



devoteam  
consulting ↑



The 2008 International  
Information Systems Security Survey

CONNECTING BUSINESS & TECHNOLOGY



**Hervé Morizot**, an ESIEA engineer came to Devoteam SA in September 2004 to manage the XP Conseil Business Unit. In 2007, he became the Director of Devoteam Consulting's Information Management and Security division.

**Hervé Morizot** has lead several major IS Security Management projects (organisation, policy, communication, performance indicators, risk management and auditing, etc.) for large French companies. He has presented at several IS Security Conferences, is currently a lecturer at the Ecole Nationale Supérieure des Télécommunications in Paris (TELECOM ParisTech) and has chaired the Eurosec' Program Committee since 2005.



# ABOUT THE SURVEY



For the 5<sup>th</sup> consecutive year, **Devoteam Consulting** has been conducting a survey on Information Systems Security issues from companies and organisations.

The 2008 survey, based on a 39-question questionnaire, was prepared by an international panel of information systems security managers (ISSMs): a total of 177 people from Europe (Austria, Belgium, Denmark, France, Italy, Norway, Czech Republic, United Kingdom), Northern Africa (Morocco) and the Middle East (Saudi Arabia) participated in the survey.

The companies and organisations which participated in the survey have more than 500 employees and are representative of the various sectors of activity: industry & services, finance and public sector.

To highlight the evolution of certain security trends and issues, some of the same topics will be addressed this year as in the previous years.

Other topics have been added to the 2008 survey so as to be able to account for any new trends and issues facing the security community today.



# RESULTS

## Security's place in the organisation

**The place of ISSMs (Information Systems Security Managers) within the organisation rarely changes, even if their roles evolve:**

- 72% of ISSMs agree that their role is recognised within the organisation, even if a slight decrease has been noted in comparison to last years (75% in 2007).

24% of ISSMs thus feel that their roles are not recognised, there is a lack of maturity and awareness about IS security issues and their actions are for the most part, “transparent” for the users.

- The average size of the teams responsible for IS security depends on the company's size and sector in which it operates: 67% of ISSMs manage a team of one to five persons, 10% of the ISSMs have a team larger than 20 persons.

The sectors whose trade rests largely on information systems are consumers of resources directed around safety (banks, finance, energy, etc.).

Large groups may have as many as a hundred security team members.

By order of priority, these teams divide up their activities among infrastructure security, operational security management, activities involving IT governance and finally business continuity activities.

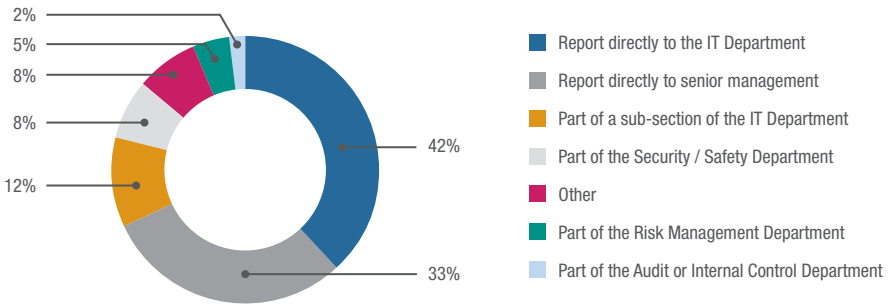
- 33% of ISSMs report directly to senior management while 54% are attached to an IT Department (either directly or indirectly via an entity of IT). The others are part of other departments (Security, Risk Management, Internal Audit Department, etc.).

This position often depends on the size of the company and sector in which it operates: attachment to an entity other than IT is often seen in companies that tend to integrate security within an overall approach to risk management. In small organisations, the ISSM may have to fulfil several operating roles (research and development, steering projects or leading management activities), as such he/she is logically attached to an IT Department.

Only 44% of the ISSMs surveyed are dedicated to the Information Systems Security at their company.

- Finally, ISSMs are systematically consulted when making changes to the company's information system and 69% of the time, their advice is taken when opposing a change which they deem detrimental to the company's security.

