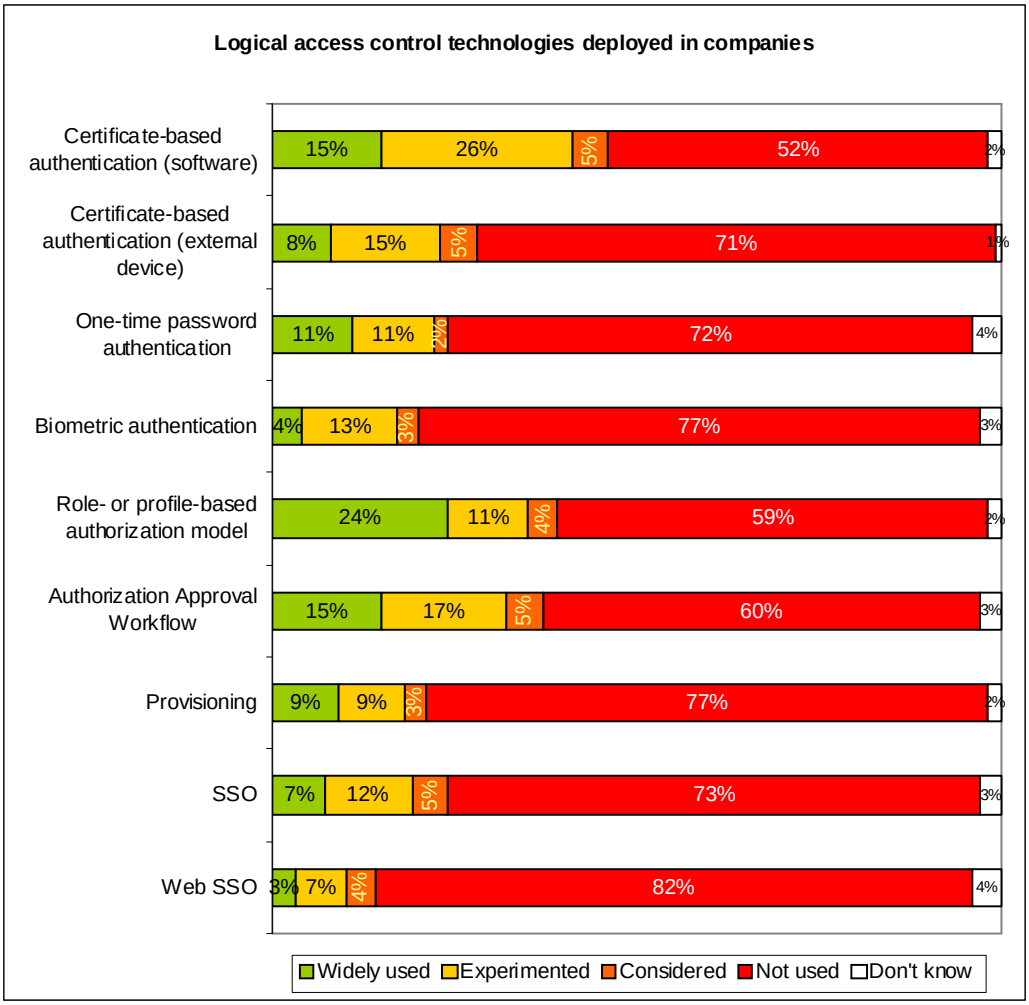

Figure 17: Logical access control technologies deployed in companies

Slight breakthrough of biometrics, rise in certificates

Authentication methods are the keystone of digital identity and thus, one of the fundamental elements of IS security, particularly with regards to traceability. While the great majority of companies still do not use strong authentication and are not considering experimenting with other available solutions in 2008, biometrics has nevertheless made a slight breakthrough: 4% of companies have begun widespread use these past two years and 8% are currently in the experimentation phase.

The use of software-based electronic certificates, a leading solution in 2006, still remains the preferred option and even shows a slight boost in its figures. An additional 5% of companies have incorporated them and a steady volume of companies are in the experimentation process. Yet with half of the companies still not considering making the move, mass adoption is far from being achieved.

The other strong authentication technologies do not show a marked evolution.

Surprisingly, the companies that were pioneers in this field are not the largest companies, but those in the 500 to 999 category. For example, 19% of them use electronic certificates in software form, and 15% in hard forms (microchip cards, cryptographic USB keys, etc.), compared to 14% and 9% respectively out of all the companies.

As in other areas, the financial and service industries stood out among the other business sectors as leaders in strong authentication method deployment. Only in biometrics did another industry (transport and telecoms) consider a more in-depth study of this solution.

Authorization management: timid progress

There have been no changes in authorization management models over the past two years. Six out of ten companies do not have role- or profile-based models (such as the Role Based Access Control or RBAC model), and are not considering acquiring them in the short term. As this model is often a prerequisite for controlling rights, the inability of these companies to streamline their rights management processes is cause for concern.

However, it seems that those companies that had put in place such a model in 2006 have continued their logic by reinforcing their management tools. Some have either implemented an authorization approval workflow (+6% in the experimentation phase; the number of workflows used remains the same), but the most advanced have even put in place a provisioning system (also +6% in the experimentation phase) for a number of stable, fully-operational devices.

The small number of companies that intend to reinforce their authorization management in 2008 is surprising considering that legal and regulatory amendments (Law on Financial Security, Sarbanes-Oxley, etc.) set forth stricter requirements concerning traceability and control of access rights.

Access control and SSO: large companies experiment

Although Single Sign-On systems (SSO and Web SSO) also struggle to attract companies, there has nevertheless been a slight improvement in view. While the number of companies that have generalized their use has remained steady, the figure doubles for those in the experimentation stage in 2008, with a sharp increase among the largest companies. Indeed, experiments are proportionally twice as numerous in the 1000+ employee category as in the other categories. However, more than three-quarters of companies are still not considering such solutions despite the genuine reassurance they provide to users, and which thereby facilitate respect of stricter password policies.

Clause 12: Acquisition, Development and Maintenance

Surveillance and management of vulnerabilities: a stabilizing situation

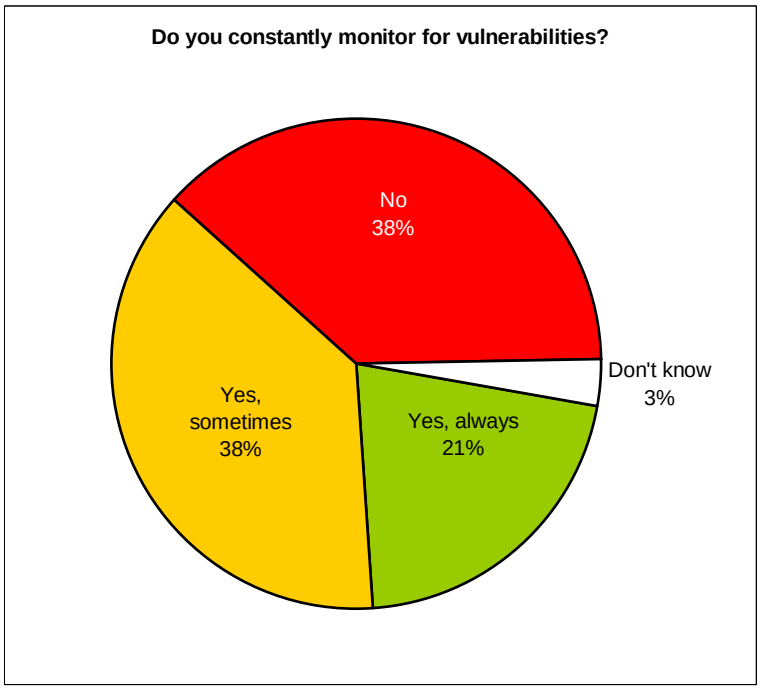

Figure 18: Surveillance of vulnerabilities in companies

According to the responses, 59% of enterprises always or sometimes monitor for new security flaws and new attacks. The large companies replied that their surveillance is systematic and covers a very broad scope of their technical environments. This figure remains approximately stable compared to 2006. Overall, companies have not reinforced their vigilance with regards to threats.

Maintenance and deployment of security patches: improved automation

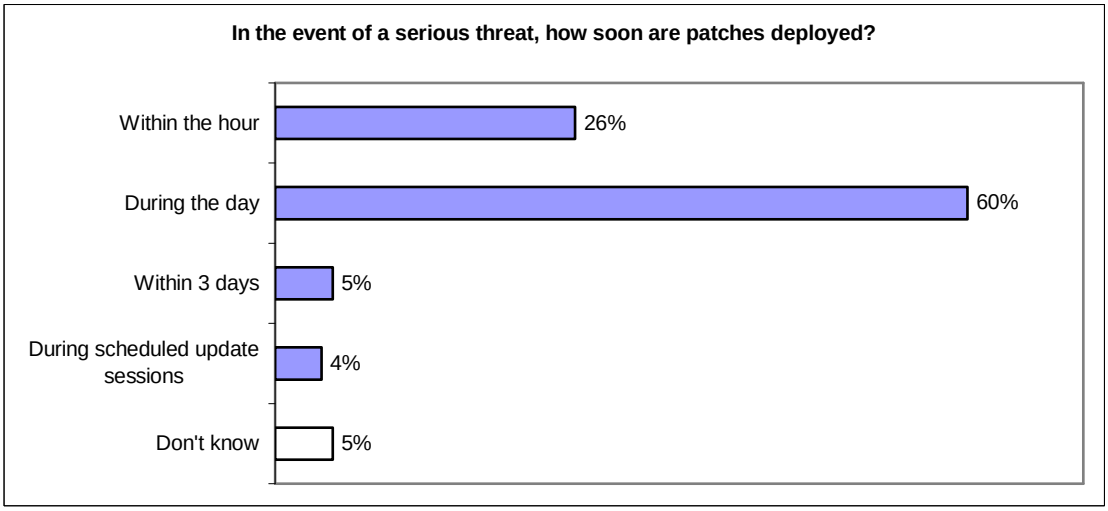

Figure 19: Time frame for patch deployment in companies

Nearly half of the companies have formalized patch deployment procedures with companies of over 1,000 employees in the lead.

Among those that apply patch deployment procedures, 86% of them deploy their patches in less than one day, which represents an increase of almost 10% between 2006 and 2008. The use of automatic deployment devices therefore seems to be significantly on the rise, at least for "workstation" environments. CLUSIF has observed that although patches are commonly deployed on work computers, its use is still not widespread in server environments.

Clause 13: Incident Management - Disasters

Little change in the follow up of security incidents

The proportion of companies surveyed that do not have a team specially assigned to manage malicious security incidents has remained nearly static at 60% since 2006. For companies that perform a follow up, a third of them have a special security unit. For the remaining two-thirds, a unit exists but it also handles other operating functions.

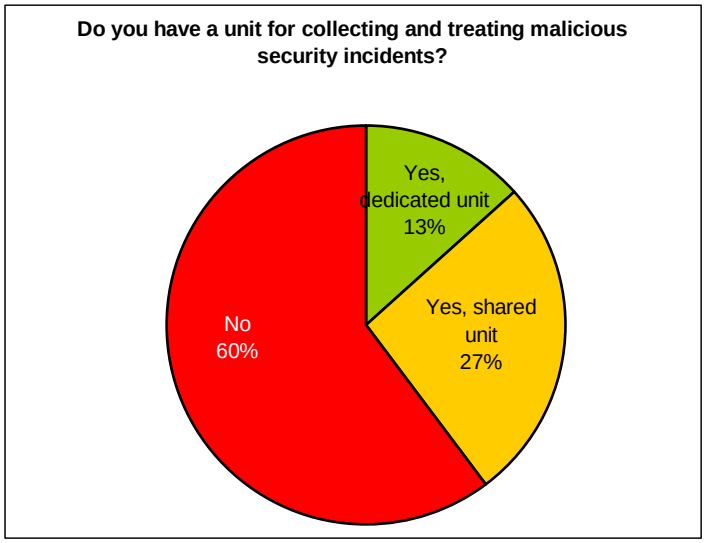

Figure 20: Units for collecting and treating malicious incidents

Companies still reluctant to file complaints…

The rate of filed complaints is absolutely stable at around 5% of surveyed companies, although a number of them had encountered incidents that called for legal action. Despite various interventions by authorities, in particular the National Gendarmerie, the Police Prefecture (BEFTI), the National Surveillance Directorate (DST) and the National Criminal Investigation Directorate (OCLCTIC), as well as awareness campaigns launched in 2007 among CISOs, these efforts have not yet produced the desired results and many cases are never reported.

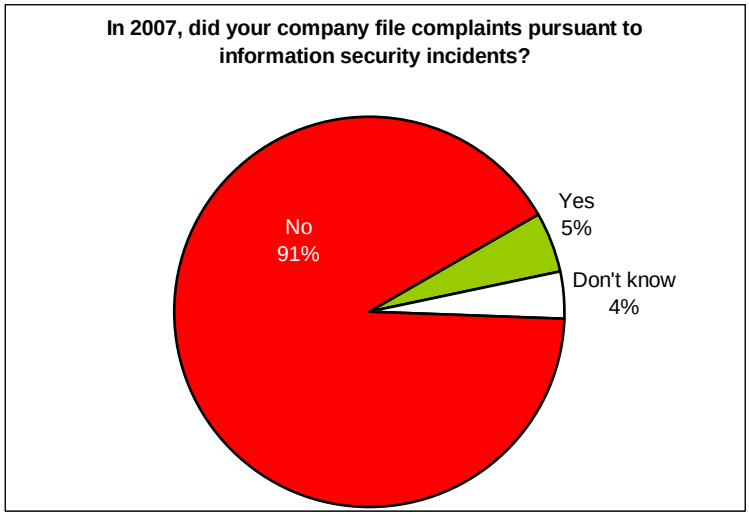

Figure 21: Complaints filed by companies

… but 56% of CISOs mentioned at least one incident

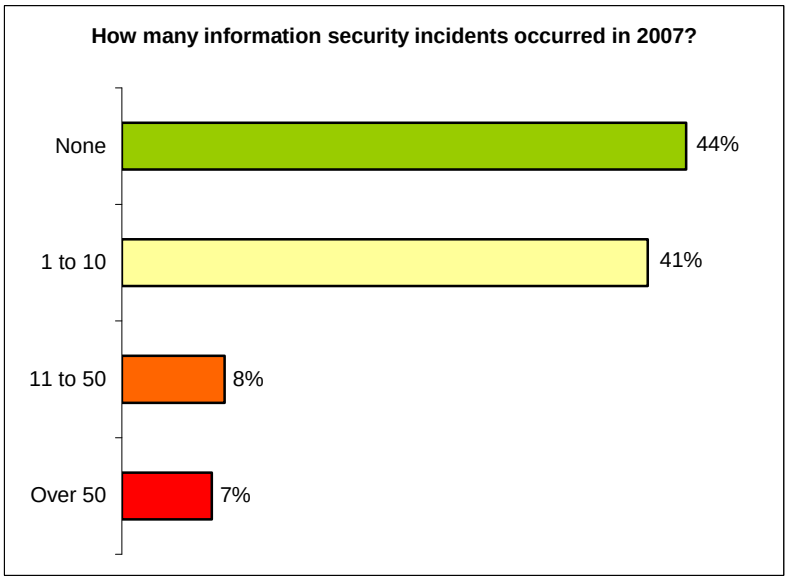

Figure 22: Number of security incidents inventoried in 2007 by companies

Evaluation of financial impact: less than one out of three companies!

The latest observation, consistent with the unsatisfactory picture already presented, reveals that only 28% of companies evaluate the financial impact of security incidents. However, this rate did rise very slightly (from 24% to 28% between 2006 and 2008) and we can only hope that this trend will be consolidated in the next two years.

Covering disasters with insurance: only in 15% of cases!

Furthermore, the financial impact of security disasters is not absorbed (41%) or is undetermined (25%) whereas they can be covered by insurance (only 15% in our study) or bank loans (0.5%).

Few variations in the types of security incidents

Compared to 2006, there is no significant change in the types of incidents reported, although the percentage of equipment theft or disappearance and viral infections has declined. On the other hand, there is a major increase in information disclosure and targeted attacks (+50%) and the evolution of this trend will need to be closely monitored in the years to come.

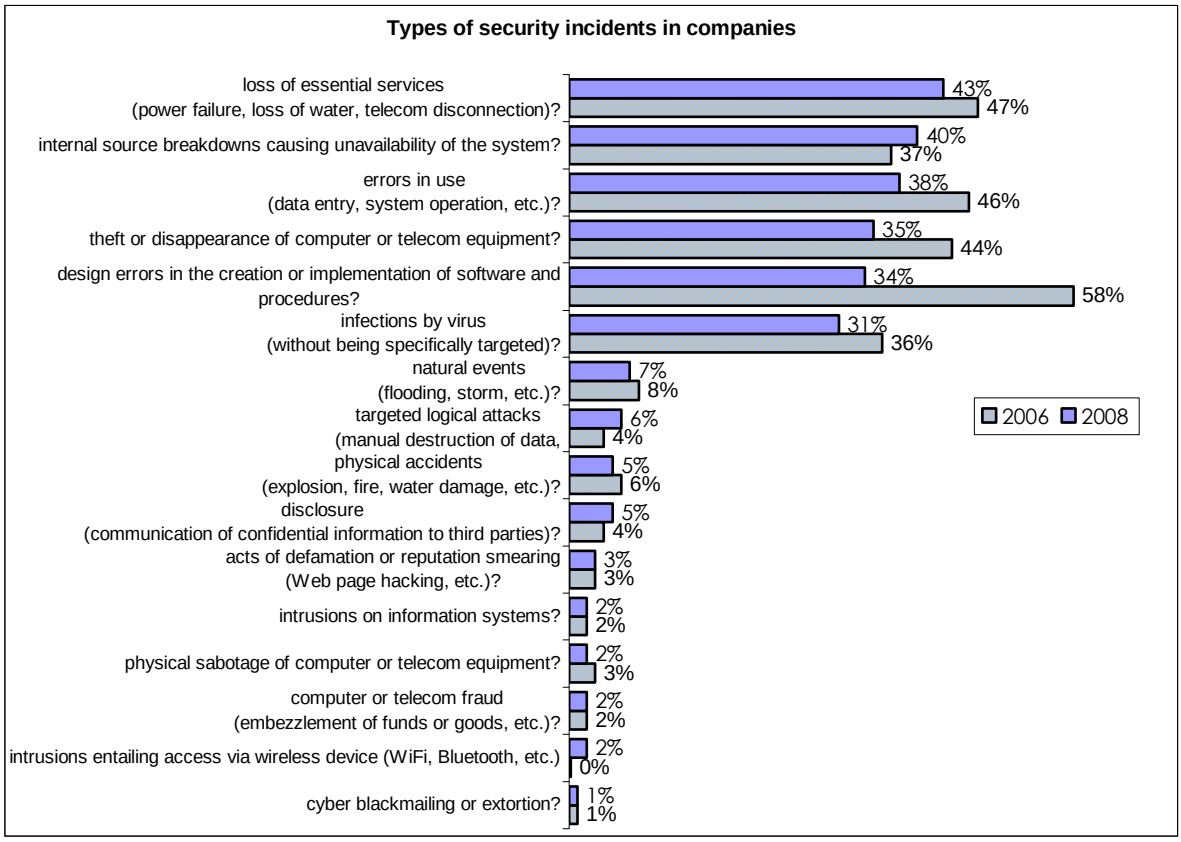

Figure 23: Types of security incidents in companies

Clause 14: Business Continuity Management

Business continuity management: major inequalities in the control of processes

Although it is a given that the company's business is dependent on its IT system, we have noticed significant inequalities in continuity management control. Forty percent of companies still have not implemented a contingency plan whereas a little over a quarter of them (28%), regardless of size, consider that they have put in place a process that covers all of their critical activities.

