Management of IT Risks

Esther Cerdeño
Deputy Director of IT
MAPFRE REASEGUROS (Spain)

"The market needs insurers to study the feasibility of insuring costs relating to loss of information; in order to do this the insurance companies analyse the various aspects in connection with these risks"

1. Introduction

The extent to which companies depend on their computer systems and their complex nature have given rise to increasing concern about safeguarding the systems' ongoing operation from faults and interference. Furthermore, protection of data on third parties, customers and employees contained in databases is of prime importance in controlling privacy and rendering it safe from interference and preventing leakage of information to others. In order to achieve the foregoing it is necessary to set up a series of measures to ensure that computer systems are securely protected against service interruptions.

Corporate concern about security and the correct functioning of equipment has led to an increase of 60% in expenditure on IT applications for data protection and security purposes, whereas other areas, such as software updates, have maintained their growth in recent years. Attacks, whether by sabotage or virus or even as a result of natural disasters such as earthquakes, fires or hurricanes can wreak havoc on equipment and databases, causing important information losses and major direct expenditure in addition to possible negative effects on the company's future image and reputation.

This concern with security entails major expenditure on contingency plans and safeguards, whose maintenance and readiness need specialized personnel in the different areas that comprise the company's IT network. In some cases these services have been outsourced to other companies, however this does not eliminate the problem because the same defence mechanisms must be set up in the outsourcing company.

In view of this situation the market needs insurers to study the feasibility of insuring costs relating to loss of information; in order to do this the insurance companies analyse the various aspects in connection with these risks, ascertain which studies need to be carried out, the costs involved, and, finally, whether the risks are insurable.

This article attempts to identify the risks and in general terms the preventive measures that can be taken to insure the information. There follows a brief review of a possible plan for continuing the business and recovering information in catastrophic situations, in addition to setting out what the insurance company can do to offset the financial costs incurred through loss of information and equipment.

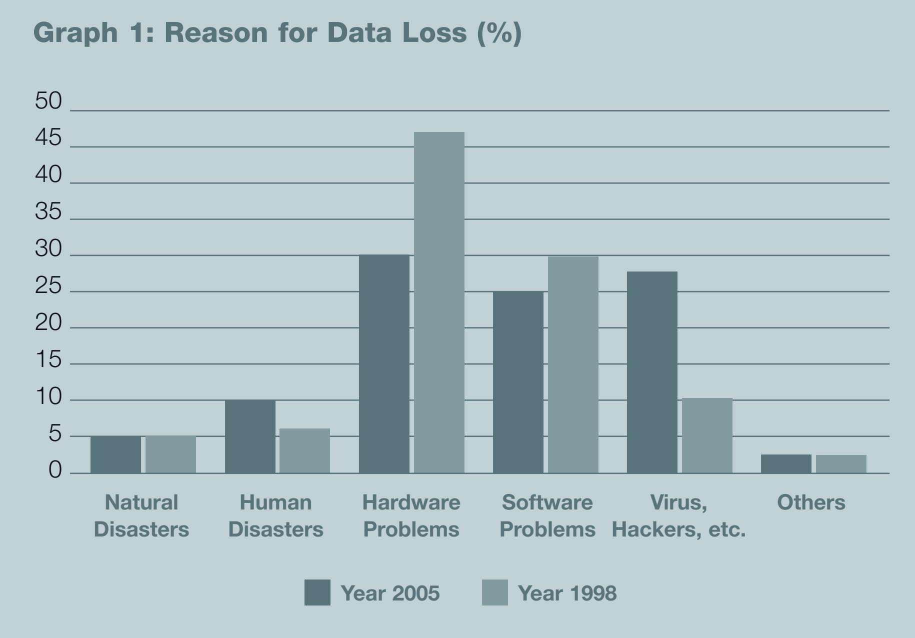
2. 2. Risk Analysis – Contingency Plans

Risk Factors

Various studies on the reasons for data loss in computer systems have shown that up until six years ago the main causes were hardware faults or equipment malfunction, whereas today losses caused by viruses, sabotage and other external factors have increased.

Amongst the reasons for corporate data loss (see Table 1-page 14) are the following:

- Hardware failures in the computer system
- Human error



- Software failures
- Threats from external sources such as viruses and outside hackers or from employees within the company
- Natural and man-made disasters, including those of a political nature

Company Situation

At a time when fresh threats to corporate and institutional computer systems are appearing constantly, it is vital to ensure business continuity. To this end companies should draw up emergency contingency plans to enable them to continue their daily activities in all circumstances.