### As an ISSM, what is your place in the organisation?



## Major security governance work streams in 2007

In comparison with previous years, issues relating to security governance have changed. The 2007 priorities were as follows:

- Development of business continuity plans (59% versus 53% in 2006),
- Legal and regulatory compliance (40% versus 33% in 2006),
- Awareness-raising and professionalization activities (43% versus 35% in 2006),
- Overall risk management (41% versus 31% in 2006),

Regarding this issue: 30% of companies have conducted an overall risk evaluation in 2007 and 27% conducted a risk evaluation on their so-called “sensitive” processes.

39% of the companies implemented this overall risk evaluation process as to respect the company’s internal policy, 27% to respect legal requirements.

Finally 36% of these companies re-evaluated their risks on a yearly basis and 37% on an ad hoc basis, thus showing a willingness to continuously develop processes.

- The fight to counter fraud affecting information systems is often neglected (22% versus 12% in 2006).

**In 2007, 23% of ISSMs emphasised the definition and setting up of security monitoring performance indicators. 55% of them disposed of performance indicators as to ensure:**

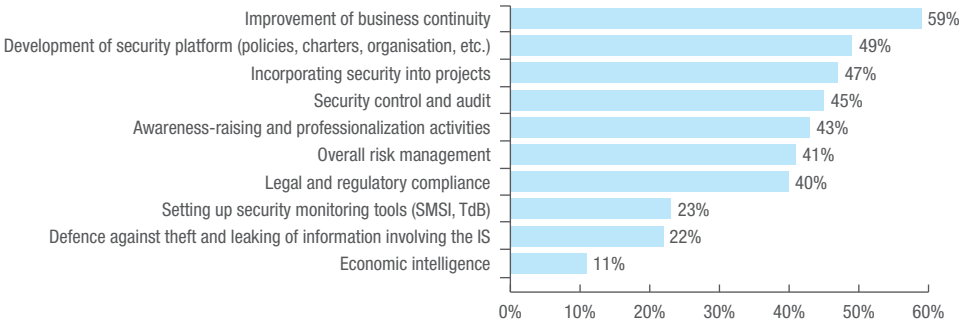
- Security monitoring during projects (28%),
- Monitoring of attacks and spreading of viruses (35%),
- Monitoring of security tool roll-outs and patches (35%).

Economic Intelligence was a priority in 2007 for only 11% of those surveyed, since this issue is often the responsibility of other entities within the company (strategy, communication, commerce, etc.).

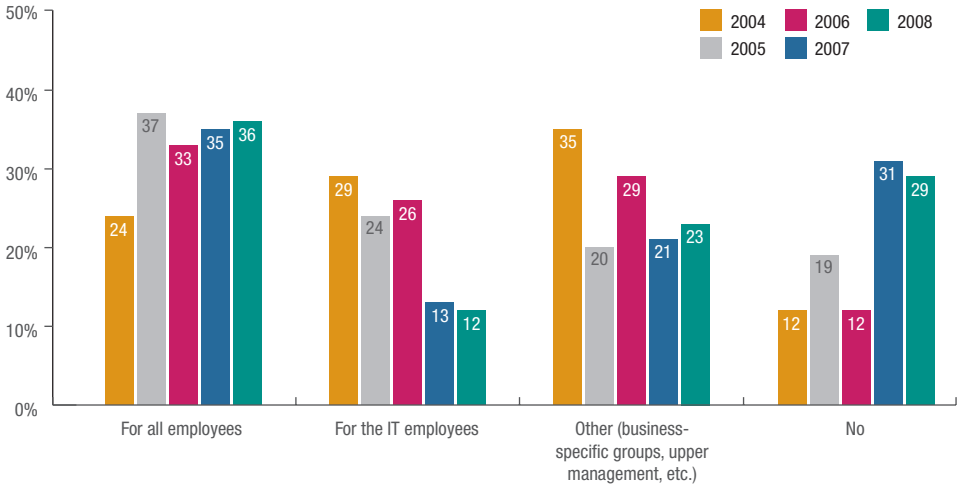
Issues relating to governance were only partially treated due to: an insufficient budget (39%), lack of time (64%), poor assessment of the teams (41%), lack of involvement of senior management (26%) and a need to prioritize other issues (24%).

Many companies have units responsible for security monitoring: 59% of these companies have set up a technological watch (security breaches, corrective actions, etc.) and 41% have a legal watch.