Generally, the smaller the company, the less it relies on a business continuity plan. This is most likely due to a misconception of the complexity and cost of implementing such a plan.

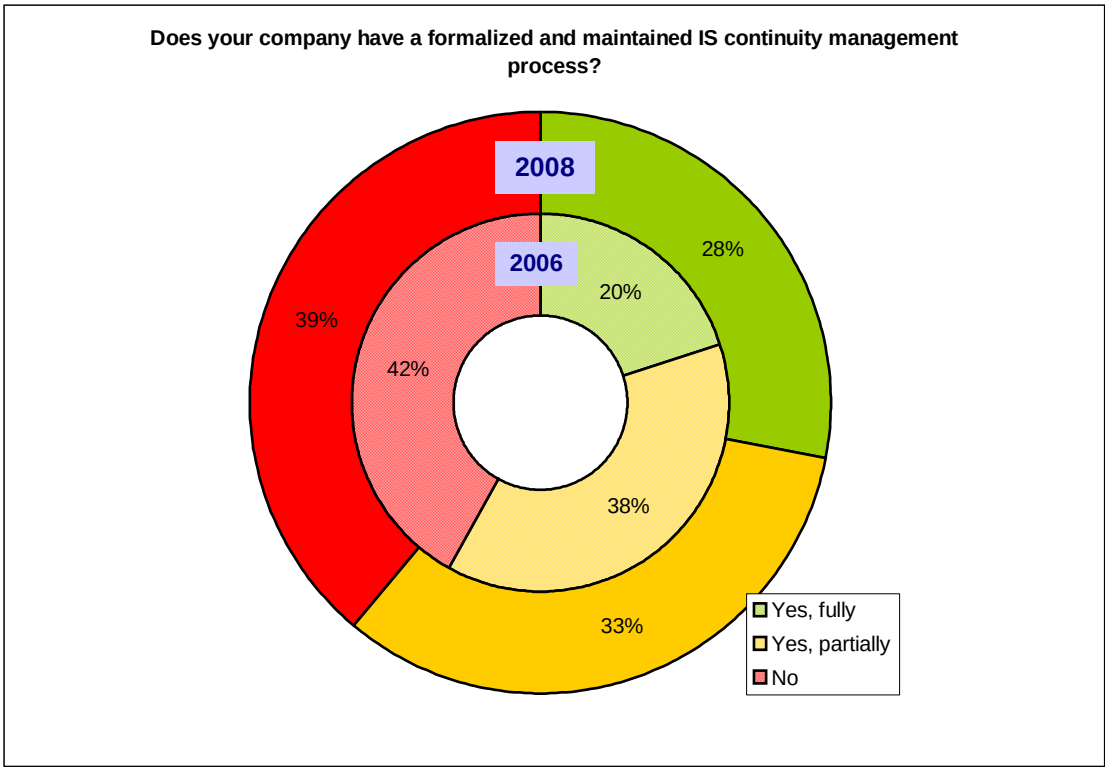

Figure 24: Existence of a formalized process for IS continuity management

Maintenance: a necessary effort

Companies that have a continuity plan seem to have fully understood the need to ensure the "operational maintenance" of this process: less than 10% only do not test and regularly update their business continuity plan. On the contrary, and reassuringly, 72% of them conduct a test at least once a year.

Although business continuity processes primarily handle the IT aspect (data backup, disaster recovery), processes for crisis management and business continuity of departments often remain underdeveloped in a great number of cases.

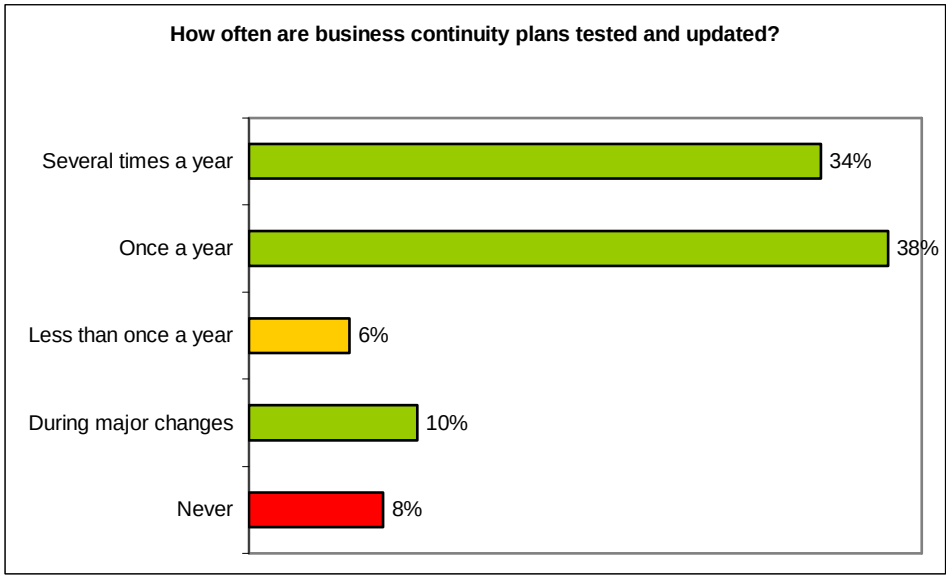

Figure 25: Testing frequency of business continuity plans

Disaster recovery: backups remain the primary tool

To mitigate major disasters, the most frequently-used solution remains traditional backup methods (nearly 80%). However, very often we have observed that basic, essential work needs to be performed to ensure that the backup plan properly incorporates regular externalization of media in accordance with the company's stakes in the event of a major impact on its critical activities. Unfortunately, all too often we still encounter companies that, while backing up data, leave devices/media in the computer room. A disaster would result in complete loss for the companies.

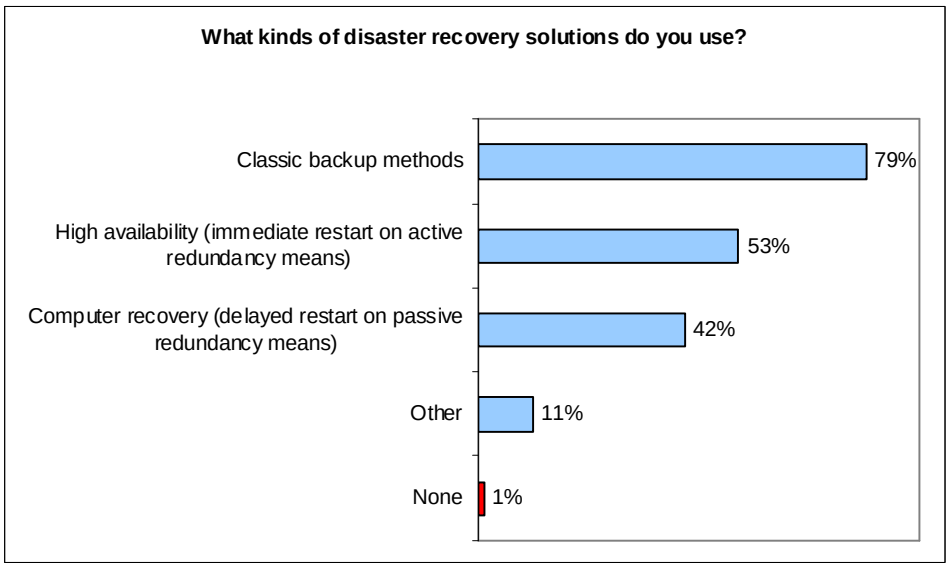

Figure 26: Disaster recovery solutions

All the 2008 figures concerning business continuity are rather comparable to those of the 2006 study. Continuity management is therefore maintaining its excessively slow pace regardless of regulatory pressure in certain industries and the overall development of risk management in companies.

Clause 15: Compliance

This clause addresses three aspects of compliance-related issues:

- compliance with the obligations of the French **Act on Data Processing, Files and Individual Liberties**;
- control of security levels through **audits**;
- monitoring of security levels through security **dashboards**.

1/ Obligations pursuant to the Data Processing Act

Just as many companies still in non compliance with the requirements of the Data Processing and Individual Liberties Act

The percentage of companies that replied as being in compliance with the obligations of the French Data Processing, Data Files and Individual Liberties Act has not changed since the 2006 survey. A third of the companies considered that they were not in full compliance. The marked development of Data Protection Officers should make it possible to boost this figure in the near future.

The Data Protection Officer – better defined

Twenty-five percent of companies (approximately 1,500) stated that they have appointed a Data Protection Officer (DPO). This year, responses from the companies surveyed correspond with official data supplied by the French Data Protection Authority (CNIL), which indicate that at August 20, 2007, a DPO had been incorporated into 1,450 organizational charts. Very recently (May 2008), the CNIL announced that 2,376 DPOs were already appointed in France. The scope of the task entrusted by the Act of 2004 to the Data Protection Officer has therefore become more defined.

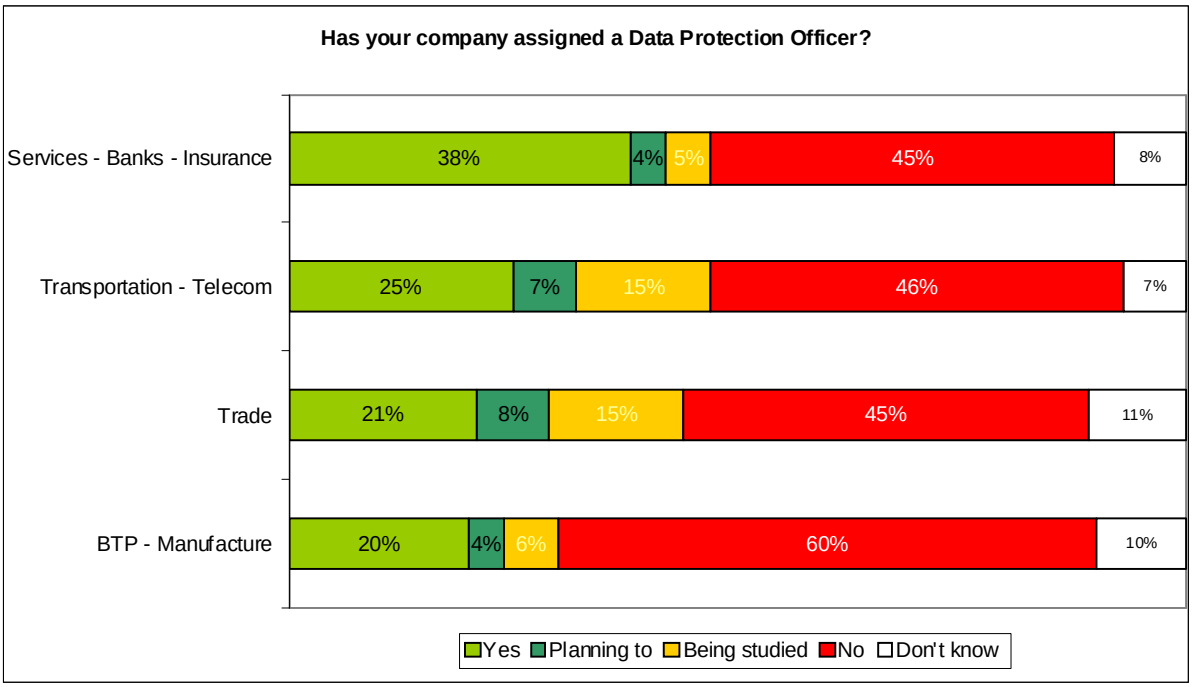

Figure 27: Data Protection Officers in companies by branch of industry

2/ Audits

35% of companies never perform a security audit

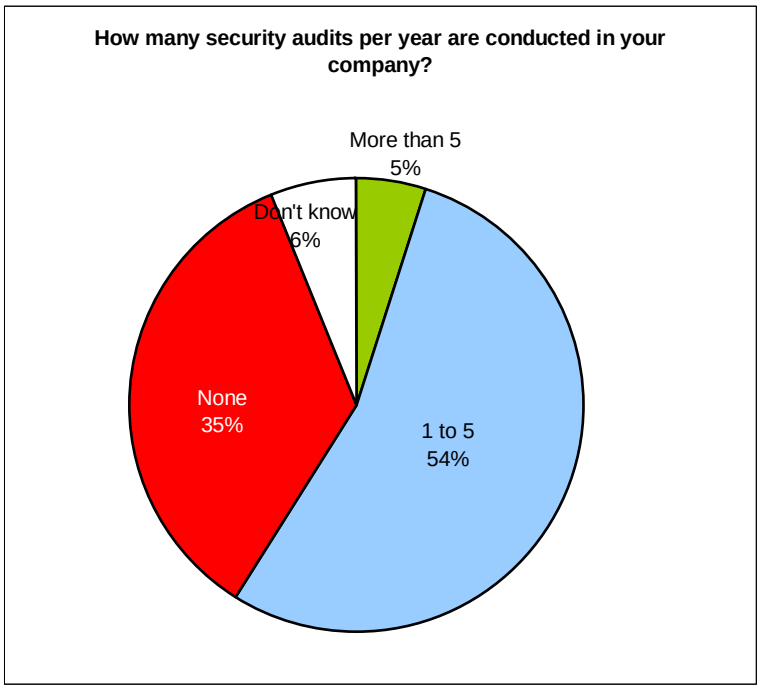

Figure 28: Number of security audits conducted a year in companies

The number of companies that carry out at least one audit (59%) has fallen slightly compared to 2006 (69%) when we had noted a spectacular jump. This rate increased only in large companies (over 1,000 employees) with 82% conducting at least one audit per year, up from the 75% in 2006. In these companies, audits are becoming systematic.

One out of two times (56%), these audits are performed pursuant to internal policy requirements or otherwise, contractual or regulatory obligations.

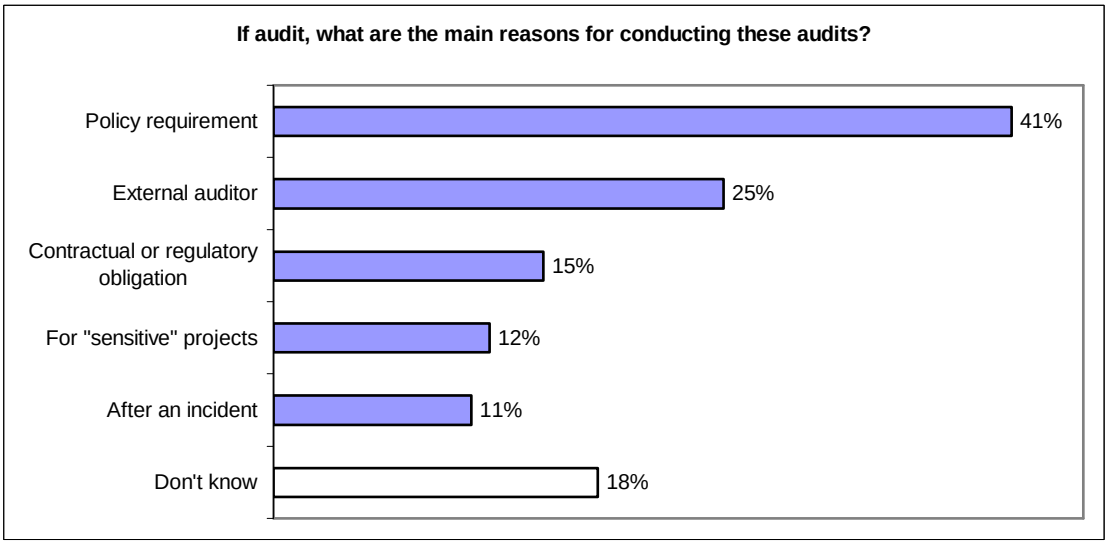

Figure 29: Reasons for security audits

It should be noted that the percentage of audits done by external service providers has risen sharply since 2006 (25% compared to 12%). This evolution seems consistent given that it is increasingly common for companies to outsource all or part of their computer processing operations.

3/ Security dashboards

Over 75% of companies do not regularly measure their security level

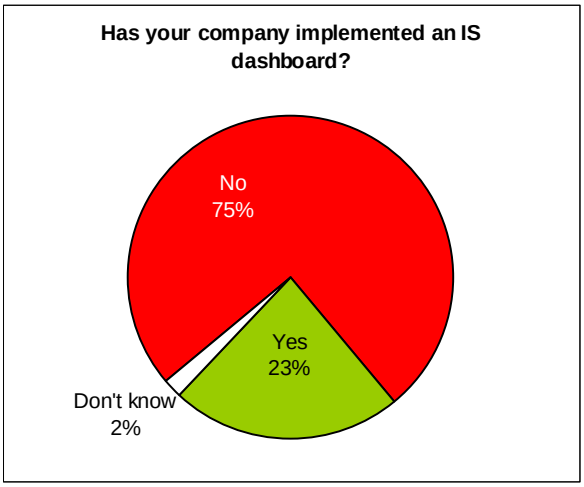

Figure 30: Implementation of dashboards in companies

A clear increase can be seen in the number of companies that distribute dashboards to executive management (52% compared to 28% two years ago).

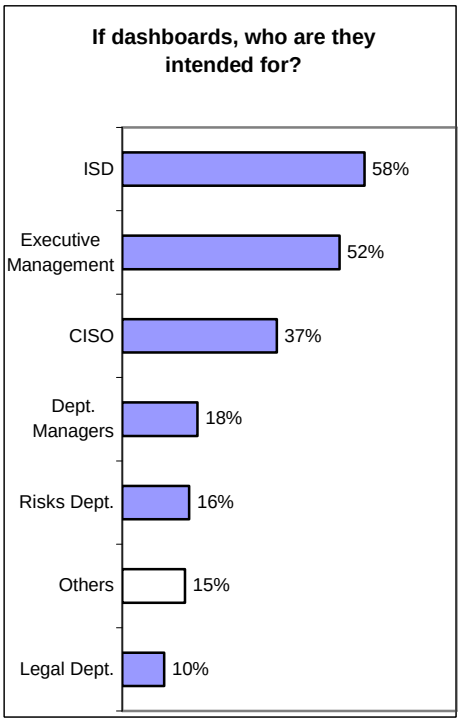

Figure 31: Recipients of the dashboard

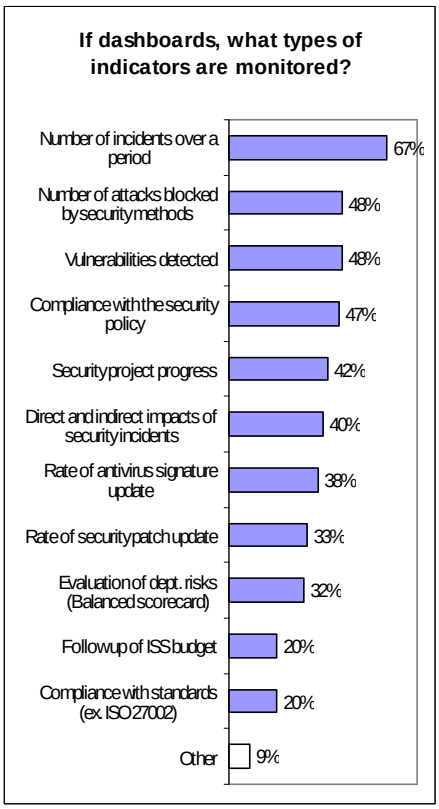

Figure 32: Indicators monitored in the dashboard

The indicators included in dashboards remain mostly technical. The most important topics for piloting (risk evaluation, project progress, budget monitoring, etc.) are rarely used.

