



Data Regulations White Paper

Are You Ready for the Regulators?

High profile fines have recently been imposed on individuals and companies for failing to protect electronic data - dramatic evidence that this is now a matter of personal concern for all senior managers, not just the IT director.

The quality, integrity and security of business records are now the direct responsibility of a company's Board of Directors.

The finance sector has been the first to come under powerful scrutiny from regulators; penalties have been imposed, where customers or staff have been judged to be disadvantaged by ineffective data management. The powers and scope of the regulators are being increased so that businesses in all sectors are likely to face increased scrutiny.

Data regulation is here to stay - what actions can you take to protect yourself and your business?



Background

The way that businesses interact with their customers, suppliers, staff and shareholders is reflected and held in its business data - an essential corporate asset which needs to be kept constantly under review, securely managed and protected.

Pressure from government, trade associations, shareholder bodies and regulatory authorities, like the Financial Services Authority (FSA) in the finance sector, is making the secure management of that data a primary corporate responsibility. Efficient archiving is also important - financial records have to be kept securely for a minimum of 5 years under the current requirements of Inland Revenue and this is likely to increase under EU legislation. For commercial reasons alone, it is vital that critical business data is safeguarded and business continuity solutions implemented - statistics show that of businesses that suspend trading for more than a day through lost data, only 45% survive at all.

Keeping data secure is important to businesses who, for any reason, find themselves involved in legal proceedings related to customers, suppliers or partners. Evidence of employees' actions is valuable protection - there is deterrence value in detailed evidence. Electronic records or emails can be vital in proving your case or defending an allegation.



Who pays the penalties?

Although the IT director or compliance director may manage the quality, integrity and security of corporate data, it is the Board that is held responsible. In a recent regulatory action against a major assurance company, Carol Sergeant, FSA Managing Director, said:

"This action demonstrates very clearly that the FSA will hold the senior management of regulated firms personally accountable for the way they run their businesses."

In other recent cases brought by the FSA, fines have been specifically imposed on Board directors and senior managers. Fines are only one part of the picture. Very often it is the damage to corporate reputation that brings the severest long-term penalties to a business. In the case of the FSA, it has the power not only to discipline authorized persons or individuals by public censure and fines but also suspend or remove a company from the industry.

Following an FSA fine on one major life and financial planning company "for record-keeping and associated compliance breaches", the business was taken over. In other examples, senior Director and Managers have been obliged to resign.



SME's are targeted

While many FTSE 100 businesses have already taken steps to secure their data, thousands of medium and smaller size companies are increasingly becoming the target of regulatory authorities.

According to The British Chambers of Commerce recent ICT Report, 67% of firms are concerned about the security aspects of doing business electronically. However only 49% of smaller businesses carry out an assessment of vulnerability compared to 93% of large firms.

Philosophy of regulation

The Financial Services Act is setting the pace for regulation of business data and the encouragement of best practice in data management. Once FSA standards have been set, companies in the finance sector have to comply with these standards or face penalties. Although the main purpose of the Act is to eliminate criminal practices and protect consumers from misleading data, as these primary objectives are met, standards continue to rise to encompass any lapse from best practice.

"Lapses in record-keeping are not the primary focus of the Financial Services Authority but very often the firms found to have inadequate record-keeping are also those whose practices have been found to be inadequate,"

says Oliver Lodge, formerly an FSA regulator and now Managing Director of Financial Services Consulting at Beachcroft Wansbroughs, providing regulatory and compliance advice.



Is the burden getting too heavy?

The British Chamber of Commerce is one of the organisations concerned about the overall levels of regulation affecting British business. Its 'Burdens Barometer' in 2002 already showed a heavy cost to business for fulfilling current requirements on data protection.

"One of the greatest burdens to business which has been added this year is the Data Protection Directive which up to May 2002 represented a burden on business of £3.1 billion."

However the Government's own Regulatory Impact Assessment (RIA), setting out the risks, costs and benefits of any new regulatory proposal, judges the compliance costs of data regulations as reasonable, judged against international levels of regulation:

The OECD report on UK Regulatory Reform in October 2002 said the UK's RIA procedures **"put the UK at the leading edge of OECD practices"**. It praised the UK's mature approach to regulation and its support of market openness and global competition. It also noted that UK entrepreneurs face a better business and regulatory environment than in most OECD countries.



