Data Management in the Digital Age

The way we store and share data is rapidly changing and so too must the way we protect it. In 2000, only one quarter of the world's data was digitally stored, yet today less than 2% exists in a purely non-digital format. Whilst many companies have been quick to embrace the benefits and increased productivity that digitisation has brought, few have successfully addressed the inherent risks, making data management the single biggest threat facing companies today.

The year 2013 will serve as a perpetual reminder of the fragility of digitised data and the level of attention it attracts. High profile leaks at global banks, the inappropriate sharing of market sensitive data throughout the LIBOR scandal and Snowden's revelations over the mass collection of personal data by national intelligence agencies has laid bare the ease with which confidential information can be illegally intercepted, shared and stored. The knock-on effect for companies is that they must operate in a more privacy-conscious marketplace. Client and consumer paranoia has reached a zenith and the onus is on companies to demonstrate that they are implementing rigorous controls and safeguards to secure confidential data. 2014 is expected to bring in a year of regulatory activism and fiscal penalisation, making it increasingly complex for businesses to capitalise on the true value of the digital economy.

Industry Changes and Challenges

In response to mounting concerns around data management, the EU has been developing a Framework to replace their archaic regulatory standards with tougher, more modern measures. The current Data Protection Directive, drafted in 1995, predates fundamental technological revolutions including cloud computing and social media, and fails to account for more risk prone business practices such as bring-your-own-device ('BYOD') and outsourcing. Whilst the upcoming General Data Protection Regulation is unlikely to be fully implemented until 2017, businesses should prepare for dramatic changes. It mandates, for example, the appointment of a Data Protection Officer (DPO) if more than 5,000 individuals' data are being processed in a 12 month consecutive period. As well as this, there are plans to raise the current £500,000 limit on fines set by the Information Commissioner's Office to allow for penalties of up to 5% of a company's gross global revenue.

If not properly managed, the increased reliance upon BYOD and cloud computing services from outside parties threatens to undermine companies' data security systems by increasing points of entry and decentralising control of the network. This issue is exacerbated by the fact that the personal devices used by employees are getting smaller whilst the amount of data they can store is increasing considerably. A typical employee's mobile phone can now store upwards of 500,000 documents and USB sticks rival the storage capacity of hard-drives. This not only enhances the probability of loss or theft but increases the ease and speed by which data can be transmitted once seized.

The nature of digital data is such that it can be duplicated an innumerate amount times with no traces left on the original file. Consequently, theft or misappropriation becomes far more damaging and difficult to detect than for tangible property. Dropbox, for example, is run from Amazon's s3 server network which boasts a global network of server farms to host stored data. If an employee uploads confidential files to a Dropbox account to work on from home, the data is instantly cloned and stored in Amazon's datacentres across the world. It can no longer be erased, because it exists in an immeasurable number of instances across multiple legal jurisdictions.

In theory, this scenario should never present itself in a business environment. Companies should have effective controls in place to prevent them relying on inferior and free products to handle sensitive data. Confidential documents would never be sent by 2nd class, unregistered mail and neither should confidential files be stored or transmitted without the proper controls in place.

Questions to ask yourself

1. The level of Board involvement: How often do your Board get involved in data management decisions?

The gravity of data related issues means that it warrants proactive action by the Board. They have a key part to play in setting a positive data security risk appetite that runs across the whole firm.

2. Employee behaviour: How much do you control and know about the personal devices that your employees take into your office or have whilst working from home?

Employees are currently the most risk-laden entry points and the security of client data increasingly depends on their actions. Firms should work on modernising their Information Technology policies to include common practices such as BYOD. To achieve this, there needs to be an efficient communication channel for employees to regularly inform management about:

- What devices they are using;
- The level of encryption on these devices;
- Any loss or theft of personal devices;
- The volume and nature of information stored on a personal device. We recommend that firms evaluate the sensitivity of their data and ensure some remains in an appropriately restricted environment.

3. Assemble an Emergency Response team: Do you have a team on standby that can quickly respond to data breaches when they occur?

We advise that you prepare a list of either internal or external experts that will have responsibility to take immediate action once a breach occurs. This will require a range of expertise – ensure that representatives from IT, Risk, Legal as well as other departments are involved. Assembling a team before a breach happens gives you the time to train staff and conduct a thorough review of external contacts.

4. Form a PR plan: In the event of a breach, how will you ensure that you stay in control of public relations and be the first to communicate the story to stakeholders?

Social media provides a crucial communication channel between companies and their clients. It is recommended that you allocate responsibility to an internal or external PR team who can keep track of your data management initiatives to show that data security is a prioritised issue. In the event of a breach, the team can help you reach out to stakeholders and repair any reputational damage.

As one of the key risks to an organisation's long-term viability and reputation, companies must take action now to review and enhance their data management strategy.

Christine Moran
+44 (0) 20 3727 1368
Christine.Moran@fticonsulting.com

Ben Montgomery
+44 (0) 20 3727 1366
Ben.Montgomery@fticonsulting.com

Lea Cosic
+44 (0) 20 3727 1111
Lea.Cosic@fticonsulting.com

About FTI Consulting

FTI Consulting, LLP. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

www.fticonsulting.com