Local Authorities

- Presentation of the sample
- Dependence on IT in local authorities
- Resources invested in information security
- Clause 5: Security Policy
- Clause 6: Organization of Information Security
- Clause 7: Risk Assessment and Treatment
- Clause 8: Human Resources and Security
- Clause 10: Communications and Operations Management
- Clause 11: Access Control
- Clause 12: Acquisition, Development and Maintenance
- Clause 13: Incident Management-Disasters
- Clause 14: Business Continuity Management
- Clause 15: Compliance

Local Authorities

Presentation of the sample

Once again this year, CLUSIF has decided to focus on the public sector. The target of the 2006 survey was broadened and is no longer limited to large town halls. The sample surveyed included the following:

- town halls in areas with over 30,000 inhabitants;
- metropolitan communities ("*communautés d'agglomération*") with over 50,000 inhabitants;
- communities of communes ("*communautés de communes*") with over 20,000 inhabitants;
- departmental councils;
- regional councils.

The sample was constituted using the same sampling technique as for companies. It was adjusted according to category to correspond perfectly with the reality of French local authorities.

	Conducted by CLUSIF	**%**	adjustment	**National data**
Town halls	79	40.7 %	➔	34%
Communities of communes	27	13.9 %	➔	32%
Metropolitan communities	42	21.6 %	➔	20%
Departmental councils	41	21.1 %	➔	11%
Regional councils	5	2.6 %	➔	3%
Total	**194**	**100%**		**100%**

Figure 33: Adjusted sample of local authorities surveyed

The survey was conducted essentially by telephone between January 24 and March 10, 2008. Only eight questionnaires were fully completed over the Internet. While CISOs or ISS public officials would have been preferable, every other questionnaire was completed by an IT manager.

The telephone interviews lasted an average of twenty-nine minutes and only approximately two out of ten participants contacted responded to the entire questionnaire. Therefore, to obtain 194 complete questionnaires, approximately 1,000 local authorities were contacted at least once.

Dependence on IT in local authorities

Strategic information systems for local authorities

The survey confirmed that information systems are considered to be strategic by a great majority of local authorities, but not to the same extent as in companies: 68% (compared to 73% of companies) would not be able to tolerate unavailability of even less than 24 hours of their IT tools. This figure falls to 59% for departmental or regional councils.

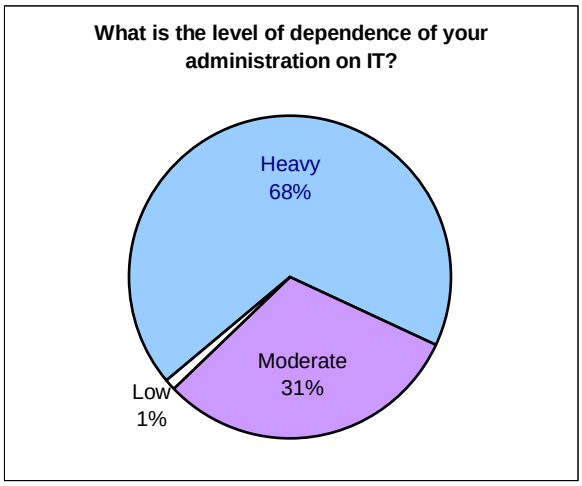

Figure 34: Dependence on IT in local authorities

Resources invested in information security

Average IT budget of €1.5 million

Over one out of two local authorities in our sample agreed to reveal the amount of their annual IT budget, including investment and operating expenditures, while only 25% of companies had agreed to provide this information. Are local authorities more familiar with their IT budget than companies or do they follow a transparency policy that is inexistent in the private sector?

	TOWN HALLS	COMMUNITY OF COMMUNES	METROPOLITAN COMMUNITIES	DEPARTMENTAL/ REGIONAL COUNCILS
Average information budget	€680,000	€1,850,000	€500,000	€3,800,000

Figure 35: Average IT budget by category of local authority

The average IT budget is EUR 1.5 million but this figure is misleading since the majority of local authorities (53%) have a budget of under €500,000.

A security budget with a poorly defined scope

In all cases, budgets allotted for security seem slightly better identified than in the private sector: 26% of persons surveyed could not cite a precise figure for their security budget, compared to 31% of companies. There are no clear trends, even if security budgets of the regions, departments and communities of communes mostly represent less than 6% of the IT budget. A variety of answers were given by towns. Security management is thus tightly linked to local policy.

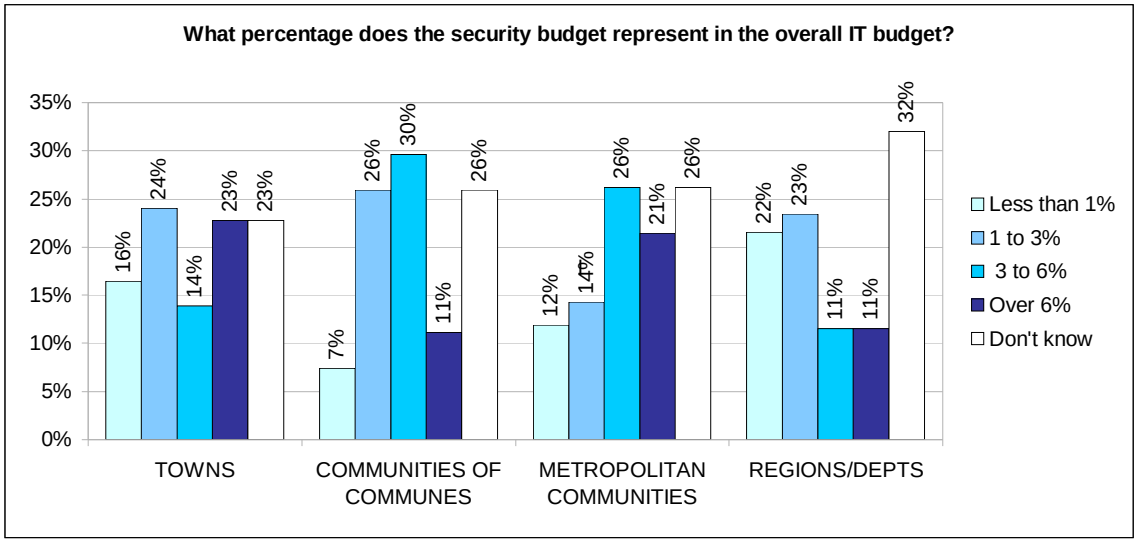

Figure 36: Portion of IT budget earmarked for security in local authorities

In comparison to 2006, public sector security budgets follow a more "wait and see" policy than companies: 49% of budgets on average remained steady compared to 43% for companies. Towns finished in last place with 55% of security budgets that have not changed since the previous survey. The increasing complexity of systems and their externalization therefore does not translate into financial terms. Regions and departments on the contrary invest significantly in security, with communities of communes finishing in second place.

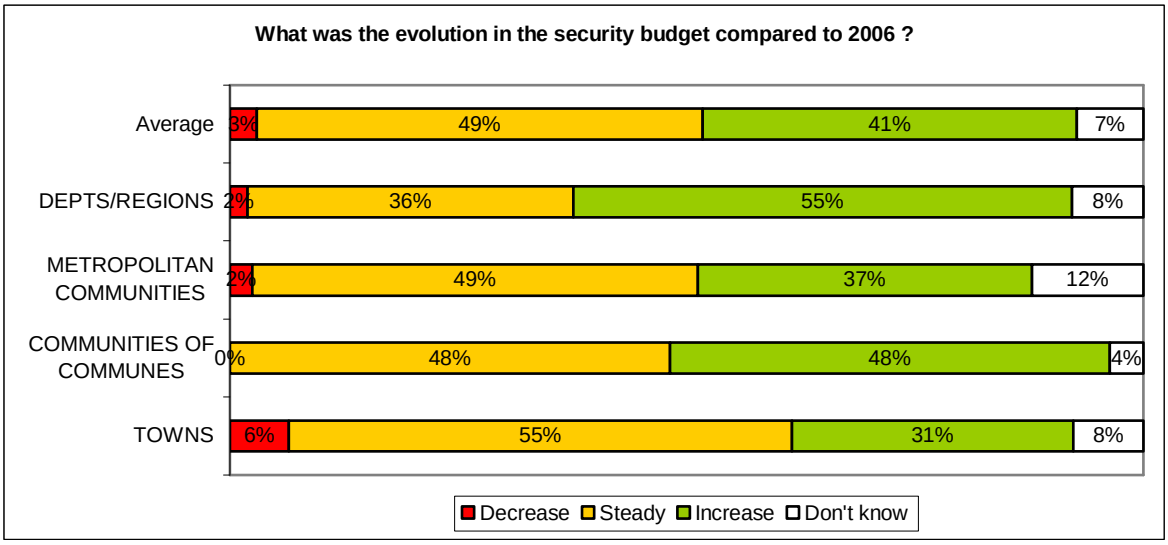

Figure 37: Evolution of the IT budget by category of local authority

When questioned about the obstacles to carrying out security tasks, local authorities cited the **lack of budget** as the main problem nearly one out of two times.

Similarly, CISOs also are handicapped by the lack of mobilization by hierarchy, users and services. Half of the responses stated this reason as the primary or secondary obstacle. This poor personnel involvement is in line with the observation discussed later in this report on the immense progress needed to be made in raising awareness among the personnel of local authorities.

The lack of qualified personnel took the number three position. It was rarely cited as the first obstacle (only by 20% of CISOs) but most commonly given as the second (34%), generally after "lack of budget" or "reluctance of users".

Surprisingly, organizational constraints that CISOs complained about the most in companies only marginally concern local authorities.

Lastly, responses showed that in both local authorities and in the private sector, CIO is an ally to the CISO.

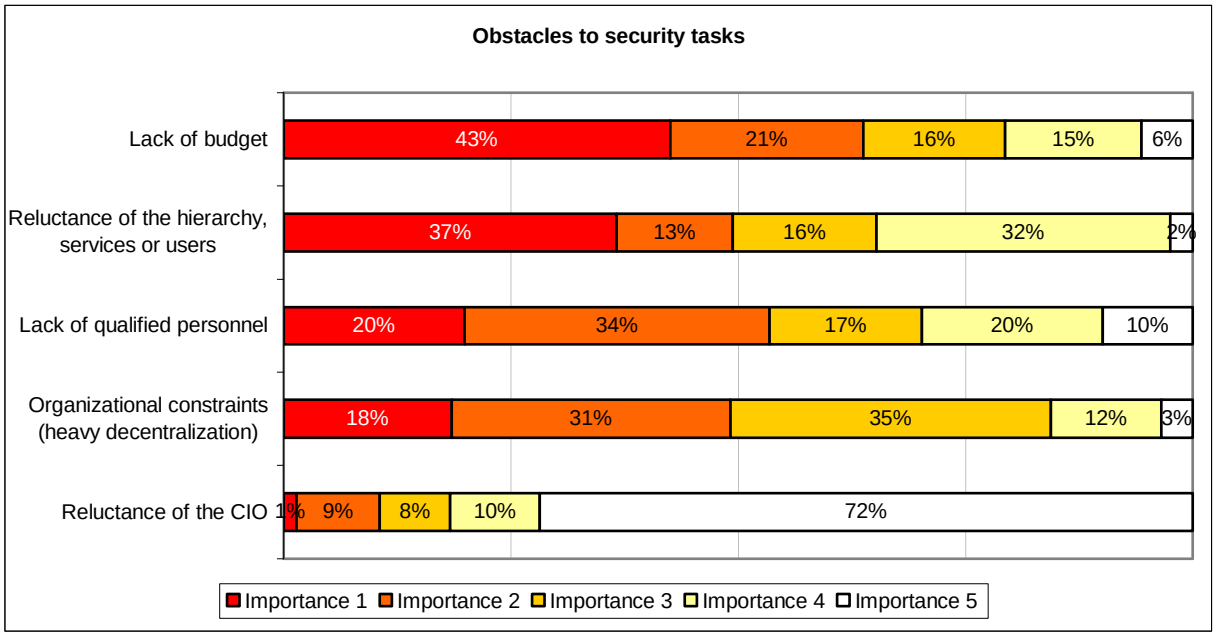

Figure 38: Obstacles to security tasks

In conclusion, budgetary deficiencies as well as the lack of collaboration among personnel (or their lack of awareness of the stakes of information security) complicate the task of CISOs in local authorities. Even if CIOs provide considerable support for projects, the necessary resources are not made available and the inherent complications seem too complex to overcome.

Clause 5: Security Policy

Awareness still remains relative in authorities on formalizing their information security policy (ISP)

Despite their reported heavy dependence on IT systems, local authorities seem to falter when it comes to formalizing their ISP. Only one out of three authorities has done so but with the "full" support of the hierarchy in 70% of cases or "partial" support in 22% of cases.

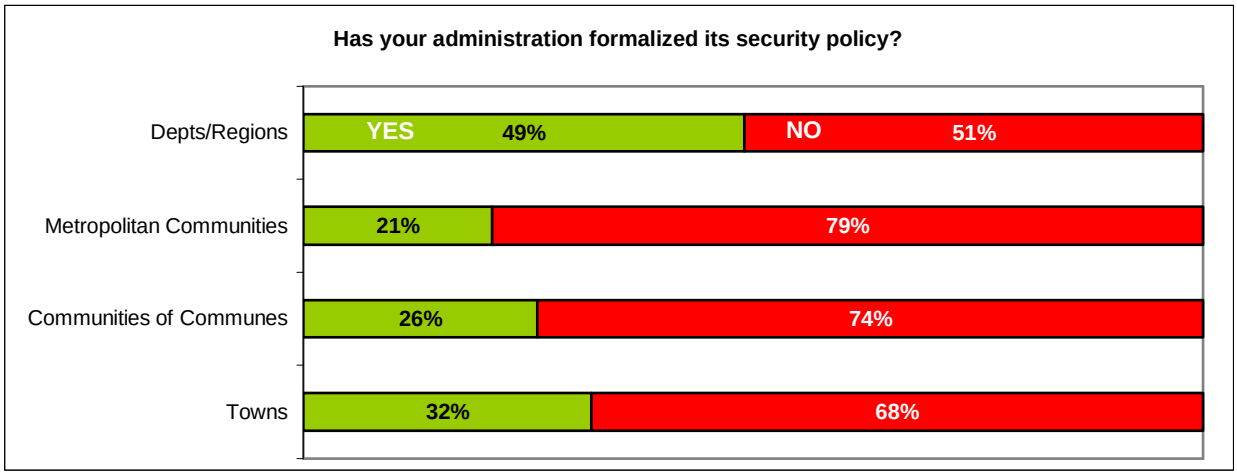

Figure 39: Existence of a security policy by category of local authority

ISP essentially in the hands of IT technicians

In the high majority of cases, ISPs are developed by IT technicians (95%) and very few other players (30% of CISOs and 22% of HRDs, etc.), significantly increasing the possibility of overlooking certain threats and risks.

Very minor reliance on comprehensive standards

Only 44% of town halls that have formalized their IS security policy referred to comprehensive standards such as the ISO 2700x or the ISSP[8] guide of the Central Information Systems Security Division (DCSSI). Lastly, 15% responded that they used another methodological framework, yet no other formal framework currently exists for local authorities!

[8] See glossary.

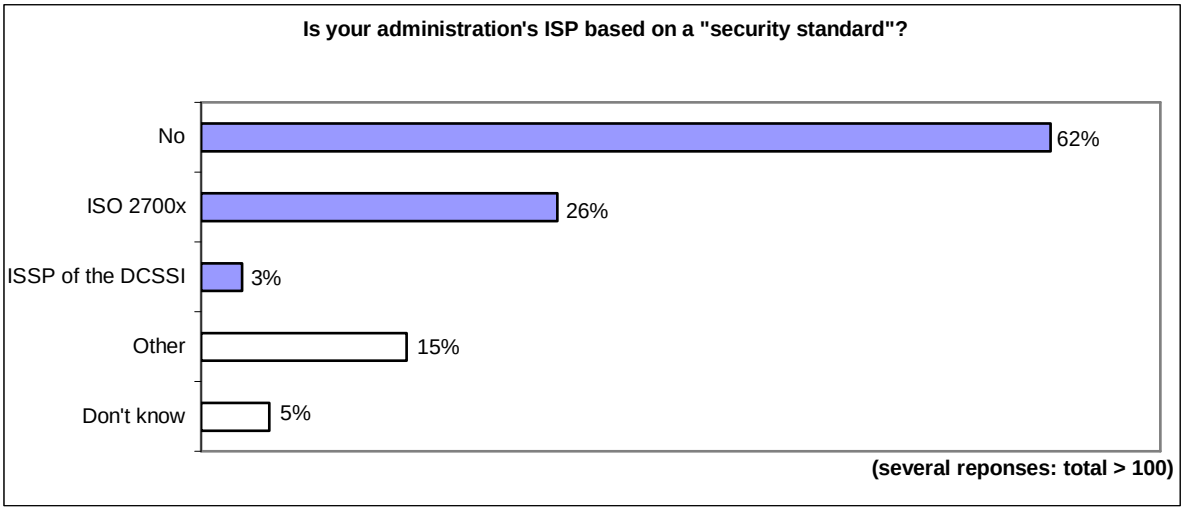

Figure 40: Reliance on a security standard for the ISP

Clause 6: Organization of Information Security

The CISO, a position still poorly identified

Only 22% of administrations clearly identified the CISO position in their organization. These results are relatively similar to those of the previous survey. However, only 6% of them have assigned a full-time role to their CISO.

In other cases, the CIO (37%) or the IT manager (31%) assumes the responsibilities of the CISO. External consultants are also used in 5% of cases.

Furthermore, local authorities lag behind companies in designating an CISO (22% and 37%, respectively).