### What were the level 1 priority security governance concerns in 2007?



## Does your company organise IS security training sessions or awareness-raising activities?



### 71% of the companies offer training or IS security awareness programs.

27% of the ISSMs consider that these programs are provided on a continuous basis with a specific budget, 40% would like to see these programs renewed on an annual basis and 23% estimate that it is an activity organised every 3 or 4 years.

The evolution shows that awareness programs are more and more oriented towards all company employees, not only to IT employees. In addition to overall security awareness programs, specific awareness-raising procedures aimed at business-specific categories are increasingly being envisaged.

Finally, 32% of those surveyed said that each new recruit must take an IS security training program.

## Work streams in infrastructure in 2007

The concerns of security teams in 2007 with regard to infrastructure protection were focused around the following priorities:

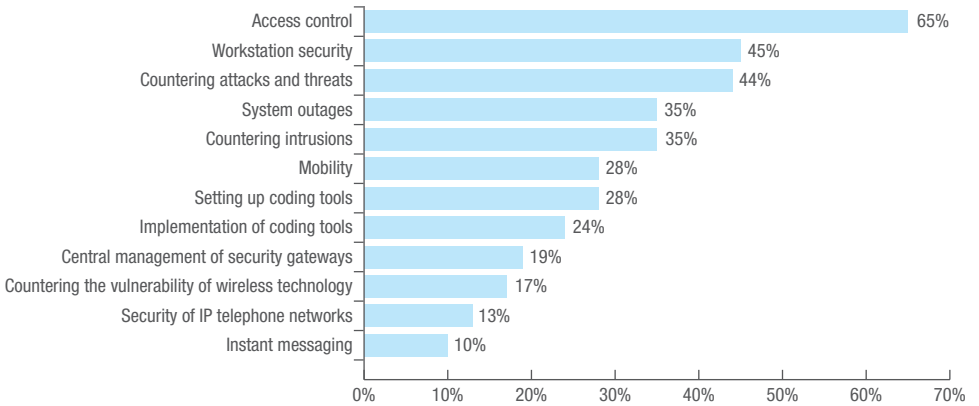
- **Access protection** (authorisations, revocations, etc.) represented the number one concern in 2006 for 65% of companies,
- Secondly, projects concerning workstation security (45%), specifically due to migrations toward Vista, and the convergence of security editors on the market,
- Protection against viruses (44%) remains a priority for companies, while protection against intrusions is increasingly present (35% in 2007 versus 12.5% in 2006),
- Unavailability of information systems preoccupy 35% of ISSMs in 2007 (versus 45% in 2006).

Projects linked to mobility, log correlation tools, and the setting up of coding tools are level 1 priorities for roughly 28% of companies.

**Certain themes only concerned a few of the companies, which considered them a major priority:**

- Management of central gateways (19%),
- Wireless technology security (17%),
- Security of IP telephone networks (13%),
- Instant messaging (10%).

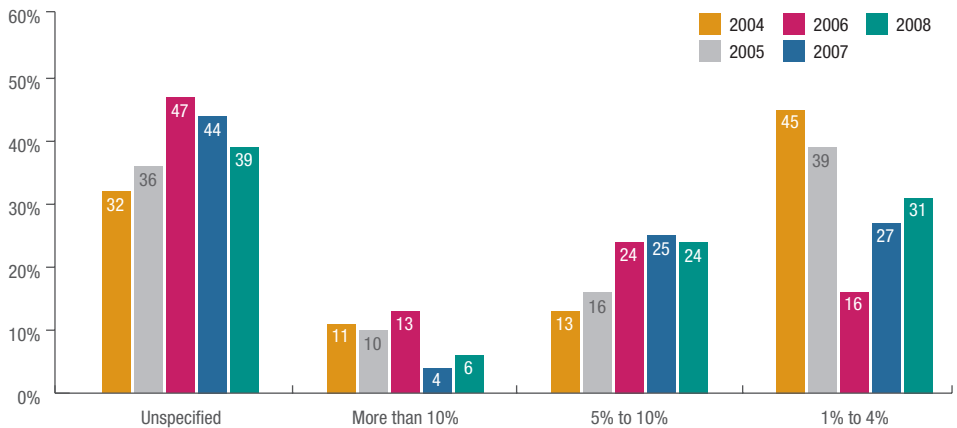
## In 2007, what were the level 1 priorities in the area of infrastructure security?



