The year of living dangerously

Data vulnerability has become a major concern in the past 12 months, posing three distinct risks to organisations

DATA VULNERABILITY AND security is an issue for all organisations, regardless of their industry sector.

"The risks of unauthorised surveillance, fraud, theft and hacktivism have become particularly apparent in the past 12 months, with a number of high-profile data security incidents in Europe and the US," says Arthur Artinian, partner in law firm K&L Gates' London office and a member of its intellectual property group.

"The issue is not specific to data-intensive businesses. It applies to any organisation that holds or collects individuals' data, whether intentionally or inadvertently. Of course, the risk profile increases as businesses become more data-intensive, particularly for businesses that are built around big data – for example, the use of geolocational data of customers –and those that operate across borders."

Data security poses three key categories of risk to businesses. "Legal risk arises where a business does not meet regulatory compliance requirements or is exposed to contractual or civil liability when incidents occur," says Artinian. "Operational risk causes business disruption and interference with internal and external communications. Reputational risk arises owing to significant public awareness and scrutiny of the data security issues."

European overhaul

A survey commissioned by the UK Department for Business, Innovation and Skills in 2014 suggests more than half of UK businesses had already experienced a loss of data or leak of confidential information in the previous 12 months.

More than 75% said they had been subject to external data security attacks.

"The European data protection regime is currently the subject of an overhaul, due to be finalised in the next 12 months," says Artinian. "Once implemented, the new EU-wide regulation will impose additional regulatory burdens, including requiring businesses to obtain specific consent from data subjects and introducing significant fines for breaches.

"At the same time, European lawmakers are progressing a draft cyber security directive that will impose regulatory and best-practice obligations on business in key sectors, including those involved in the provision of essential infrastructure and services. Similar moves are under way in the US." **SR**

'The new EU-wide regulation will impose additional burdens'
Arthur Artinian,
K&L Gates