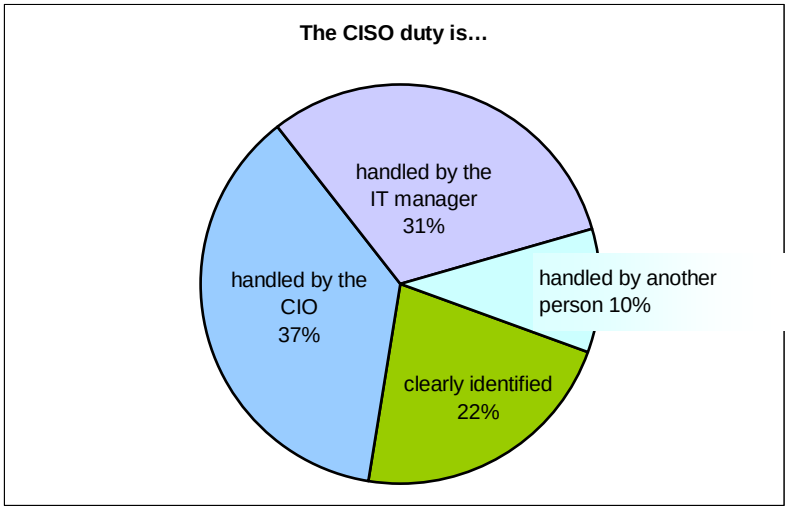

Figure 41: Identification of the CISO duty

The CISO, associated with the Information Systems Department

This trend has intensified since the previous survey with 61% of Information Systems Security Managers working within the Information Systems Department. A small number of local authorities however has directly linked the CISO to the highest elected official (or his/her office), which indicates a strong willingness to protect assets, albeit rare.

While the process is underway for companies, supervision provided by executive management is taking longer to accomplish in administrations.

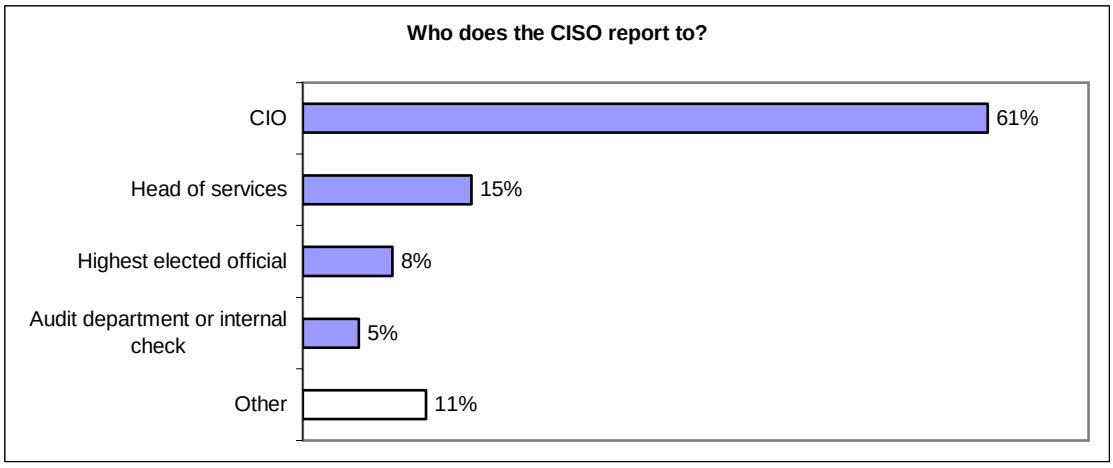

Figure 42: Hierarchical association of the CISO in local authorities

The CISO: a balance of operational, technical and functional duties

The role of the CISO is divided almost evenly into three areas. This distribution is classic and comparable to those found elsewhere.

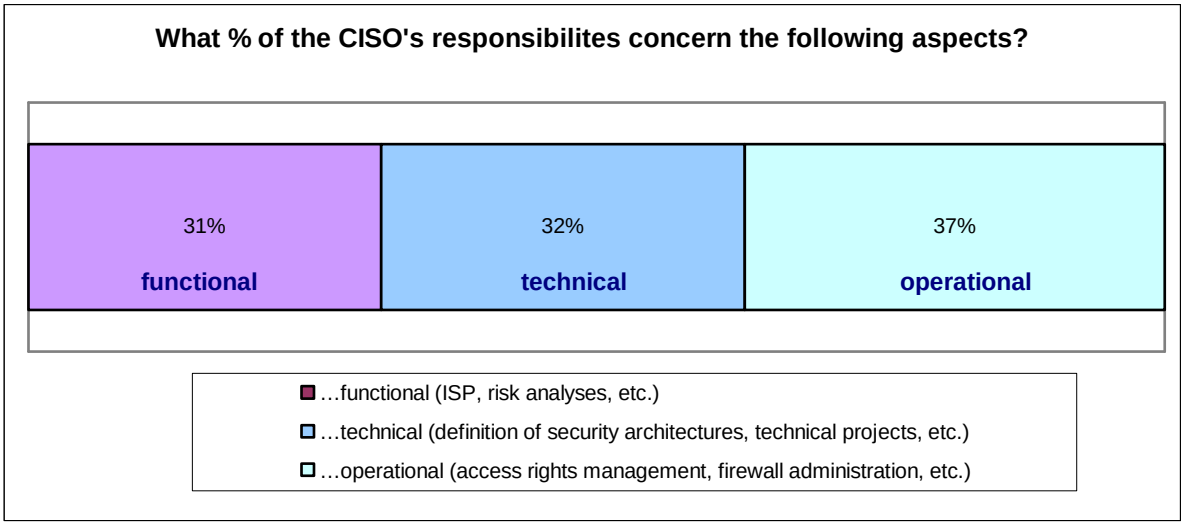

Figure 43: Distribution of the CISO's responsibilities

Full-time IS personnel is rare

Nearly half of local authorities do not have a full-time security team. For those that do, this team is rarely comprised of more than two members. Often, very few personnel are assigned to security on a full-time basis, which is also generally true for the size of the entire information technologies team.

Clause 7: Risk Assessment and Treatment

Local authorities less "risk-oriented" than companies

Forty-two percent of local authorities have performed an overall analysis, at least partial, of IS security risks, and 53% have developed and defined a plan of action based on this analysis.

Yet, only in 16% of these administrations does the risk analysis cover the entire scope of their Information System, revealing a lower maturity level than companies.

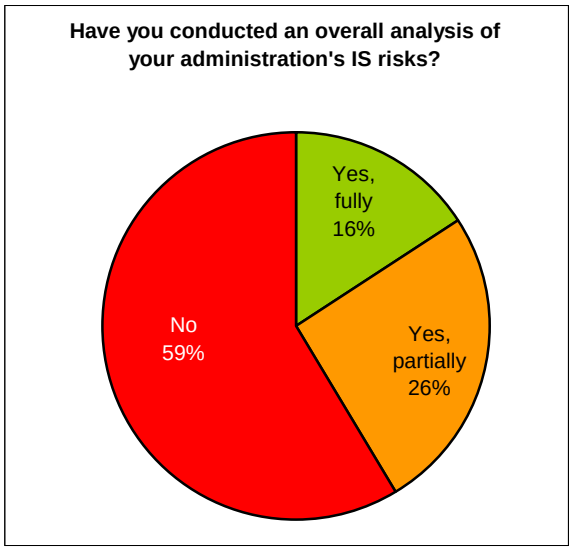

Figure 44: Risk analysis conducted in local authorities

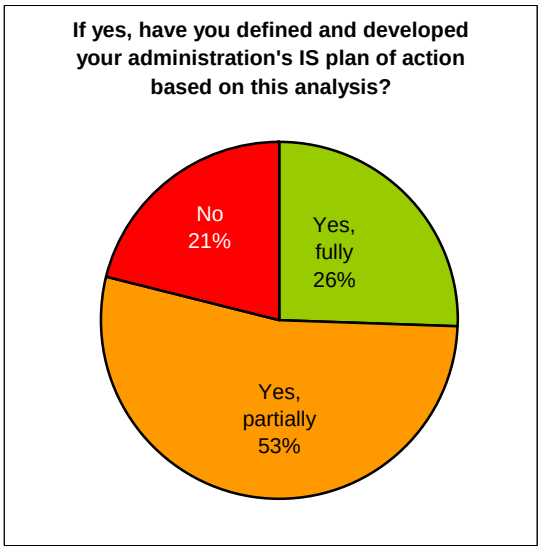

Figure 45: ISS improvement process in local authorities

Nonetheless, security is taken into account more frequently for projects: 75% of local authorities conduct project risk analyses, and 36% carry them out systematically.

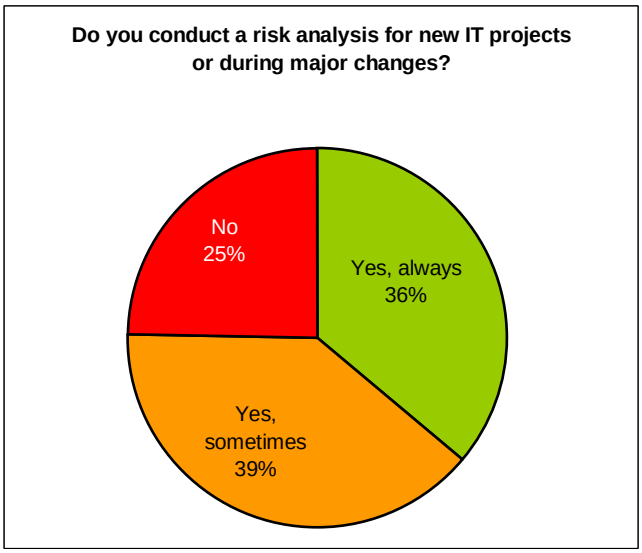

Figure 46: Consideration of risks in projects

The major players in identifying security risks are:

- the CISO (32%),
- the IT project leader (13%);
- the owner of an asset or the master builder (6%);
- other or undetermined in half of the cases.

“Risk” culture is very uncommon for department managers or clients. The CISO is most often cited as being the person in charge but only in one-third of cases. The figures tend to confirm that risk analysis is generally not a formal analysis founded on a dedicated method requiring a certain level of experience and specific skills.

Clause 8: Human Resources and Security

Compared to companies, security charters are less common in local authorities (41% have implemented such a document) and they are generally provided to personnel representatives. However, the gap is even more noticeable when it comes to provisions on disciplinary measures in charters. Only one-third of local authorities incorporate them into their rules and regulations as opposed to 56% of companies that have a charter.

Within local authorities, charters are more likely to be enacted to comply with regulations rather than to become an important element in the information security policy, even if the proportion of charters currently being developed is very significant (18%). Disassociating the principles set forth in the charter from the penalties for non-compliance with these principles raises doubts as to the effectiveness of security charters in local authorities.

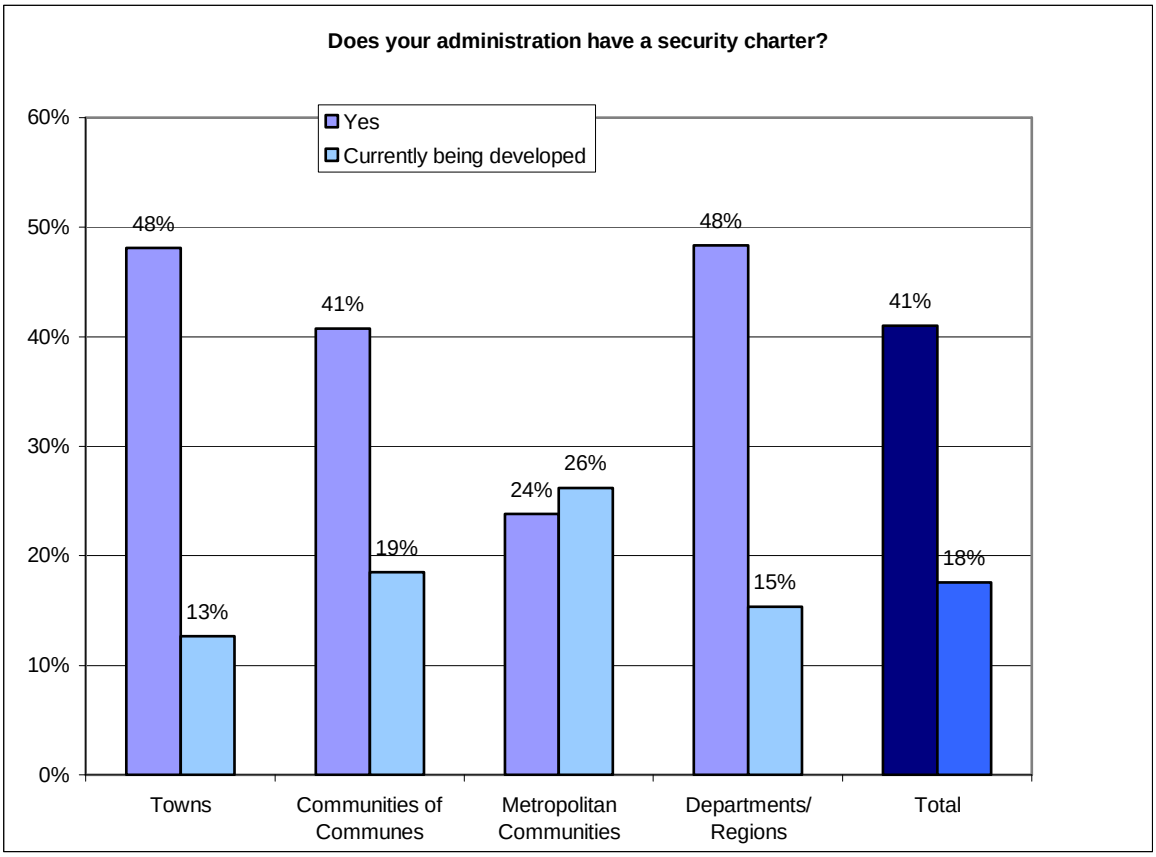

Figure 47: Existence of security charters in local authorities

Major progress remains to be made in the area of user awareness. Only 23% of local authorities have launched such actions and 10% are currently preparing them. As a consequence of these poor figures, it is no surprise that few personnel members follow the security policy and that CISOs cite the reluctance of users and services as a major obstacle in accomplishing their tasks!

As for resources, the list of preference follows the classic order: publications, awareness sessions and training. However, the impact of these actions is not measured in nearly nine out of ten administrations.

The information system user is the final barrier of protection from potential threats; therefore, not involving the user in the security policy would be an unfortunate loss of a precious partner.

Clause 10: Communications and Operations Management

Local authorities more cautious with new technologies than companies

The graph below summarizes the use of new technologies, and in particular mobile technologies, in local authorities.

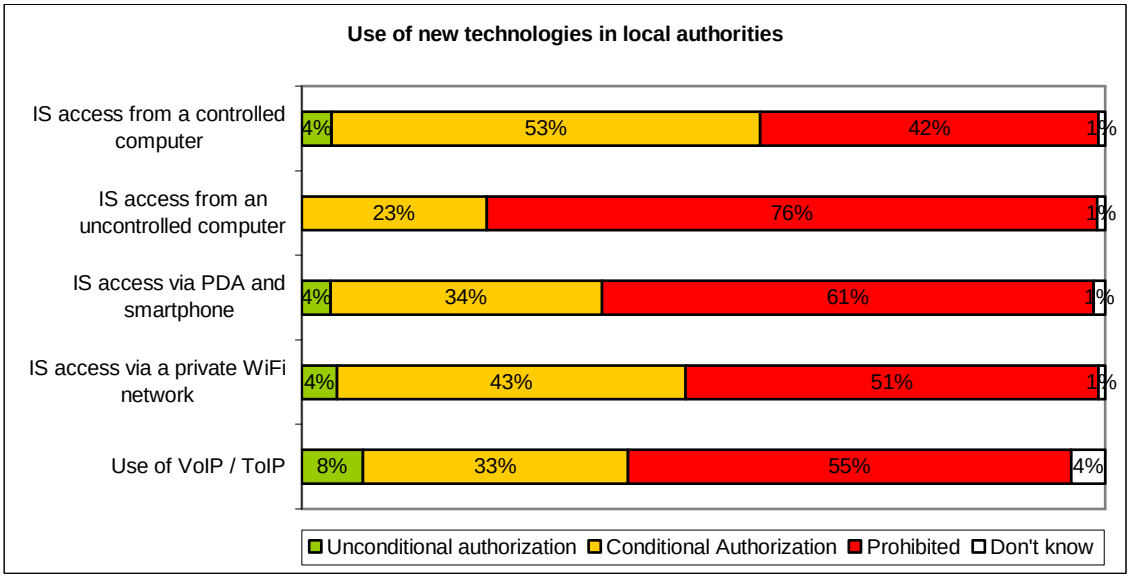

Figure 48: Mobility and IS access control in local authorities

Remote access using mobile equipment is less developed in local authorities than in companies (prohibited in 42% of cases compared to 13%, respectively) except in the case of regional and departmental councils for which, on the contrary, use is almost common practice (forbidden only in 11%). The same distinction between departmental/regional councils and other authorities appears when dealing with access from unidentified computers. The use of PDAs and smartphones is practically at the same level.

As for IP telephony, the breach between companies and authorities is greater particularly with regional and departmental councils, only 35% of which prohibit VoIP and ToIP, while figures for communities of communes and metropolitan communities nearly reach those of companies.

In summary, results show that new technologies are more often deployed in regional and departmental councils with a growing use of external mobility and ToIP devices that exceeds the average level of equipment observed for all companies and local authorities.

Protection of mobile access is generally addressed with similar types of technologies as companies but with some remarkable differences on the level of this use: strong authentication is more widespread in companies (56% in companies compared to 40%) as are personal firewalls (25% in companies compared to 16%). Inversely, local data encryption tools are more commonly used by local authorities (29% in compared to 14% in companies).

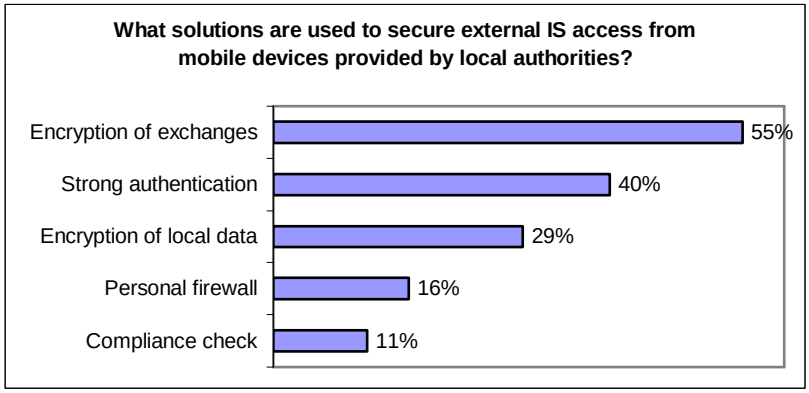

Figure 49: Technologies for securing mobile IS access on controlled equipment

An appropriate level of equipment for "basic" security technologies

Local authorities possess an appropriate level of equipment for the more classic security technologies such as antivirus, antispam and network firewalls. This level nevertheless trails behind that of companies with regards to tools such as personal firewalls, Intrusion Detection System (IDS) or Intrusion Protection System (IPS). Surprising data: one-third of administrations use an event log tool, or Security Information Management (SIM).

