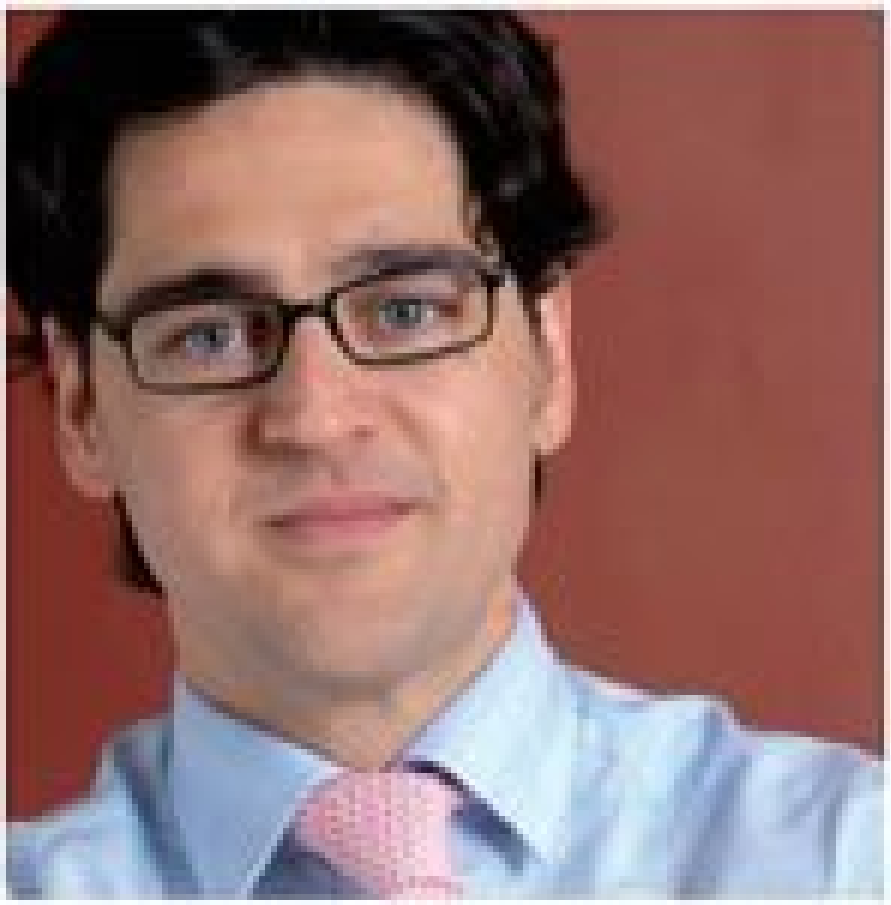
PROTECTING AGAINST KNOWLEDGE THEFT - ÉCIJA

Posted on 30/10/2009



Category: Uncategorized

Businesses need to be aware of the need to protect their data from loss or 'leakage'™ and understand that most issues arise internally rather than externally

En el siglo XXI el conocimiento es poder y las empresas de todos los tamaños y de todos los sectores tienen que estar alerta ante la amenaza de fuga de información y especialmente en el actual clima económico, comenta Álvaro Écija, socio director de Écija en Madrid.
Businesses of all sizes and across all industry sectors have to be alive to the threat of 'data leak' and particularly in the current economic climate, says Alvaro í‰cija, co-managing partner of í‰cija.

'In the 21st Century, knowledge is power, and in this highly competitive and economically uncertain environment the protection of sensitive data must be a priority for both private and public

enterprises. Most company data is no longer kept in a physical form that can be simply locked away,' he warns.

Databases utilised for client and deal lists, employee records and many other types of sensitive data, may be highly valuable, but they are also easily transportable. The removal of which, whether intentionally stolen or accidentally lost, can have serious financial, reputational and regulatory consequences for an organisation.

'Obviously sectors, such as the IT, finance and banking industries have a clear business and regulatory need to protect information such as product codes, client account numbers and customer details and databases, but the issue is not simply restricted to them, it can affect any business,' says i‰cija.

And contrary to popular mythology, the threat of attack or data theft does not usually come from external hackers but much more often from inside a company itself. For businesses particularly undergoing a restructuring or facing the prospect of redundancies the temptation to take client or contact lists to a future employer, and potential competitor, may be too tempting for some.

Employees may swap user names and passwords, download information, or send information across non-secure communication media such as email. But i‰cija believes that by reviewing processes businesses can protect themselves from both external and internal threats.

'Security cannot rest merely on technical components, or just depend on tools or techniques, but should be based on establishing risks, communicating those risks and managing them across the organisation. It is only then that we can clarify lines of responsibility and better manage security access and restrictions on how data is shared to avoid the threat of security incidents'