Managing risk

While successful business managers are natural risktakers, there are some risks that regulators believe must be minimised absolutely.

Risk management is now part of modern corporate life. The Basel Committee on Banking Supervision has summarized operational risk as: **"the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events."**

As businesses become increasingly networked and commerce relies more heavily on electronic communication (both internal and external), so our businesses become more vulnerable to electronic failures, disruptions or loss of data. The current climate has an extensive and serious list of potential threats to business.

The table below identifies just some of the risks that Boards should consider when putting in place systems and procedures.

Internal influence External influence

Accidental erasure	Hacking
Malicious acts	Bomb
Software error	Fire
Application error	Flood
Hardware error	Virus
Vandalism	Power outage

In a world post 11 September 2001 and following the recent war in Iraq, the heightened threat of terrorist attack and use of 'dirty bombs', has increased the extent and magnitude of both external and internal risk.



Are you ready?

Most IT Directors are expected to have some plans or procedures to address these risks. However, the March 2003 Chartered Management Institute business continuity survey, published in association with the Business Continuity Institute and the UK Government's Civil Contingencies Secretariat, showed more than half of all managers admitted that either they did not have a business continuity plan in place or were unsure. Of the 46 % that did, only around half again had actually rehearsed its effectiveness during the past year. Of small businesses (up to £1 million turnover) only 24 per cent had a business continuity plan in place. In the face of such risk, international standards are driving the agenda on risk management and corporate data protection. Table 2 below, outlines the scope of some of these standards:

Regulation Main provisions:

ISO 17799 Affects all issues of security in business:

- protection of the integrity of software and information
- maintaining the integrity and availability of information processing and communication
- ensuring the safeguarding of information in networks and the protection of the supporting infrastructure
- preventing loss, modification or misuse of information exchanged between organisations

Data Protection Act Has 8 enforceable principles of good practice. Data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to countries without adequate protection

Regulation of Investigatory Powers Act Regulates the way that data must be protected from criminal use of IT and made available to

investigative

authorities. It covers data:

- integrity
- authentication
- confidentiality
- availability
- non-repudiation

Financial Services Authority Regulations for record-keeping cover details of every transaction for every customer over at least a 3

year

period and sometimes 6 years, or forever. Data covered by the Financial Services Authority includes:

- transactions with customers and all details related to them
- financial dealings with distributors and third parties
- financial adviser training and competence
- financial promotions
- customer complaints
- managing customers' assets
- reporting to customers
- dealing with trustees
- corporate arrangements
- money laundering checks
- business supervision and monitoring
- management control



What steps should company directors take?

There are a number of questions which Boards and IT Directors should ask themselves, such as: (i) Is it still appropriate to pass physical unencrypted tapes of my company's data to an employee or external courier? (ii) Should my corporate data reside in a central city location where, in the event that I cannot access that office, my business cannot continue? (iii) Can I save money by centralising servers and storage in a facility managed by an external provider with both expertise and economies of scale which I can use to my advantage?

There are also a number of straightforward steps that companies can follow to protect their data, minimize risk and reduce their IT cost at the same time. The infrastructure services provided by Tiver's / InTechnology and offered through its system integrator and reseller partners are specifically designed to address these concerns. Tiver's / InTechnology manages secure data storage services for certain UK government departments and other public sector clients including police and healthcare trusts. The cost-effective nature of the service is underscored by its use by organizations such as the Multiple Sclerosis Society and the National Housing Federation.

In the corporate sector, the service is advocated particularly by those who value highly their corporate data such as financial institutions, lawyers and media companies. and data can be accessed by staff working remotely, assuring seamless business continuity.

Data integrity, confidentiality and security is assured, meeting all current and likely future requirements of data regulations. Use of Tiver's / InTechnology Managed Services for assuring data security also has the potential for major cost savings. Investment in Managed Services for business continuity computing reduces IT management costs, improves efficiency and above all ensures that business continues unaffected in the event of significant disruption.