Drawing up a "business continuity plan" involves analysing the potential risks and evaluating the potential losses. According to some studies however, up until the 2007 financial year only 35% of large companies will have a solid business continuity infrastructure, in spite of recommendations from those in charge of IT in this regard.

As a recent examples of the aforementioned risks it is worth remembering that some companies located in New York's Twin Towers disappeared after the terrorist attacks of 11 September because they lacked data backups held outside those buildings. The power cut in New York and Canada also had major financial consequences. In February 2005 the fire in the Windsor Tower in Madrid's financial centre disrupted businesses and affected thousands of workers; in some cases it took up to 96 hours for some companies to resume their normal business activities.

Armed with this information, it is clear that expenditure on security and business continuity will grow rapidly in coming years to reach a figure of approximately USD116 billion (EUR 91.17 billion) in 2007, according to IDC (International Data Group), who analyse world markets and forecast future Internet and IT trends. Furthermore, a report by Gartner Dataquest states that "one out of every three North American businesses could lose data vital to their continuing operational ability in the event of a disaster, unless they draw up an emergency contingency plan immediately", and "rather than prioritizing investments, emphasis should be placed on ensuring that businesses can recover productivity quickly following an incident".

As will be seen from preceding paragraphs, the answer is to have a contingency or business continuity plan covering the entire organization and computer systems, whether on paper or in electronic format. It is a matter of analysing how to prepare such a plan, who should draw it up and monitor it and what the cost will be.

ISO 17799

ISO 17799 is a list of flexible suggestions that assists those responsible for corporate IT security to set up an effective plan, irrespective of size or sector.

The technical standard was purposely designed to be flexible, without advocating any specific security solution. The suggestions contained in ISO 17799 are impartial as to technology and help to assess and understand existing security measures.

It establishes a progressive model based on security at different stages, from which the most appropriate should be selected in accordance with the company's business.

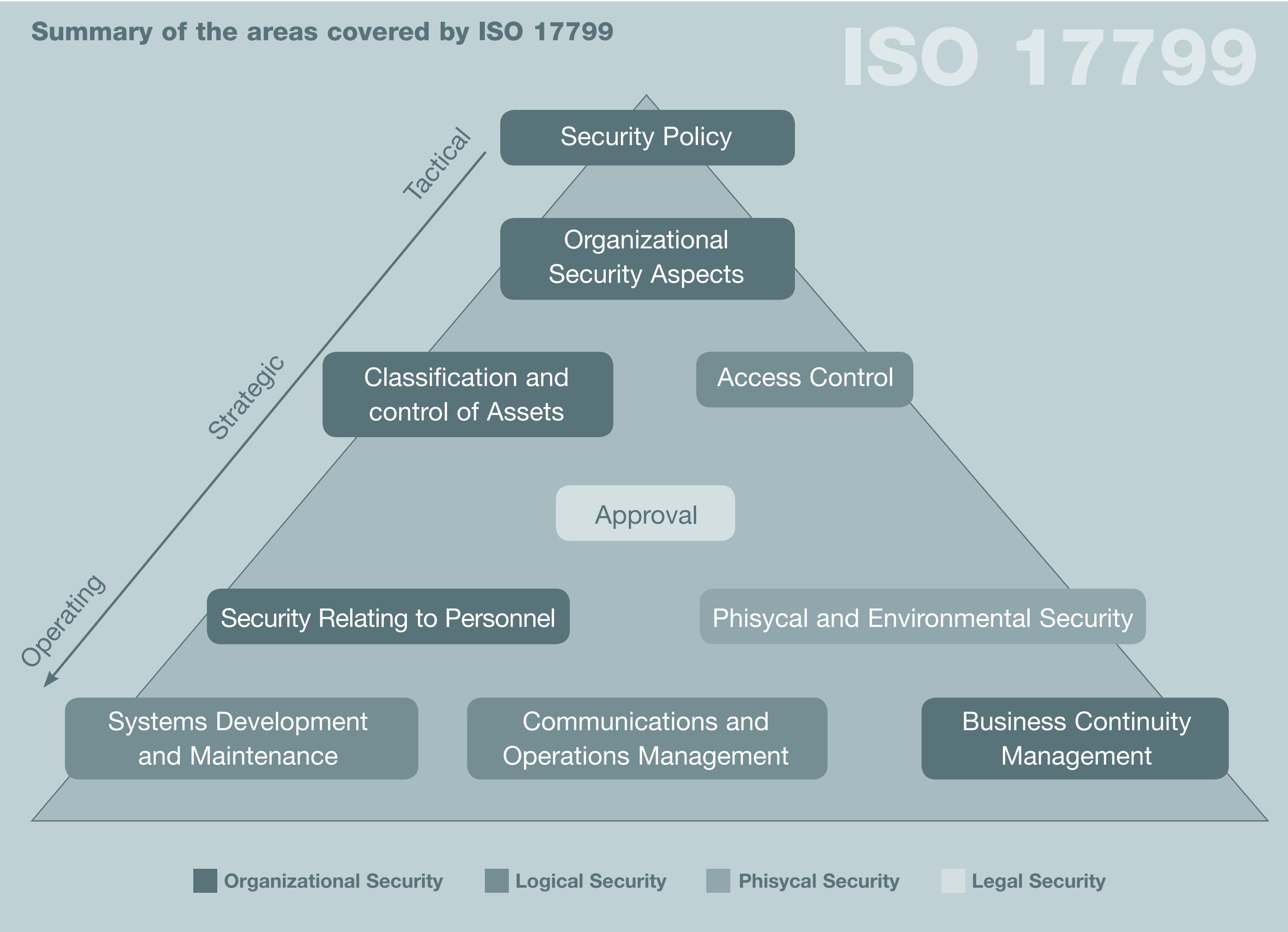
Within the area concerned with maintaining business continuity, it is advisable to be prepared to effectively deal with business disruption and protect assets in the event of a natural disaster or a man-made event.

