FT.com FINANCIAL TIMES
TECHNOLOGY
Digital Business

Legal fears holding back some initiatives

Print

By Geoff Nairn

Published: November 26 2009 18:04 | Last updated: November 26 2009 18:04

Like modern-day alchemists, organisations are urged to invest in business intelligence (BI) systems to transform raw data into valuable and, hopefully, actionable information.

But as the amount and variety of sources of information have grown, so too have regulations that seek to restrict how that information is used.

Information compliance and governance tasks are most onerous in the financial services and healthcare sectors, which are subject to strict data protection regulations. But across all industries, the regulatory burden has increased.

“We have seen more than 40 new regulations that have come into effect in the last 12 months,” says Mike Lynch, chief executive of **Autonomy**, the UK specialist in information management software.

In the past, organisations could often afford to adopt a cavalier attitude to their data. Enforcement of rules was lax and those overstepping the fuzzy line could plead ignorance and get off with a light fine.

But legislation such as the Data Protection Act in the UK, and Sarbanes-Oxley in the US has changed corporate governance. Senior executives are now personally liable for infringements of data handling and protection laws. Ignorance is no longer an excuse.

“What has changed recently is that there have been a number of high-profile data losses. The penalties for not getting it right have become much more stringent,” says Andy Vernon, BI specialist at PA Consulting Group.

Fearful of draconian penalties for non-compliance, businesses may be tempted to lock away or even delete sensitive data to ensure they never fall into the wrong hands. But such attitudes reveal a fundamental misunderstanding about what compliance means.

“Most regulations are not designed to prohibit the use of the data but require you to preserve them and that creates a big information management challenge,” says Robert Tennant, chief executive of Recommind, a US specialist in information risk management.

Industry experts argue that it is possible to strike a balance between the need to protect sensitive data and the desire to unlock greater value from that same data using the technologies of BI.

There isn’t really a compliance issue around BI,” says Matt Leighton chief architect for BI at Logicalis, the IT services firm. “The issue is more about deciding who I want to gain access to the information and implementing the appropriate policies.”

Nevertheless, there is some evidence that the fear of overstepping compliance boundaries, warranted or not, is holding back IT initiatives, particularly in industries such as financial services and healthcare.

In the US healthcare sector, for example, a recent study concluded that the laws designed to protect patients’ data could be restraining the adoption of electronic medical record (EMR) systems.

The widespread use of EMR technology is seen as key to creating a more efficient healthcare system.

As part of President Barack Obama’s stimulus package, the Health Information Technology for Economic and Clinical Health (Hitech) Act earmarks $20bn for the creation of an electronic records system.

As well as eliminating inefficiencies and errors associated with paper-based records, EMR systems allow patient data to be aggregated and mined to spot trends.

But researchers at the Massachusetts Institute of Technology and the University of Virginia found some hospitals were wary about exchanging data with hospitals in other states because of complex privacy laws.

The researchers found that states that made it easier to exchange data experienced a 21 per cent gain in hospital EMR adoption rates compared with just an 11 per cent gain in states with more restrictive laws.

The Health Insurance Portability and Accountability Act (Hipaa) is the principal law governing patient data in the US. But it is a federal law and allows the privacy laws of individual states to take precedence if they are stricter.

This “pre-emption” clause makes healthcare IT professionals understandably nervous about sending patient data across state lines particularly to litigation-happy states.

To complicate the legal framework further, the Hitech Act brings rules designed to strengthen Hipaa – preventing confidential patient data from being sold commercially, for example. The law came into effect earlier this year but many of its provisions have yet to be implemented.

The growing mass of legislation in this area is designed to address increasing unease about the way patient data are being used for non-medical purposes.

In 2007, the UCSF Medical Center in San Francisco admitted that it had shared information on more than 6,000 patients with Target America, a data-mining company with a database of 7m wealthy individuals.

By comparing its patient records with Target America's list, the hospital wanted to identify wealthy patients who could be approached for donations.

Surprisingly, perhaps, Hipaa allows healthcare providers to disclose protected health information to commercial organisations, providing they have a contract describing permitted uses and safeguards.

In this case, Target America's safeguards failed. The patient data ended up on the internet and the breach was not discovered until three months later.

The UCSF case illustrates the dangers of using personal data in a BI context.

Nevertheless, with safeguards and procedures, healthcare IT experts say it is possible to overcome the compliance hurdles and extract valuable information that would otherwise remain hidden.

NHS Islington, the public healthcare provider for north London, is developing a BI system to identify high-risk patients before they have to be admitted to hospital, so saving money and, hopefully, lives.

The system uses open-source technology from US vendor Pentaho to mine the medical records of about 195,000 citizens.

"The system is looking for 70 risk factors that increase the chance of an emergency admission," explains Ian Tritschler, associate director of IT at NHS Islington.

The system combines data from hospital admissions with the medical records of general practitioners.

Prior to using the Pentaho system, NHS Islington developed a similar application using just the data from hospital admissions.

But they realised it was only picking up a limited range of patients – some people are reluctant to go to hospital until it is too late.

The current system incorporates GP data as well, thus catching more people in its net and also building a more complete medical history of each patient.

Mr Tritschler says the system is a relatively simple BI application. "The same data testing approach could be used to identify who is most likely to purchase a brand of washing powder. The technology is the same."

Nevertheless, because the data involved are patient records, the project had to be designed to meet strict compliance considerations.

"We had to get the agreement from each of the GPs to use their patient information and the data are stored on a dedicated server," he says.

Instead of names, social security numbers are used to identify each patient and only one person, trained in compliance procedures, is authorised to process the data.

Most would accept the need for stringent procedures to protect medical data. But many organisations are reluctant to apply similar principles to their personnel records or customer data.

For example, many call centres have software to call up customer data on an agent's screen. In the US, this information may include the social security number, which is a potential breach of privacy laws, according to Francis Carden, founder of OpenSpan, a US firm that makes compliance applications.

His company's software can obscure sensitive information in "legacy" call centre applications and also prevent voice recording systems, whose use is obligatory in many call centres, from recording personal data.

Not surprisingly, IT vendors argue that the compliance problems created by legacy systems are best addressed by modernising IT systems. But for those whose budget will not stretch to a major overhaul, there are often other ways to address the problem.

For example, a business might want to see how well a product is selling in a particular town. For this purpose, the BI application does not need customers' names or even full addresses.

Account numbers and the first few letters of their postcode – enough to identify the town but not the street – would be sufficient and reduce the chance of the company potentially breaching data privacy laws.