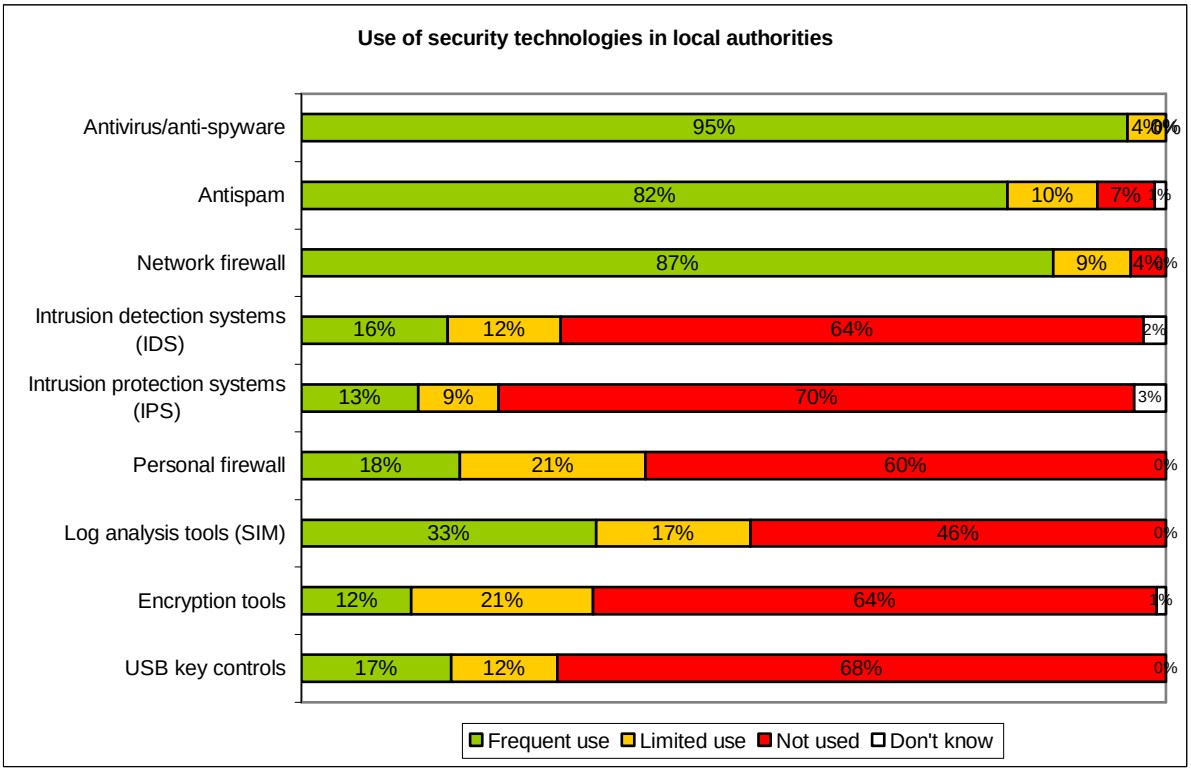

Figure 50: Security technologies used in local authorities

Clause 11: Access Control

Logical access control is considered from three aspects:

- strong authentication methods that may be used;
- means of managing and implementing user access rights;
- centralized access control and single authentication (Single Sign-On).

To facilitate the comparison with the results of the 2006 survey where only towns were surveyed, two graphs are provided covering all territorial authorities, then only the town halls.

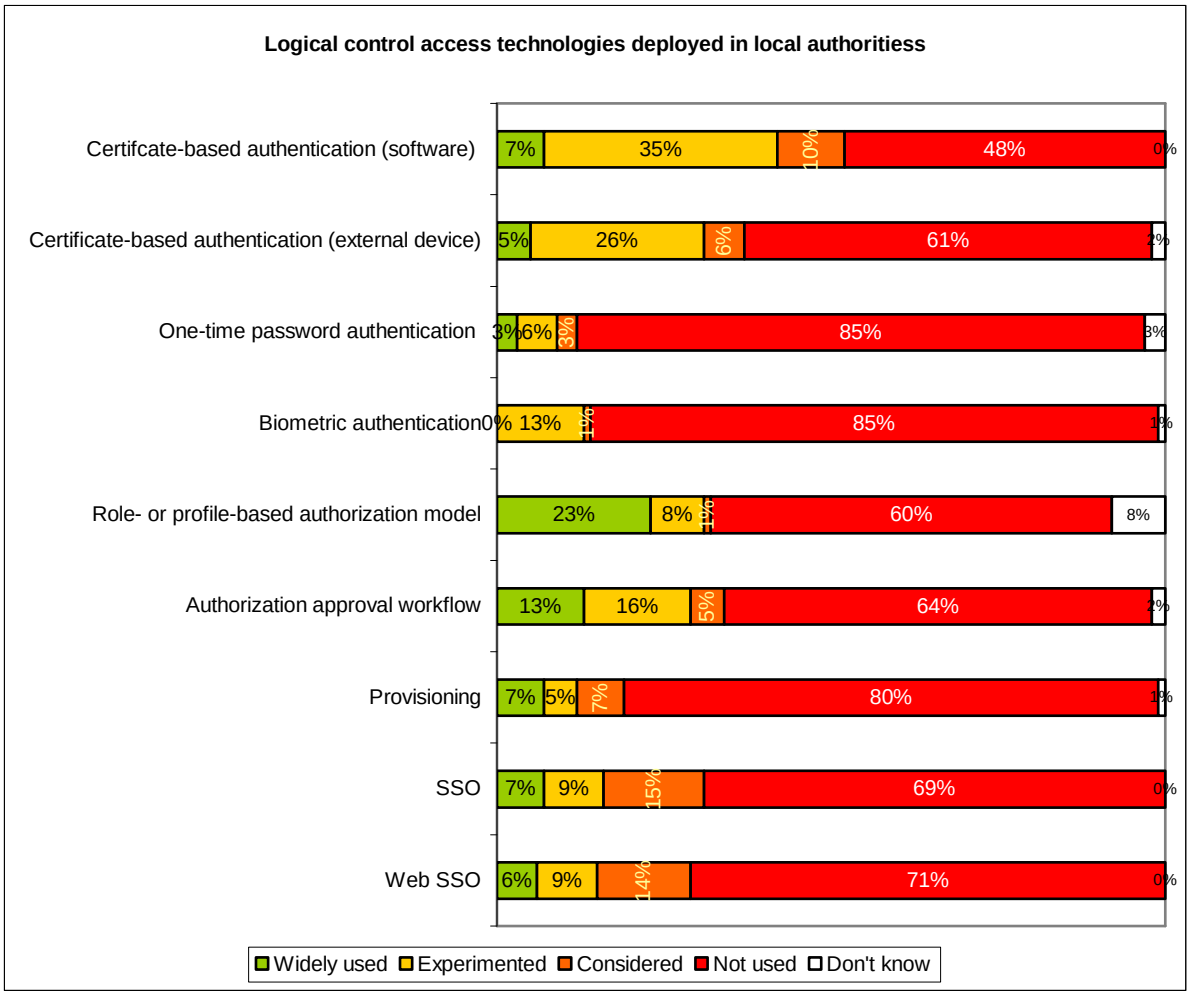

Figure 51: Logical access control technologies deployed in local authorities

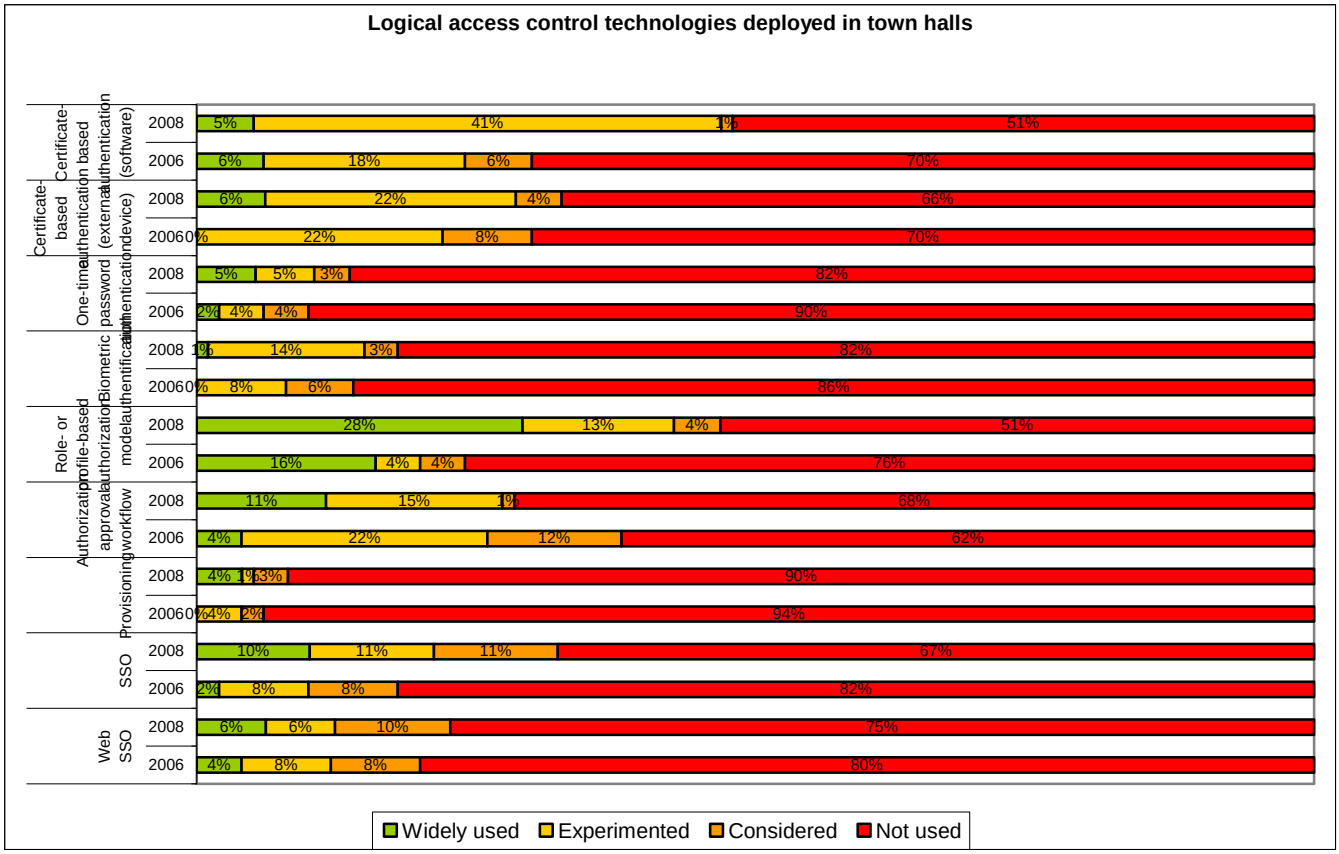

Figure 52: Logical access control technologies deployed in town halls, 2008 and 2006

Certificate-based strong authentication: renewed interest in town halls

Certificate-based strong authentication is widely used by local authorities, most often in software form but sometimes on material media as well. Biometrics is beginning to stir interest, while one-time password devices are rarely chosen as an option.

Contrary to companies, a great difference from 2006 can be seen for town halls. Usage patterns concerning material certificates have not fundamentally changed, but other means of strong authentication have visibly progressed: one out of four town halls has recently converted to electronic certificates in software form. Interest in biometrics has also risen slightly, at least for experimentation or partial deployment.

Lastly, the level of disparity is noticeably high depending on the type of authority. Town halls seem to prefer electronic certificates for example, while regions and departments rely much more frequently on other technologies.

Authorization management: progress in town halls

Whereas only four out of ten administrations have implemented a rights management system based on role or business profile, or at least wish to do so, it is nevertheless evident that this model is gaining momentum since nearly one additional town hall out of four has made this chose in the past two years.

Implementing a Role-Based Access Control (RBAC) model logically supports an authorization approval workflow. The number of town halls that have started or generalized such a measure has increased since 2006 by the same proportions as those that have chosen a rights management system based on business profile. However, provisioning systems which did not exist in 2006, have not generated any more interest today.

Centralized access control: advantageous for regions and departments

The percentage of town halls that have used or experimented with Web and SSO control systems has doubled in proportion since 2006 and one out of ten town halls plan to deploy one of these systems in 2008.

Once again, regions and departments have taken a firm lead over the other authorities: two-thirds have already taken the SSO leap, and half have done so for SSO Web. On the other hand, three out of four metropolitan communities and four out of five communities of communes are more hesitant to adopt these technologies and have no plans of acquiring either.

Clause 12: Acquisition, Development and Maintenance

Surveillance and management of vulnerabilities: a stabilizing situation

The figures are similar to those concerning companies: 61% of local authorities conduct some sort of surveillance on vulnerabilities.

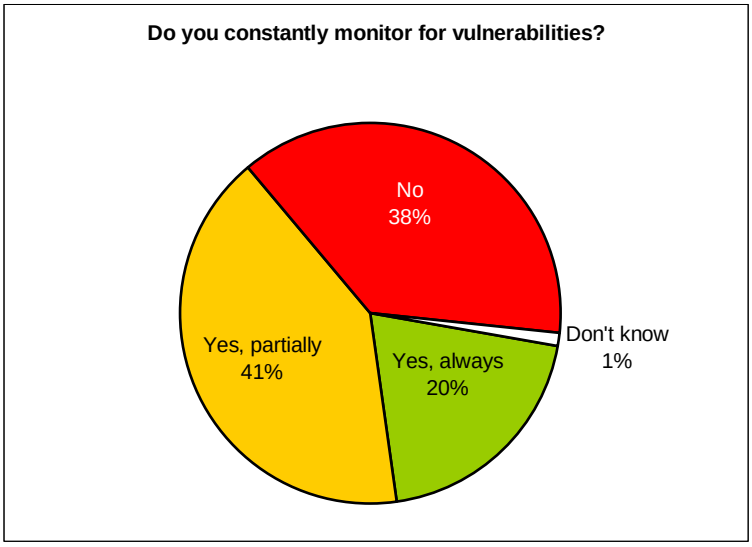

Figure 53: Constant surveillance of vulnerabilities in local authorities

Maintenance and deployment of security patches

Over half of the local authorities have formalized patch deployment procedures.

Among those that have implemented procedures, 84% deploy their “workstation” patches in less than one day which demonstrates that the time frame in local authorities is rather similar to that of companies. Here again, it would be hard to ignore the fact at even if the practice of deploying patches is now common enough for workstations, it remains under used for servers.

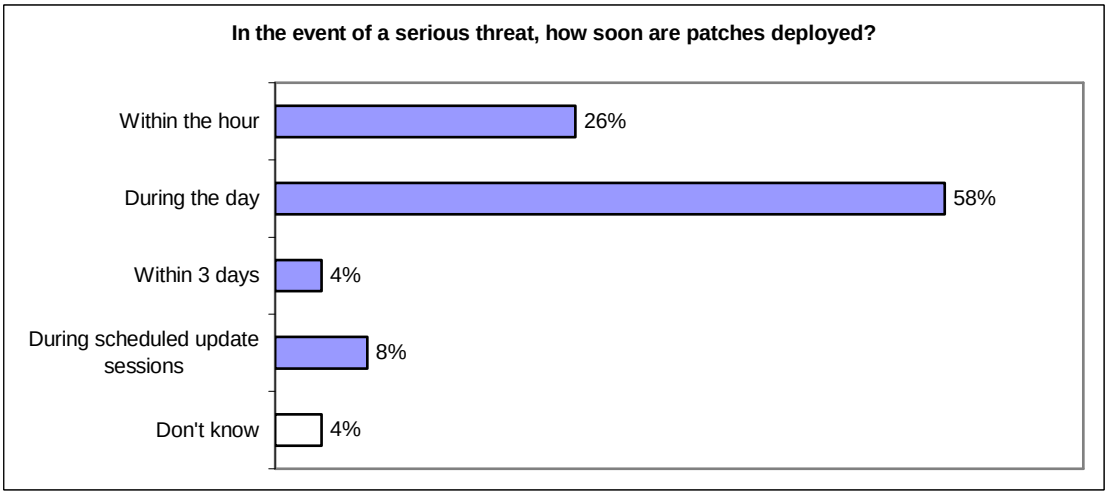

Figure 54: Time frame for patch deployment in local authorities

Clause 13: Incident Management - Disasters

A nascent consideration of security incidents

In local authorities, like in companies, incident management is still poorly organized: a little more than a quarter surveyed have a dedicated unit (6%) or one that participates (20%) in managing these incidents.

As a result, only 5% of local authorities have filed complaints for security incidents whereas 38% of them have declared being the victim of computer equipment theft or disappearance. What is even more disconcerting is that only 7% of local authorities stated that they conduct a financial evaluation of the incidents they suffer.

Responses vary greatly depending on the type of authority and 19% of regions and departments reported having filed complaints for security incidents over the course of the year.

A conflicting view of incidents

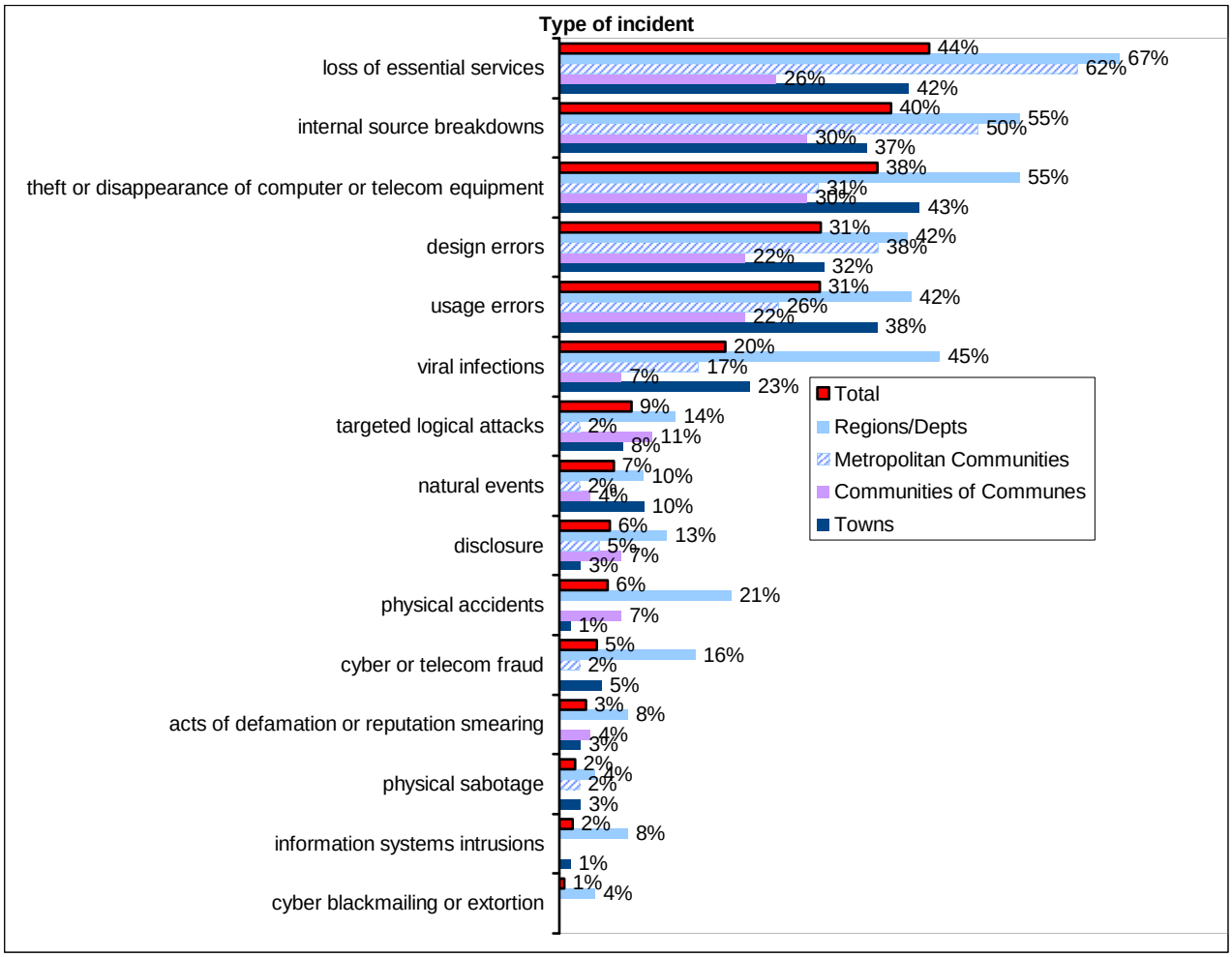

Figure 55: Types of security incidents in local authorities

Theft or disappearance of computer equipment is always a serious cause of disasters. Likewise, information systems intrusions (1%-8%) and other frauds (2%-16%) reach non-negligible levels.