Table 2 (see page 16) sets out a possible means of implementing a contingency plan which should, at a minimum, cover the following points:

- Classification of technological resources. Analysis and inventory of:
  - Electronic equipment on which the company relies
  - Applications (accounting, administration, HR)
  - Services (inter-office links, internet access, etc.)
- Classification of logistical resources
  - Fixtures and fittings
  - Office equipment
- Classification of operating resources
  - Description and identification of the business carried out by the company, highlighting key procedures

Security at different stages ISO 17799

Basic Level	Low fraud risk. Absence of Personal Data. Low dependence on technology.
Intermediate Level	High fraud risk. Personal Data and legal regulation. High dependence on technology.
High Level	Heightened fraud risk. Personal Data and legal regulation. Fully dependent on technology.
Governmental Level	Information to be protected, which, if divulged, could compromise the nation's security and defence.



– Security

– List of those responsible for the different areas (databases, application servers, etc.)

– Supply of water, light, etc.

- Risk analysis. List of risks (human error, sabotage, etc.) and classification.
- Search for potential weak points in the existing infrastructure
- Estimate of maximum period of inactivity (disruption time) and maximum period that a key procedure may be interrupted without affecting the organization's viability.
- Identification of recovery times at a minimally acceptable initial level, and thereafter, full recovery times for the company's business.
- Options in the event of failure (duplication, replication, additional backup copies)
- Identification of procedures to be implemented in the event of an incident
- Setting up a schedule for periodic reviews and updates
- Setting up a test schedule.

Table 1: Causes and Preventive Measures

Hardware Failures: Incorrect Operation

Causes	Faults in a given key device: – Disks. – Controlling mechanisms. – Processors. – Memory. Electrical faults.
Preventive Measures	Duplication of server equipment. Duplication of components such as fans and power sources. Backup controlling mechanisms. Backup disks. Computer rooms protected against fire, flood and high temperatures. Uninterrupted power supply system (UPS). Creation of backup copies. Location of backup devices in places other than computing centres.

Human Error

Causes	Accidental deletion of files, data. Boot-up whilst confusing disks with valid data. Execution of incorrect application sequences.
Preventive Measures	Development of applications in non-production systems. Testing of all applications in so-called preproduction systems, with a series of data similar to that used in production. System of daily backups.

Table 1: Causes and Preventive Measures. (continued)

Corruption of software

Causes	Updating to new versions of operating systems. Updating to new versions of a specific application. Installation of patches that are not compatible with the existing system. Installation of new controllers. Failures arising from complex configurations. Failures arising from unregistered applications.
Preventive Measures	Installation of drivers, patches, etc. in non-production systems. Daily creation of backup copies. Systems for backing up online. Additional copy systems. Analysis and diagnostic tests prior to installing new applications.

Viruses, Hackers and Malicious Codes

Causes	Massive generation of email that overwhelms the system and corporate mailboxes. Use of security flaws that prevent system connections. Denial of service attacks. Unexpected system restarts. Access to websites viewed as dangerous. Use of programs such as e-Donky.
Preventive Measures	Implementation of preventive measures regarding opening emails from sources unknown to users. Use of antivirus. Updating antivirus at least once a day. Use of tools for analysing packages on the Web. Tools for analysing contents and blocking access to blacklisted sites on the World Wide Web.

