

Time for a fundamental change of thinking and behaviour

Background

There is an increasing awareness of the need for more effective corporate governance which is evidenced by the creation of legislation such as Sarbanes Oxley, and new industry-specific regulation such as MiFID in the European Union and HIPAA in the United States.

Much of this regulation has arisen as a result of seismic events such as the collapse of Enron or the recent difficulties in global financial markets. Inevitably, the pendulum swings from one extreme to the other as legislators react to media pressure as private investors suffer at the hands of poorly run companies.

Most recently we have seen the finger point increasingly at executives, with personal accountability of the CEO or CFO common in these new approaches, although the number of executives facing incarceration has largely been restricted to the United States.

Challenges

Having recognised that attempts by various bodies to impose greater transparency on markets, complex global business have enormous difficulty on achieving what is required of them. The complexity of the problem magnifies as a factor of sector, territory product and so on. In the absence of a formal, structured approach to governance, even to understand *what* has to be complied with is an almost impossible task, never mind the issue of *how*.

Not an IT problem

In such a situation, there is inevitable pressure to be seen to address the problem; but not unlike the issue of business continuity, there is often a misconception that the problem is one of the IT function failing to manage the issue - when in fact without senior management ownership and direction, the IT function cannot hope to effectively comply.

Current position

Having spent the last 30+ years sleep walking into our current state, maybe we should be clear where it has got us.

A glance at any newspaper of late will reveal the latest report of the loss of personal data by an organisation that claims the incident is a 'momentary lapse' of control. Those of us that understand the difficulty of the task know that is far from the truth.

The recent BERR report on information security breaches¹ makes for interesting reading. The uninformed and in the non-expert could be forgiven for thinking that 'everything in the garden is rosy', but despite the claims of executives and senior civil servants that everything is under control, this is not evidenced in day to day life.

Furthermore, has the approach taken to date made a tangible difference? One could suggest that if the efforts made to date had not been made, then the situation could be

¹ Department for Business Enterprise & Regulatory Reform – 2008 Information Security Breaches Survey

much worse, but that is of little consolation. A simple search on Google reveals over 100 hits for information governance, the vast majority being for the NHS and UK government.

Reasons for Failure

When presented with a complex business problem that has developed over several decades, it really doesn't matter how many technology-based 'sticking plasters' are applied, as they simply won't solve the problem.

To paraphrase Einstein, "the thinking that caused the problem is not the thinking that will solve the problem". In other words, unless we fundamentally change the way we approach the problem, we're wasting our time and money.

Furthermore, if we simply rely on the next gizmo to be the silver bullet that will solve the problem, we're not only deluding ourselves, but everyone else too. The solution is likely to involve the use of technology, but sound business thinking must come first.

Technology vendors are in the habit of seeing the world based on their product set. It's therefore no surprise, that when we discuss the topic of information governance and assurance that the vendors view it in terms of storage and backup. If, however you examine why these products were invested in, they have absolutely nothing to do with IA, they were designed to restore a particular configuration to a failed piece of hardware.

Unless you understand these kinds of issues, as the person responsible you are navigating very dangerous waters. Your ability to spend your multi-million budget *and* actually end up in compliance is limited. Without a sharp change in thinking; brought about by a new culture around the value of our information assets, and stiff penalties for non-compliance, we are unlikely to change the current situation.

In the limited space available in writing this paper it's not possible to cover all aspects of such a vast topic, but it's worth pointing out a few other areas worthy of consideration, including:

- There's currently no involvement in the business processes
- Training and awareness in the area of IA is almost non-existent
- It is common to do as little as possible to 'claim' compliance with governance
- Use of standards – do not 'do' process – just point inspections
- There are no real drivers – just embarrassing news items
- No real deterrent as the regulators can't or won't use their 'teeth'

What we really need

Before we can effectively manage data assets and gain a clear understanding of what our obligations are, we must start by classifying the data at the point of creation.

By doing this, a number of benefits accrue including:

1. Clarity over how and why the data was created at the point of creation – essential if it is ever to be used evidentially
2. Clarity over the value of the data based on the judgement of the business *not* IT
3. The ability to make informed decisions about legal and/or regulatory obligations in managing the data
4. The ability to manage the data itself based on management policy
5. The ability to control use of the data based on management policy, including the

- use of data outside of organisation
6. The ability to demonstrate to regulatory bodies and the courts that duty of care has been exercised by executives
 7. The ability to make better judgements of technology selection and use instead of based on technical features, functions and benefits which often do not align to the *true* business need
 8. Information governance must be consistent, practical, and auditable
 9. The Board of Directors and executives are personally responsible and accountable for information governance, which is then implemented by business units (including IT)
 10. Severe penalties should exist, that are enforceable and used
 11. Regulators who are able to, should use their powers to rebuild public confidence in a seemingly failing occupation, which exists to specifically safeguard the public

How to Achieve It

We would propose a 'top-down' approach to managing the problem, which must include:

1. Develop and implement a binding Bill of Rights and Responsibilities to protect all citizens
2. Put in place a framework for information governance. This allows the board to see, and comply with their obligations based on market and geography
3. Accountability and responsibility should go hand-in-hand. The board is the appropriate place for this and no abdication to the technology function must be allowed. This should stretch to named individuals having responsibility with clear penalties for failure, and with examples being made of firms and/or public bodies that fundamentally breach regulations
4. Carry out random, independent audits using properly certified bodies to ensure public confidence in the process
5. Sharpen the focus of those responsible by allowing those affected by data loss, or shareholders affected to sue for damages
6. Ensure traceability and personal accountability in all interactions
7. Use a risk driven approach to detect control requirements and ensure that the process is flexible enough to capture and manage new needs

Conclusions

In summary, we need:

- A digital 'Bill of Rights' that the ordinary person understands
- To move IA up the corporate and government agenda to drive education and action
- Ownership at board/minister level to drive down change through the organisation
- Ensure legal accountability and prosecution of those that flout the law
- Ensure traceability of interactions so should things go wrong, (which they sometimes will) proof can be provided of who is responsible, who the victim is, and hopefully allow mitigating action to be taken.