One out of five local authorities hit by viruses

Of the 20% that have been affected by a viral infection, 13% came from an internal source and 24% were of an unknown source.

CISOs themselves confess that the impact of these infections is non-negligible one out of five times.

Local authorities are victims of viral infections eleven times on average; some have been hit more than a hundred times...

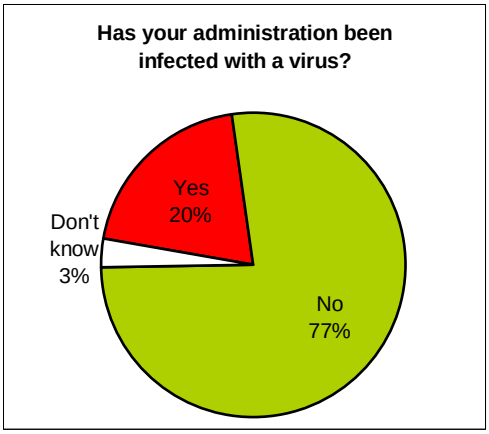

Figure 56: Rate of viral infections in local authorities

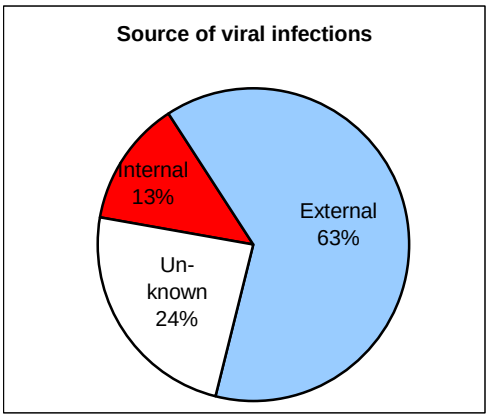

Figure 57: Source of viral infections in local authorities

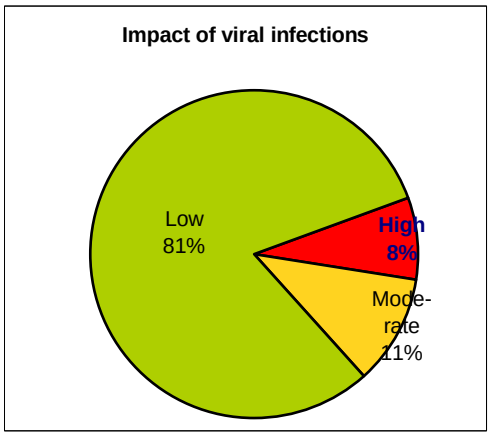

Figure 58: Impact of viral infections on local authorities

60% of local authorities affected…

Although local authorities do not have incident collection and treatment units, more than one out of two CISOs estimate that they suffered disasters last year. Seven percent of them have even counted over 50 and some more than…400!

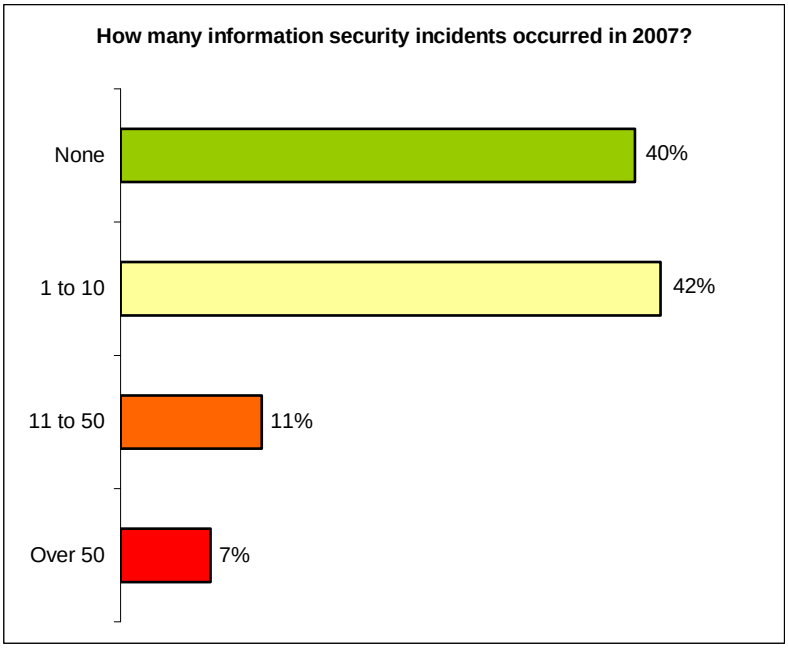

Figure 59: Number of security incidents inventoried in 2007 by local authorities

… for a less-than flattering toll

In conclusion, while 60% of local authorities confess to having suffered incidents, 74% do not include collection and treatment units in their organization, 95% never file complaints and 93% do not even evaluate the financial impact of these incidents.

Clause 14: Business Continuity Management

Slight improvement but much progress remains to be made

Whereas 61% of companies have completely or partially formalized a continuity management process, only 38% of local authorities have done so. In other words, this means that nearly two-thirds of them still do not have any recovery solution following a major incident.

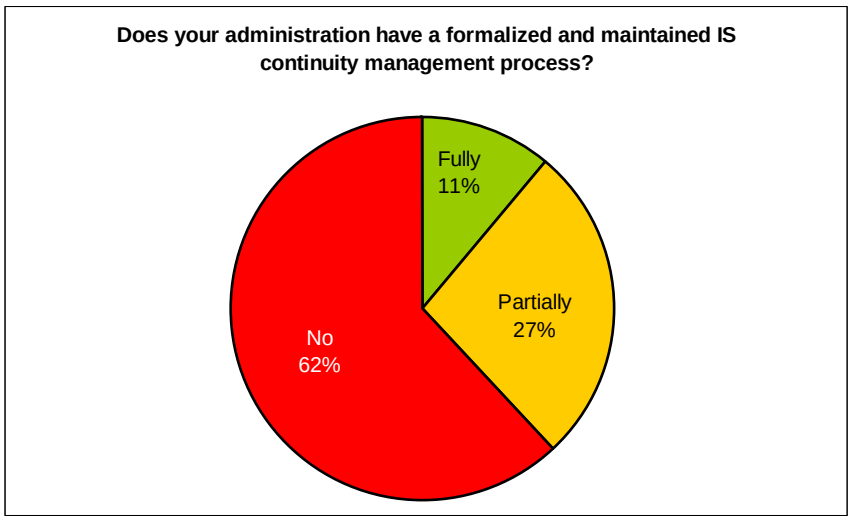

Figure 60: Existence of a formalized process for IS continuity management

The report is poor but is attenuated by a clear trend towards improvement that is particularly noticeable in town halls. During our 2006 survey, 72% of town halls in cities with over 30,000 inhabitants did not have a BCP, but today this figure has dropped to 61%.

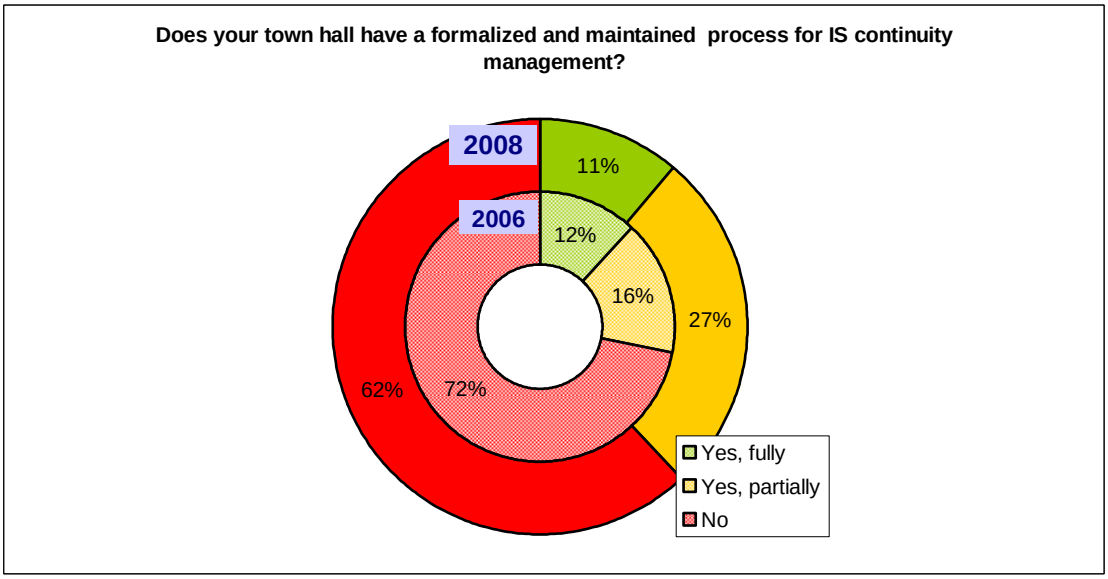

Figure 61: BCP in town halls with over 30,000 inhabitants, 2008 and 2006

We can hope that these improvements concern the entirety of local authorities and that this positive trend will continue and accelerate. Once again, the work to raise awareness is not over for professional organizations and associations such as CLUSIF.

Maintenance: significant discrepancy with companies

Fifty-six percent of local authorities with a business continuity plan conduct tests and updates at least once a year. Only 11% of them conduct several tests each year, which is a very low rate compared to the figures found for companies (38%).

Yet, a continuity solution that is not tested regularly presents serious risks of not being operational when they are finally set in motion following a disaster…

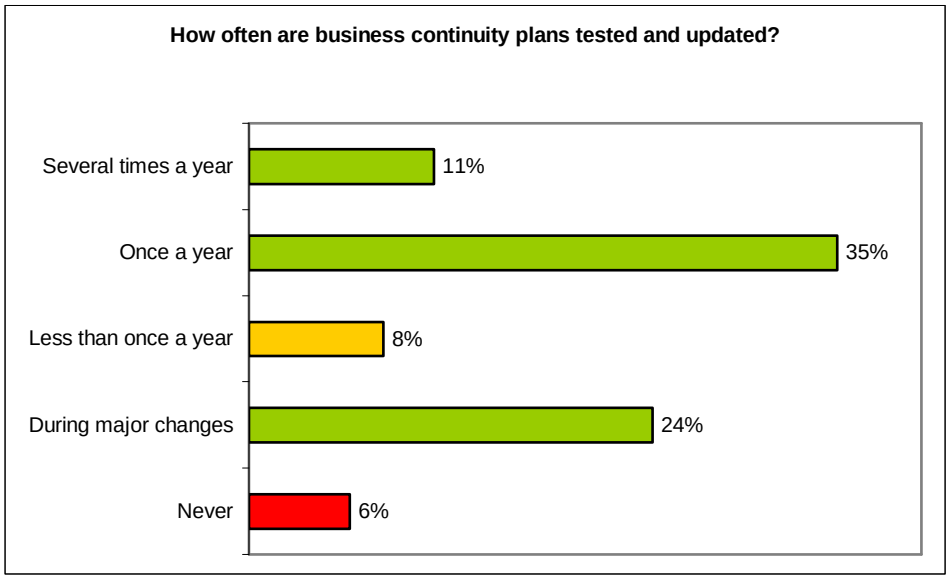

Figure 62: Testing frequency of business continuity plans

We can also see that local authorities wait and/or take advantage of major changes to test continuity plans (24%) while only 10% of companies do so under these circumstances.

Disaster recovery: popular backup methods

Responses given for recovery solutions also differ slightly between the private and public sectors. More than nine out of ten local authorities use traditional backup solutions as opposed to 29% in companies.

It should be noted that trends and results are nearly identical in proportion when comparing towns, communities of communes, metropolitan communes or regions.

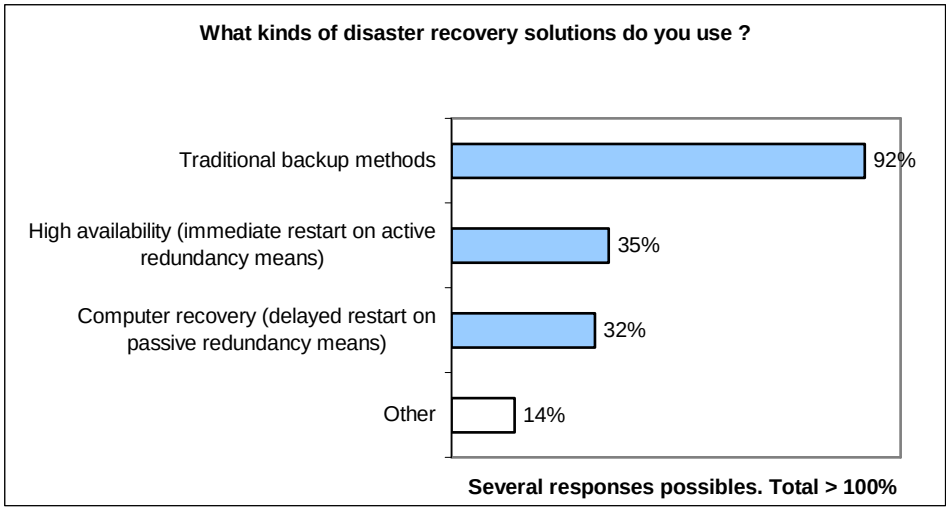

Figure 63: Disaster recovery solutions

It clearly appears that local authorities still lack the means. Indeed, the great majority of them (92%) still only use classic backup methods compared to 79% of companies.

The proven high availability/computer recovery technologies are much more present in companies (53%/42%) than in local authorities (35%/32%).

Clause 15: Compliance

This clause addresses compliance-related issues, focusing on three subjects:

- compliance with obligations of the French **Act on Data Processing, Data Files and Individual Liberties**;
- security level control through **audits**;
- monitoring of security levels using security **dashboards**.

1/ Obligations pursuant to the Data Processing Act

Local authorities ahead of companies

Although the situation is less than perfect, local authorities do fare slightly better than companies with respect to the Data Processing, Data Files and Individual Liberties Act (69% and 64% in complete compliance, respectively). In town halls however, the situation has worsened (69% in complete compliance compared to 84% in 2006).

Furthermore, 30% of local authorities reported having appointed a DPO compared to 25% of companies. Once again, town hall results have slipped since 2006 but we can safely assume that these results are closer to the reality, as the notion of the Data Protection Officer has been much better defined in the past two years.

2/ Security audits

An underdeveloped practice

Over 40% of local authorities conduct an audit at least once a year, whereas 56% do not conduct any.

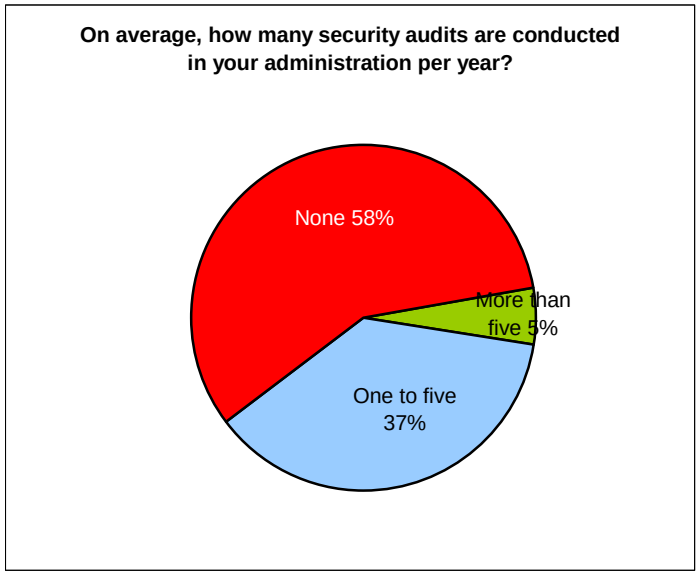

Figure 64: Number of security audits conducted a year in local authorities

The 41% figure has clearly declined compared to 2006 (using a constant scope that only includes town halls, 42% compared to 56% two years ago).

The audits conducted more often deal with technical aspects (verifications of technical configuration, intrusion tests) rather than organizational aspects.

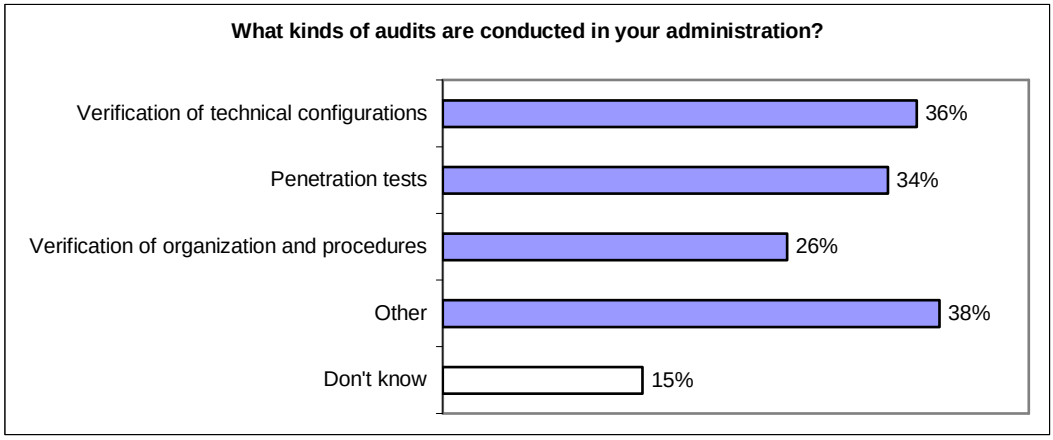

Figure 65: Types of security audits

One out of three times, these audits are performed pursuant to internal policy or contractual or regulatory obligations. Those conducted by external auditors are visibly fewer in number than in companies.