Natural and Man-Made Disasters

Causes	Fires. Storms. Earthquakes. Floods. Sabotage. Terrorism.
Preventive Measures	Establish security policy. Protection of buildings (reinforced basement and roof). Fire extinguishing equipment. Air-conditioning systems. Systems duplication in different locations.

Table 2: Methodology for a contingency plan

Analysis of effect on the business	Setting up of plan development group. Identification of key functions. Analysis of the impact of a disaster on each key operation. Identification of minimum service levels. Assessment of the cost/benefit ratio of each alternative.
Planning	List of applications. Appointment of person responsible. Preparation of plans. Documenting the plan. Confirmation of plan.
Recovery Strategy	Backup systems – online/offline. Duplicate backup systems, additional copies.
Simulations	Estimating the scope of the simulation. Establishing the applications or services. Possibility of tests in real time. Carrying out tests. Documenting tests.
Maintaining the Plans	Updating the contingency plan in accordance with the results obtained in the tests. Periodic reviews. Updates to include new services, applications and systems. Audits.

Table 3: Summary of the stages for drawing up the Business Continuity Plan

Define and Document the Continuity Strategy	Time for activating the plan. Technological infrastructures. Key locations. Alternative manual procedures.
Development of the Manual for the Continuity Plan	Support information. Working groups. Procedure for replying. Recovery stages. Restoration stages. Procedures.
Approval of the Plan by Senior Management	Persons responsible for execution.
Test Plan	Identification of potential deficiencies. Updating the Plan.
Plan maintenance	Awareness campaign. Continuous training. Review.

Insurance Companies

Faced with the situation described in the preceding paragraphs, it is necessary to analyse what the insurance companies can offer and on what they should base their studies for accepting such risks. The companies that are writing this type of policy are those that specialize in technology and the dot-coms, because they are more aware of the pitfalls.

There is a lack of knowledge on the part of policyholders on the availability of cover. Some surveys on the existence of a policy and what is the cover for damage caused or loss suffered to IT systems, indicate that about 40% of the insurance market is unaware of it. In most cases, policies do not cover incidents arising from earthquakes and storms. It is also noted that about 34% did not have any type of insurance. In order to obtain appropriate cover, and for an insurance company to offer it, it is necessary to quantify and identify the risks to be insured; this requires time, knowledge and human resources.

Insurance policies covering computer equipment fall under engineering business, classified as "Computer Insurance" or "Electronic Equipment Insurance". Purely for information purposes, "Computer Insurance" may cover damage suffered by data processing equipment, in accordance with the information given in the contracts. Damage arising from wear and tear, installation, effects of temperature, etc. is excluded.

Cover may be extended to costs arising from recuperation of data due to damage suffered by such items as disks and tapes.

"At a time when fresh threats to corporate and institutional computer systems are appearing constantly, it is vital to ensure business continuity. To this end companies should draw up emergency contingency plans to enable them to continue their daily activities in all circumstances."

In the basic type of policy, the cover includes material damage to equipment, including that to magnetic data tapes, even in transit (caused by impact, fires and falls).

Specifically, "Extraordinary Risk" cover offered by the Consorcio de Compensación de Seguros Español extends to a series of risks including damage caused by:

- Earthquake, extraordinary floods, volcanic eruptions, storms, falling astral bodies and meteorites.
- Terrorism, rebellion, revolution, riot and popular uprising.

Other additional risks that may arise relate to compensation for expenditure incurred by the policyholder for rental or use of other equipment due to inability to access the computer room as a result of an accident in the area of the building or of the room housing the insured equipment. The failure of the public electricity supply that accidentally interrupts the operation of the insured equipment, giving rise to rental expenditure and use of other equipment, will also be viewed as a covered risk.

In line with the foregoing, each insurance company should carry out a study of the situation of the computer equipment belonging to the company taking out the insurance, prior to accepting the policy. One important aspect would be to establish whether there is a contingency plan, or, without going to such an extreme, to ask what measures are being implemented to back up equipment and what the policies are relating to security, antivirus and detection of hackers, as outlined in the preceding paragraphs. Clearly, risk cover and its price will depend on the level of knowledge of these aspects and on the action plan to avoid contingencies and reduce costs, in addition to the period of inactivity.

In accordance with the clauses contained in the insurance contracts, a large part of the expenditure should be covered by the insurance companies, although, as indicated by the surveys, most companies are not currently aware of the extent of available cover. ■