11-S: learn from vulnerability
Josep Valor, IESE professor

The fatetul events of 11-S have helped those responsible for company technology to better understand the importance of protecting tangible and intangible assets. Business information is a kind of value that, if “well exploited” by enemies, may leave companies out of the game.

Security measures must adapt to the vulnerabilities of the goods they are trying to protect. In the physical world, they are dealing with more stable measures because the vulnerabilities that they are trying to prevent are also vulnerable. On the other hand, the management of company information is a complex and changing activity demanding constant new infrastructures which may leave vulnerabilities uncovered.

The technology to break into the information systems of companies is evolving pretty fast as well, forcing them to make important changes in their security systems. Business security systems, above all in the Internet age, are constantly “under construction”, a provisional situation that increases the risk of having holes or back doors open to intruders.

More and more, companies are trying to overcome this complexity by resorting to specialised suppliers that provide, in addition to the expected “defence” services, security audits based on an attack on the systems of the client company. Although some people fear it, the strategy of allowing the attack is the only way companies have of knowing the difficulties a person may face if he wants to enter their systems. In that case, attack is the best defence against vulnerability.