# Budgetary trends

With regard to budgetary trends, as in the 2006 / 2007 surveys, 85% of the ISSMs posted that their 2008 security budget is either the same, or higher than the previous year. The security perimeter from one company to another (safeguarding, Business Continuity Plan, informational risk managements, etc.) and the average budget is around 5% of the IT budget.

## In 2008, what proportion of your company's IT budget will be allocated to security?



## Observations on the implementation of IS Security policies

### A noted improvement in countering attacks:

In 2007, 52% of the companies surveyed stated that they had been the victim of minor attacks with limited consequences (versus 57% in 2006), 7% said that they had been the victim of an attack with significant consequences (versus 8% in 2006), and 39% said that they had not been the victim of any attack (versus 35% in 2006).

Among the companies having had an IS security problem (intrusion, data theft, unavailability, viruses, etc.), only 12% were able to identify the financial losses.

However, 55% of ISSMs do not measure the return on investment on the security of their information system, only 29% actually do.

# Priorities for 2008

In 2008, the major work streams in the area of security governance were of three types:

- **Development of the security platform**

On average, 90% of the panel has a security referential (policies, directives, charters), but it will be integrated into a maintenance and monitoring process.

- **Launching of ISO 27001**

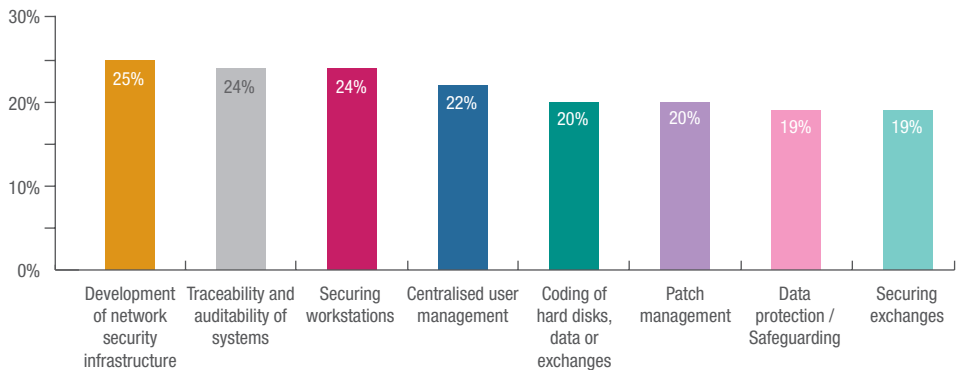
Even if the standard brings about control (identified as a low priority in 2007), many companies still aim to comply with the standard without initially being certified.

- **Risk evaluation**

This priority was only noted by 30% of the panel, but the situation at year start and the perspectives to strengthen regulatory requirements predict an increase of the risk evaluation method.

The major work streams for 2008 are focused on security network changes (departitioning, strengthening, etc.), securing workstations and system traceability and auditing.

## What work streams are a priority in 2008?



# Compliance

## Regulatory

The percentage of ISSMs directly or indirectly responsible for the company's regulatory compliance continues to be high at 76%.

Besides the Législation Informatique et Libertés (only 55% of ISSMs are involved), the companies are subject to business-specific regulations (31%), LSF (25%), Bâle II (23%), SOA and CRBF (20%).

## Internal / External Audit

65% of the ISSMs declare having carried out at least one internal audit during the year and are mostly all involved in the designing and monitoring of the action plans.

62% of them have also carried out an external audit throughout the year as to identify the weaknesses (40%) and to check the regulatory compliance (15%).

## Norms, Referentials

44% of companies use ISO 17799 / 27002 to design their security policy (34%) or to carry out a security level diagnostic (20%).

38% of companies use ISO 27001 to set up their security management platform for their information system (SMSI) and 10% of them are already preparing for a certification, often for a very restricted perimeter.

However, frameworks such as COBIT or COSO are still rarely used (respectively 24% and 9%).



devoteam  
consulting 

86, rue Anatole France 92300 Levallois-Perret  
Tel. : +33 (0)1 41 49 48 48  
[www.devoteam.com](http://www.devoteam.com)