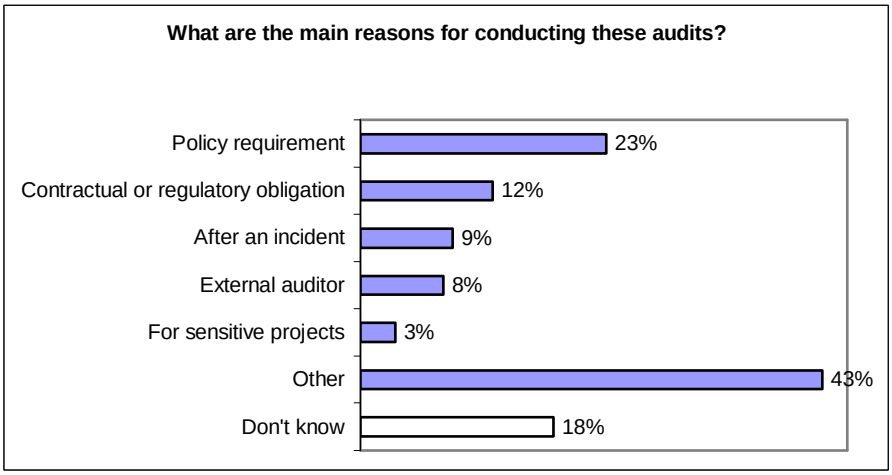

Figure 66: Reasons for security audits

3/ Security dashboards

The need for dashboards in local authorities is not always present, which may explain their marginal use by only 10% of local authorities. The indicators included in these dashboards refer mostly to technical aspects.

Internet Users

- Part 1: Profile of Internet Users
- Part 2: Internet Uses
- Part 3: Perception of Threats and Risks
- Part 4: Security Means and Behavior
- Conclusion

Internet Users

One of CLUSIF's objectives for this study was to characterize the population of French Internet uses, understand their Internet use and above all evaluate their perception of computer threats and risks by questioning them on their security practices.

Part 1: Profile of Internet Users

Constitution of the sample

For this population sample, CLUSIF solicited Harris Interactive, an institute specialized in public opinion surveys, which conducted the entire study by Internet. The sample was comprised of 1139 people extracted from a large panel of 700,000, guaranteeing the inclusion of all Internet user profiles. Using a precise description as a basis also enabled us to constitute a structured sample that accurately represented the reality of French Internet users in terms of SPC[9], age, sex, region, type of metropolitan area, etc. At the final scoring, minor adjustments were made in order for the responses to be directly transposable to the reality of the French population.

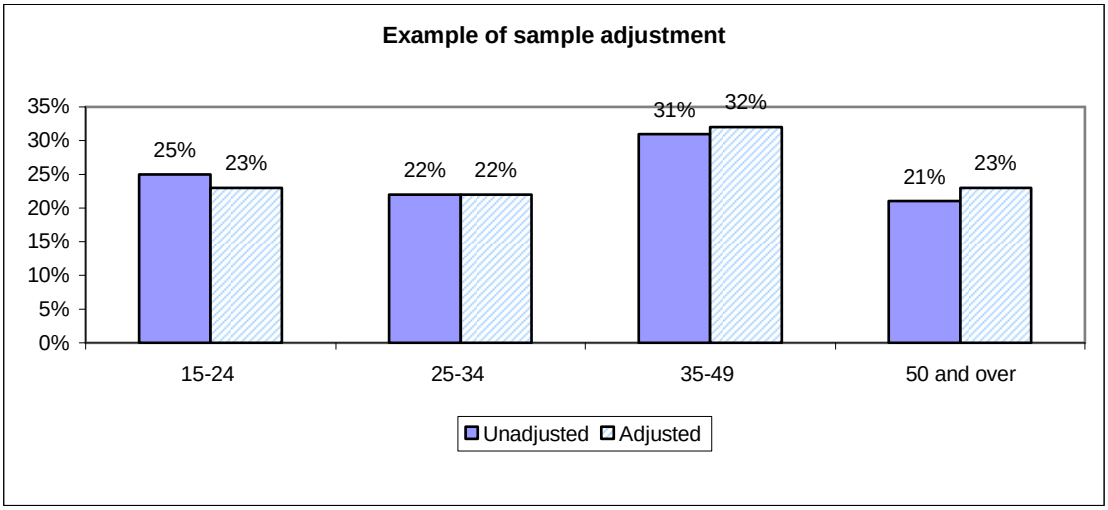

Figure 67: Example of sample adjustment

As shown above, the CLUSIF sample included 25% of 15-24 year olds although the average national is 23%. To be more consistent with the real figures, the survey responses underwent a post-processing procedure to reweight each age bracket more fairly.

[9] See glossary.

One or two computers per household

Only those households equipped with Internet access were surveyed. The following characteristics emerged after inventory of family computer equipment.

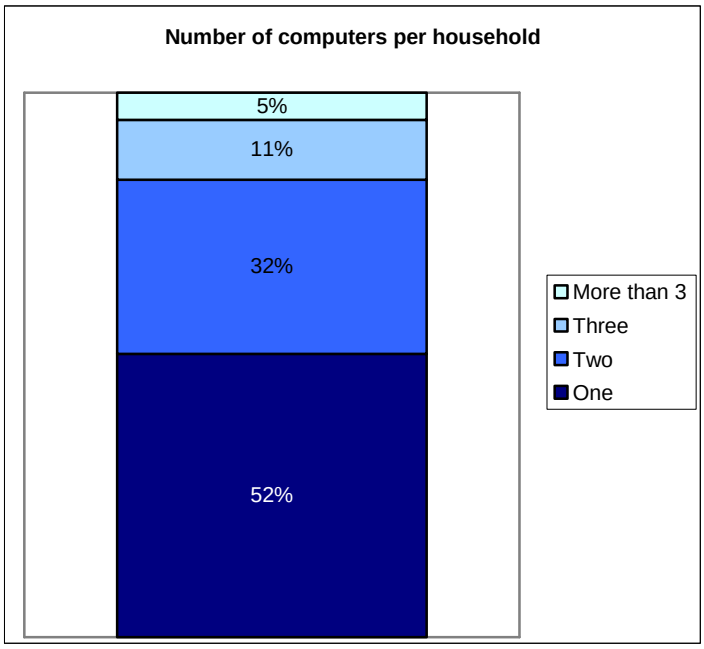

Figure 68: Number of computers per household

Fifty-two percent of households have only one computer (national average):

- 48% in the SPC+[10] category
- 57% in the SPC- category
- 58% in the 25-34 age bracket
- 54% in the over 50 age bracket

Sixteen percent of households have three or more computers (national average).

- 20% in the SPC+ category
- 11% in the SPC- category
- 20% in the 35-49 age bracket

There are relatively few disparities in the rate of equipment according to geographic area and socioprofessional categories.

Rather recent computing equipment

Nearly 60% of households had purchased these computers in the past three years. Computing equipment is thus rather recent given the maturity of technologies available on personal computers.

Among the households with two or more computers, 80% had at least two computers connected to the Internet.

Prevalence of WiFi

Fifty-one percent of households (national average) were equipped with WiFi, and the results revealed the following peaks:

- 59% of households in the Paris metropolitan area;
- 60% of households with 15-24 year old inhabitants;
- 61% of SPC+ households where the relay to a television set can be decisive.

The prevalent use of WiFi can be attributed the very rapid proliferation of “triple play boxes” (Internet-TV-telephone services) and the newness of the equipment (as detailed in the preceding paragraph) such as laptops, all of which have integrated WiFi connections.

The French do what is necessary to fulfill their desires and new wireless computers allow them to surf when and where they want.

[10] See glossary.

The personal computer is a family computer…

It is not surprising that in the home, the computer is shared by the different members of the family in three-quarters of cases. Only 26% of computers are only used by a single user.

On average, the family computer is used by **2.4 users**.

… but used professionally 33% of the time

According to the responses, private individuals use their family computer for their personal affairs in 66% of cases but 33% have used it for both professional and personal matters.

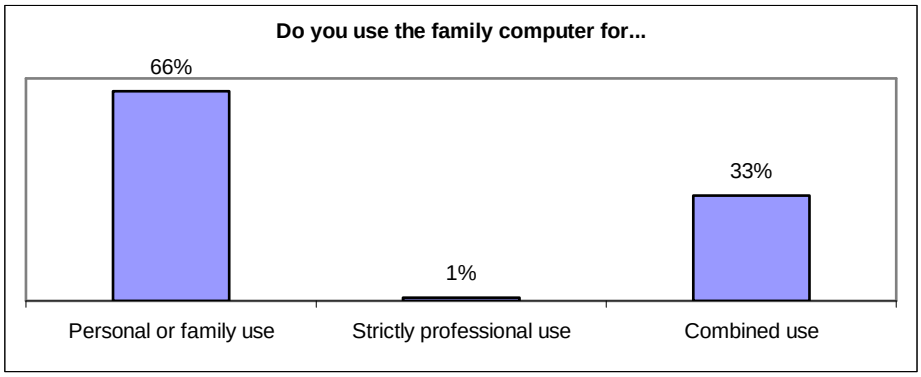

Figure 69: Types of use of the family computer

Combined use is common for the following occupations:

- artisans, store owners, entrepreneurs with <10 employees (80%);
- freelance and similar (66%);
- high officials in public services, intellectual and artistic occupations (60%);
- students, apprentices (59%).

40% of company executives work from home

Of the different socioprofessional categories, CLUSIF found that the category of company executives deserved special attention. Forty percent of executives replied that they worked from their personal computer and therefore handled confidential or sensitive company data in a cyber environment completely uncontrolled by the CISO. In acknowledging this "mixed" practice, information security systems managers should consider the potential risks and the relevant protection it would require. It is also essential to decide whether prohibiting "mixed" uses would be realistic or if would be more advantageous for companies to simply tolerate, or even encourage them, while following up with awareness actions and appropriate protection tools.

The computer, a favorite for photos

The family computer is used for various and important reasons, and particularly for storing and handling:

- photos or personal videos in 97% of cases;
- personal documents (mail, accounting, etc.) in 88% of cases; and
- professional or academic documents in 49% of cases (with a peak of 72% in the 15-24 age bracket and a low rate of 31% in the 50+ age bracket, likely less familiar with computer tools).

Part 2: Internet Uses

80% of users are permanently connected to the Internet

Of the survey sample, 80% replied that they are connected to the Internet all the time or most of the time, which means as soon as they turn on the computer.

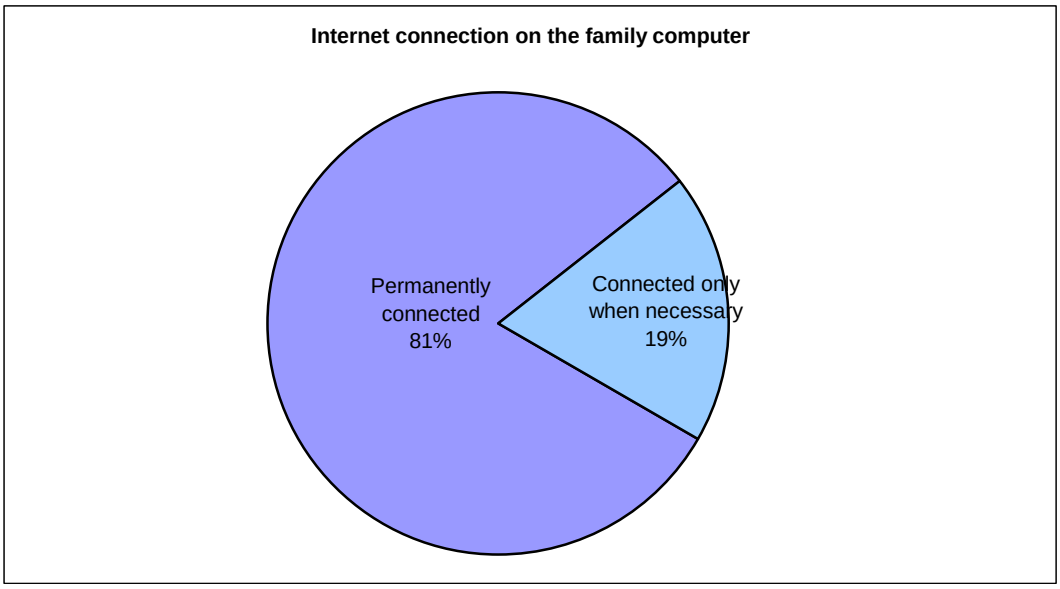

Figure 70: Internet connection time

With the generalization of broadband access, Internet users may not realize that they are increasing their exposition time to risks.

Different ISPs according to geographical location

Three Internet service providers (ISP) dominate the market in the following order: Wanadoo/Orange (35%), Neuf (26%) and Free (24%), with a very different distribution according to geographical location. Wanadoo/Orange serves 53% of inhabitants in rural areas but only 18% in the Ile-de-France region. The situation is inversed for Free, which is the chosen ISP for 11% of rural inhabitants and 38% of Parisians.

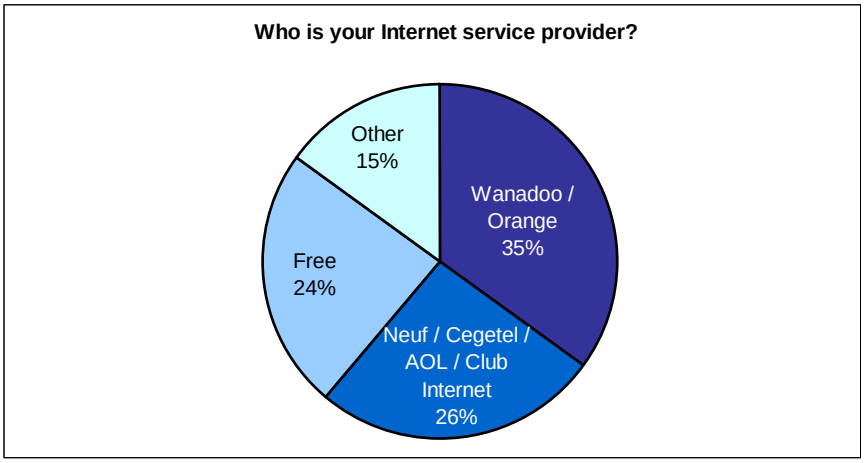

Figure 71: Market share of ISPs

Furthermore, cable connections today represent a negligible market share except in the Paris metropolitan area where it reaches just 10% of households connected.

Internet uses are numerous and varied

Nearly all private individuals responded that they use the Internet to surf and for e-mail (> 97%).

Half of Internet users go online “often” and “very often” for the following reasons:

- to chat through instant messaging: 55% (19% never do);
- to carry out bank transactions: 51% (23% never do);
- to make online purchases: 52% (10% never do);
- for administrative procedures: 49% (ex.: filing taxes, enrolling children at the school cafeteria, etc.).

Using the Internet for the following is less frequent (35% to 15% in decreasing order):

- auction sites or sales transactions between private individuals;
- online games;
- Internet telephony;
- communication with a webcam;
- blogs.

Less than 10% of Internet users use the Internet to:

- communicate on social networks;
- download software;
- participate in dating and friendship networks.

Lastly, and even if personal computers serve both professional and personal purposes for one out of three Internet users, this professional use rarely entails connecting to the company network from the home:

- only 10% of Internet users who work (thus excluding employment seekers) replied that they connect often or very often to their company network;
- 10% connect to it sometimes;
- 80% never connect to it.

Legal downloads, illegal downloads

If the average person were asked about their illegal activities, they would most likely respond "under declaration". CLUSIF was nevertheless tempted to carry out the experiment and the results obtained are… difficult to comment on and should be taken with precaution.

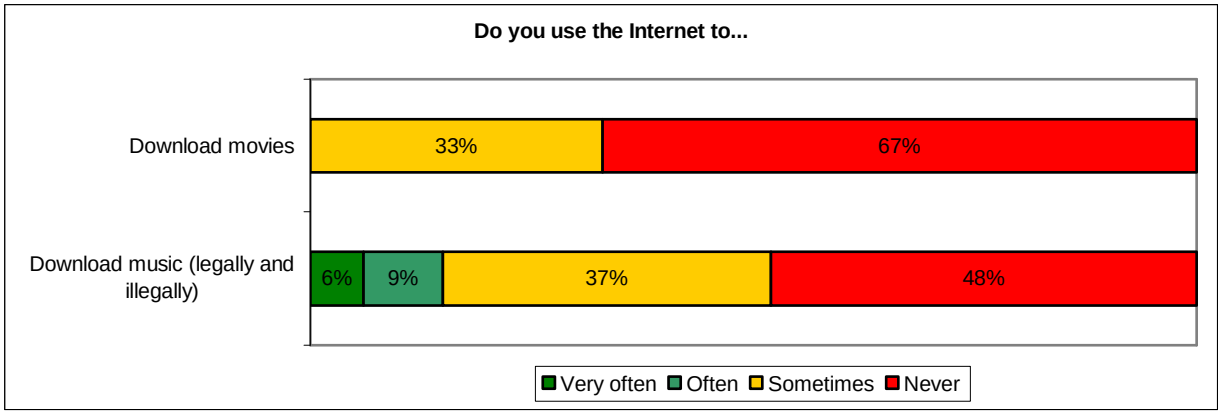

Figure 72: Downloading habits for music and movies

One out of four Internet users pays online without a second thought

For those who make online purchases (approximately 92% of Internet users):

- 24% do so without requiring any special conditions;
- 76% check one or more of these conditions before paying:
  - the site "seems" secured (padlock, https:, etc.);
  - the site is known (reputed brand or name);
  - the use of specific techniques (PayPal™, e-credit card, etc.).

Internet users thus appear attentive when it comes to protecting their personal financial interests but are they really well-informed? The question that follows seems to prove the contrary! In fact, 86% of those surveyed ignore that their cyber vendor (or its banking intermediary) is entitled to keep credit card numbers in their information system. Do the 14% of the better-informed Internet users know of the immense business of card number sales? We do not have the answer but the majority of "those who know" (60%) deplore that their precious number is stored.

