Protection, a Strategic Value
José María Insua
Expansión
27/02/04

Security is an essential element for a company’s reputation. An error, like the loss of key information, can ruin the good name of a company.

News about corporative information leaks severely damages a company’s credibility. The constant loss of confidentiality and/or accessibility to personal information, the leaking of bank data by the different financial entities that operate on the Internet and the lack of critical services being available in the face of contingencies, among other points, warn us of the importance of information security within a business environment, which is more and more interconnected and open to its partners, suppliers and customers.

These breaches of security prove that the focus on information security is still highly reactive and centred exclusively on information systems. Only external factors like rules and regulations place a certain pressure and awareness on organisations.

On this point, the “Ley Orgánica de Protección de Datos de carácter personal (LOPD)” or the Organic Law on Personal Data Protection in Spain has been added to other regulatory national and international initiatives, that aim to gauge, among other things, aspects of transparency and good corporative governance related with suitable risk management associated with the information of organisations. These circumstances are what are turning information security into an indispensable element of corporative reputation and a more and more valued asset by top management. What is more, while the good name of a company takes years to acquire, it can be destroyed in a flash by a mistake like the loss of key information.

However, most companies still see information security as something predominantly tied to technology. The report “The State of IT Security 2003”, made by PricewaterhouseCoopers and the CIO magazine, points out that 62% of companies assign security control to their IT heads while the CEO is in charge of security in only 16% of the cases.

These data confirm that there is still a long way to go before companies stop treating information security as a purely administrative task in their overheads budget or as a mere technical aspect easily tackled by a standard technology product.

This is a serious mistake as information security does not solely lie in technology. It must be considered within an integrated business solution based on the strategic combination of resources in organisation, processes and technology.

External factors
The PwC study reveals that most of the security initiatives are still motivated by external factors (industrial and regulating practices) and are not dealt with from a risk management perspective. This is another slip-up as companies must take into account that information security is a strategic business process for organisations. Because providing a balance between protection and the possible coherent use of information assets on the one hand, and business objectives on the other, will mean a considerable improvement in operating performance. Therefore, security strategy can result in smaller running costs, an increase in income, a competitive advantage and lastly, value for shareholders.

For this to happen, information security has to be included as a priority in the corporative agenda and to be considered as a strategic business process that affects what organisations value most: their business objectives, their yield and most importantly, their responsibility and credibility towards third parties. The creation of an objective formula to calculate the return on investments in security (what is known as ROSI) could help security professionals to win the support of their superiors. For the moment, only 14% of the companies surveyed by PwC have a process to calculate the ROI on investments in security while 12% quantify the cost of a breach in security. But there is no reason to lose hope: 2004 looks like being the year in which companies include security in their strategies.

What are the main trends in information security?

A great variety of facets
Elena Maestre, Senior Manager PwC
At present, the trend in information security can be expressed in terms of the need for protection and the guarantee of accessibility and, what is even more difficult, in terms of a balance between both factors. This need defines a model that enables the structuring of security in the different activities that create value for organisations, always taking the business strategy objectives as a starting point while bearing in mind the resources and abilities to support the diverse security solutions to be implemented. The business objectives must direct the right balance of security, taking such factors into account as the need to abide by regulations, the internal corporative and good governance strategies and those factors that come from the relationship or collaboration that is developed with third parties. However, the abilities to support the model will be conditioned by the combination of three basic factors: the organisation of each company, the business processes supported and the existing technological infrastructure.

Towards a necessary balance
Brian Subirana, IESE professor
Security responds to the need to control valuable information that is potentially accessible by unauthorised machines or persons. As there is more and more digital information that can be intercepted, there is also a flood of solutions. Each one has its own special features, in accordance with the multiple characteristics of security. Three of these stand out. Firstly, more and more information now comes coded in many devices, so that threats cover everything from attacks on microprocessors to viruses in
the macros of spread sheets. Secondly, the probability of intrusion and its cost varies
from one situation to another, so the regulations do not provide enough legal cover.
Lastly, business processes increasingly demonstrate the impossibility of having a
technology that is totally reliable. Thus, contradictory models, which are to a certain
extent complementary, have made their appearance. In fact, security has as many facets
as the number of people in the world.