Part 3: Perception of Threats and Risks

Few security problems experienced by Internet users

The security problems that Internet users report having encountered in the previous eighteen months are as follows:

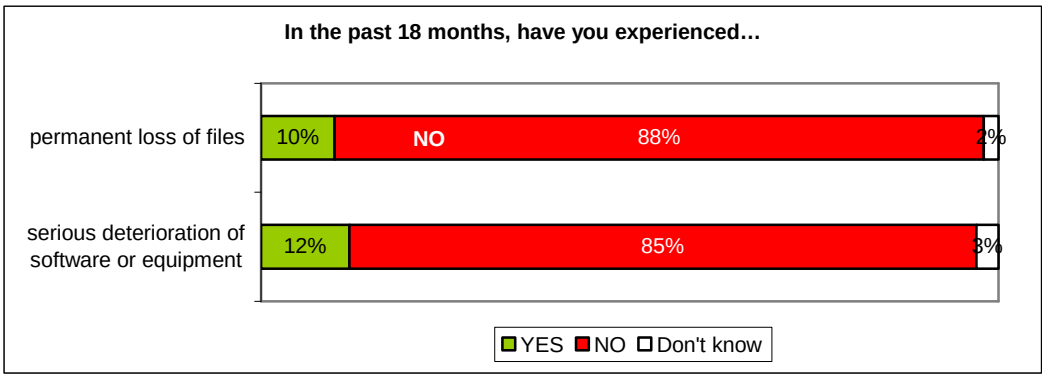

Figure 73: Security incidents encountered by Internet users in the past 18 months

Depending on the nature of the problem, 10% to 12% of the population surveyed responded that they have had security problems during the past eighteen months.

Awareness of security also comes from experience!

A significant fraction of Internet users expressed strong concern about threats and risks inherent in Internet use:

- 13% of Internet users reported being very worried about the protection of their privacy;
- 25% have serious fears about their files or equipment.

These levels of concern are doubled when files had been lost or equipment damaged during the previous eighteen months.

Yet, no specific opinion emerged as to future trends in the evolution of threats and risks:

- 20% believe that risks are declining or heavily declining;
- 21% believe that they are increasing, possibly very strongly.

Privacy: Internet users are cautious but poorly organized

Sixty percent of Internet users feel that the Internet could compromise their privacy “a little” or “a lot”.

Most are fully aware of the potential troubles that may arise as a consequence of supplying personal information over the Internet:

- 19% of them never fill out data collection forms;
- 75% only do so if there are criteria deemed objective (in their opinion) for trustworthiness on the site requesting the information;
- 6% always respond unconditionally.

The least wary are young users (in the 15-24 age bracket) who are much more willing to respond to questionnaires. Awareness programs[11] launched by associations or public powers lay witness to this fact.

Even if Internet users are generally mistrusting of how the information they supply is used, they are nonetheless less preoccupied with privacy issues linked to:

- unsecured WiFi: 42% do not see any risks;
- theft of data storage equipment (computer or flash drive): for 56%, the potential risks are inexistent or not very significant.

Yet, less than one out of ten private individuals only rarely uses local data encryption.

For the present, we can only take note of the major incongruence between the intentions and the practices of Internet users to protect their personal data or privacy. It will be up to associations, public powers and the media to increase awareness on all of the possible risks.

[11]See the technical sheet “Protection of Children” on the “Information Systems Security Portal” Website of the Secretariat-General of National Defense, Central Information Systems Security Division (SGDN/DCSSI) at http://www.securite-informatique.gouv.fr/gp_article201.html.

Viral threats are still the number one concern

The graph below presents the threats that have been identified or are perceived by Internet users. The dominant fears still entail attacks by viral infections or by spyware.

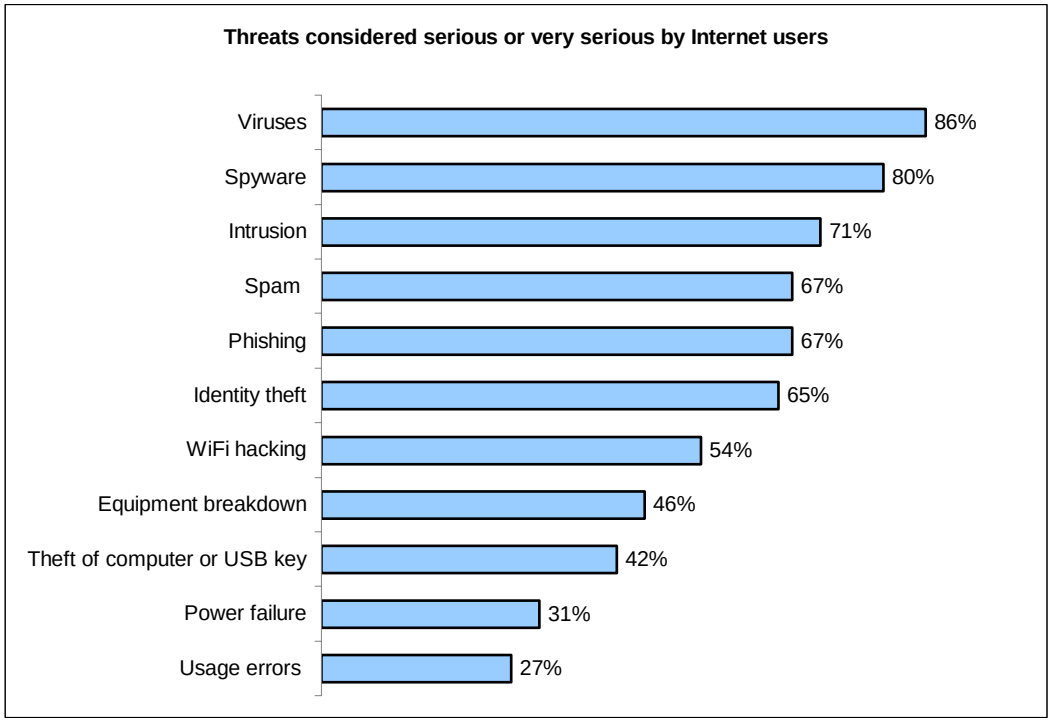

Figure 74: Threats by order of importance for Internet users

This graph synthesizes the threats considered as “very serious” and “serious” on the family computer. On the contrary, the following threats are considered to represent “zero risk”:

- theft of the computer or a USB key (20%);
- usage errors (15%);
- power failure (15%);
- WiFi hacking (11%).

Men relativize more than women

Compared to men, women have a much greater tendency to qualify the aforementioned risks as “very important”, with the sole exception of theft.

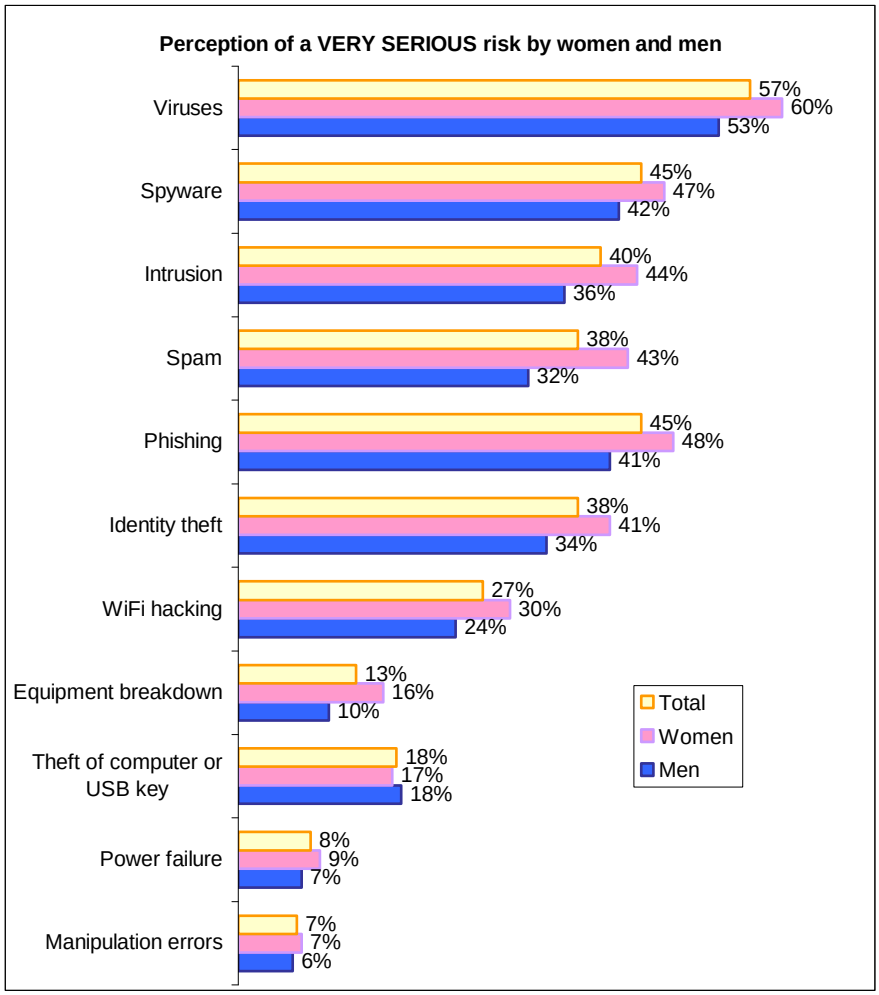

Figure 75: Differences in risk perception by gender

Major gaps in understanding risk situations

Similarly, when questioned on behavior and risk situations, nearly all Internet users logically cited the absence of protection against viral threats.

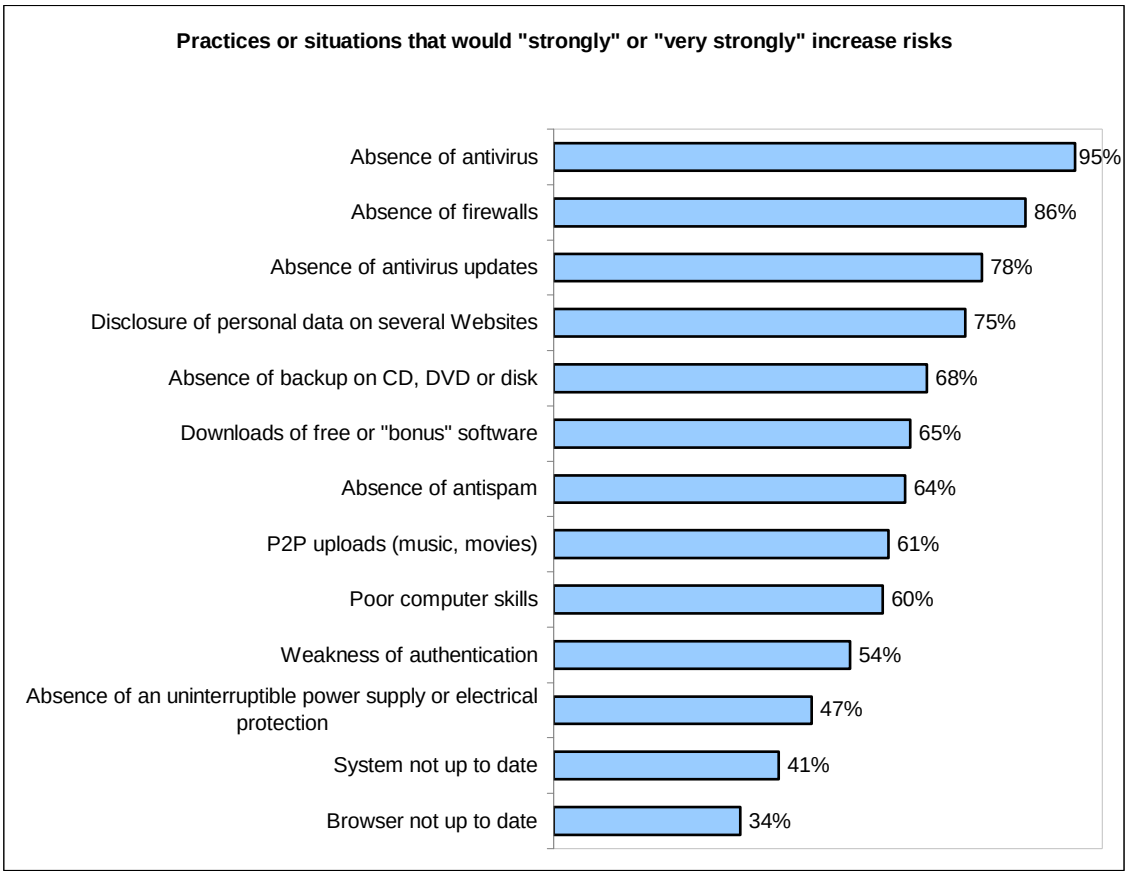

Figure 76: Practices and situations considered risky by Internet users

It is essential to educate and raise awareness of good practices among users, a majority of whom falsely believe that risks do not increase if systems and browsers are not updated. An operating system, even equipped with an antivirus, will in most cases be vulnerable to external attacks if not regularly updated.

Part 4: Security Means and Behavior

Not surprisingly, Internet users rely on "traditional" protection methods

Given the risks perceived by Internet users, it is not surprising that they employ "traditional" protection methods according to the level of threat they feel they pose.

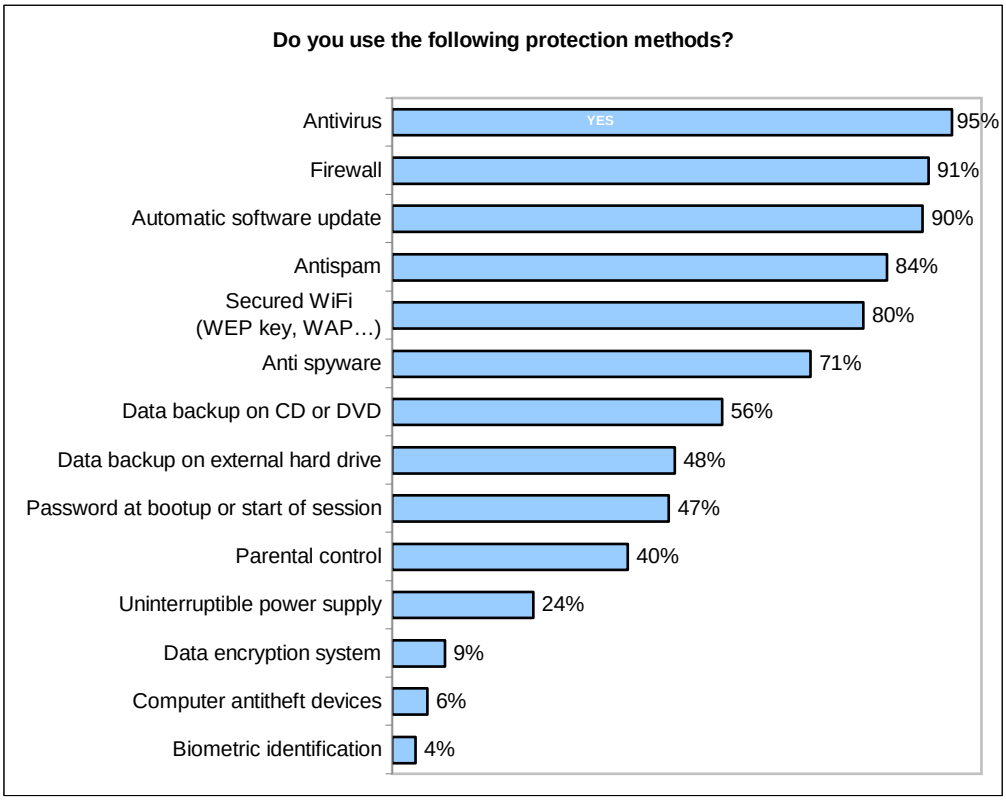

Figure 77: Protection methods employed by Internet users

Numerous Internet users have installed Internet threat protection tools on their computers, especially antiviruses and firewalls. Moreover:

- 90% use automatic updates for sensitive software as well as for the system and browser. This is nevertheless reassuring even it if it offset by the fact that 54% of Internet users feel that risks are does not at all (17%) or hardly (37%) increased with an outdated operating system and 60% think the same of outdated Internet browsers;
- 84% think they have an antispam;
- 80% state that their WiFi connection is secured;
- 71% use an anti spyware.

Cost of protection and automatic updates

In the hierarchy of protection methods, the survey shows a certain correlation between the rate of equipment and two factors: free access and automation.

The most frequently used protection methods according to our survey are very often free, included without extra costs in the operating system delivered with the computer or easily downloadable from software companies or specialized sites. Similarly, automatic updates, performed by 90% of Internet users surveyed (operating systems, antivirus, browsers, etc.) do not, by definition, require any particular effort from the Internet user.

On the contrary, certain security tools are less widely used if they need to be purchased and/or require an effort from the Internet user to understand the risks and weigh them against the expenses. Nevertheless, these tools concern risks that are statistically less common (electrical protection, encryption, biometrics, theft protection devices, etc.) than viruses and spyware.

A counter example, and a significant one at that, is the antivirus. To address the threats felt and the risks expected (sometimes perceived as such due to an unfortunate personal experience), Internet users do nevertheless invest in antivirus update subscriptions.

Conclusion

Our survey has revealed that Internet users are generally not very preoccupied by potential threats resulting from their Internet use. Only 25% of expressed strong concern for the protection of their data or equipment and 94% of them felt “mostly or completely” safe when using the family computer to access the Internet.

This observation seems surprising given that current events have shown that not only are threats not diminishing but they are also increasingly ingenious. If Internet users believe to be in relative security, it is certainly due to the presence of a defensive arsenal that does indeed appear sufficiently developed (widespread use of antivirus, anti spyware and personal firewall). However, there is no guarantee that these tools are correctly used and configured. This situation may deteriorate in the future, as young Internet users seem less cautious about revealing their identity on the Internet and downloading software. There is no doubt that actions to raise awareness, or even training, need to be more fully developed in the future.

Appendix


TELECOMS
TRANSPORTS
BTP
COMMERCE
SERVICES
INDUSTRIE
COLLECTIVITES PUBLIQUES
98
99
00
01
02

Appendix

Glossary[12]

Term	Definition
BCP	Business Continuity Plan Sometimes Disaster Recovery Plan or DRP is used. Note that this term does not take into account the company's business activities.
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISMS	Information Security Management System
ISO 27002	International standard constituting an information security "best practices guide" (formerly ISO 17799:2005).
ISP	Information Security Policy All of the criteria enabling the provision of security services (ISO 7498-2).
ISS	Information Systems Security
ISSP	Information Systems Security Program. Guide for developing information system security policies, established by the Central Information Systems Security Division (DCSSI). See http://www.ssi.gouv.fr/fr/confiance/pssi.html.
MEHARI	Method of risk analysis, developed by CLUSIF. See http://www.clusif.asso.fr/mehari/.

[12] To complement these definitions, readers are advised to refer to the "**Glossary of Threats**" available on the CLUSIF Website at http://www.clusif.asso.fr/fr/production/glossaire/.

Term	Definition
SIM	Security Information Management Tool used to collect, report and analyze various information sources related to information systems security events.
SPC	Socioprofessional Category Characterization of the French working population in classes and occupations, established by INSEE. See http://www.insee.fr/fr/nom_def_met/nomenclatures/prof_cat_soc/pages/pcs.htm.
SSO	Single Sign-On System enabling information systems users to authenticate themselves only once to access several applications.
ToIP	Telephony over Internet Protocol
VoIP	Voice over Internet Protocol

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS
30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Download all CLUSIF publications at
www.clusif.asso.fr