INTRODUCTION

'Can IT align with the business?'[1]

Your immediate response to this question gives a sense of the adequacy or otherwise of your IT governance arrangements. If you think it's a good question, one worth pursuing, then you've just identified the first, and most critical, symptom of inadequate IT governance: a disjunct between your most important business enabler and the business itself.

If you find the question incomprehensible – because, to you, it's axiomatic that IT aligns with the business – you may not need this book. However, before putting it aside, consider this: a late-2004 global study[2] of North American and European businesses found that only one-quarter of the respondents considered their business and IT strategies to be 'fully integrated and developed simultaneously' – which is a backward step from the findings of the same study in 2002, in which one-third of respondents considered these processes to be fully aligned.

Symptoms of inadequate IT governance

1. How does your board assess (measure) the real contribution made by any of your IT systems to improving the organization's competitiveness?
2. What divergence is there between the views that your sales/operational management has of the benefits of IT systems and projects and those of the IT management? Who is right and how do you find out? Are you getting maximum value (maximum business benefit for minimum actual total cost) for each of your IT investments? How would you know? How

[1] *Computer Business Review*, March 2005

[2] 'Why Today's IT Organization Won't Work Tomorrow,' AT Kearney, 2005

would you know if your IT spending is putting your company at a cost disadvantage?

3. What is your board's process for comparing the (fully costed) ROI on your technology projects to those of any other strategic options, including acquisitions, and how does this affect strategic planning?
4. What is your board's view on the relationship, in your organization, between the potential impact of a compliance or information security failure (in financial terms) and the (fully absorbed) cost of meeting the compliance and security objectives? What is the total actual (direct and indirect) cost of all the compliance and information security incidents in your organization in the last twelve months?
5. What is the real, financial value to your organization of its information and intellectual capital and how are you leveraging it?
6. How are you driving up the intellectual capital/headcount ratio? What's the relationship between this ratio and the IT intensity (IT investment to headcount) ratio?
7. Do all your IT projects come in on time, to budget and to specification?
8. How does your D&O insurance deal with the personal consequences for directors of IT failures arising from inadequate board oversight of core business processes and significant financial transactions?

If you organization has a clear, widely understood set of answers to these questions, complete with meaningful metrics, then you probably have an effective IT governance framework in place. The fact is, very few organizations do. There are a number of reasons for this.

Competitiveness

The first is that IT and IT governance simply don't feature on the CEO's top 10 list of challenges. Tighter cost control makes it in at number seven; transferring knowledge/ideas/practices within the

their organizations perceived information security as a CEO level priority.[9]

Is it therefore surprising that authorities are increasingly looking to regulation to force the issue up the agenda? 'The road to information security goes through corporate governance. America cannot solve its cyber security challenges by delegating them to government officials or CIOs. The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of boards and CEOs.'[10]

Directors' personal liability

Historically, the outside, or non-executive, directors of companies have been personally immune – financially, if not in terms of reputation – from the legal consequences of failure of the companies on whose boards they sit. A Stanford University study, for instance, found only four US cases, by 2003, where individual defendants had been forced to contribute personally to the settlement securities class actions.

However, in 2004, an ex-Chairman of Global Crossing made a substantial (US$30 million) personal contribution to settling a class action.

In January 2005, substantially all of the outside directors of both WorldCom and Enron agreed to settle class actions by contributing personal funds to the settlements. Ten Enron directors agreed to contribute an aggregate US$13 million; ten WorldCom directors agreed to contribute an aggregate US$18 million, which reportedly represented approximately 20 percent of their wealth. These personal contributions were in excess of the amounts provided by Directors and Officers insurance, which was exhausted by the cases.

While these settlements don't constitute an admission of liability or of wrongdoing by any of the settling directors (the cases are still, at

[9] Ernst & Young, 'Global Information Security Survey 2004'

[10] 'Information Security Governance: a Call to Action', US National Cyber Security Summit Task Force, April 2004

LONGER. Not much longer though: ICT makes revolutionary business models[18] possible and dramatically transforms the business environment. The fact that online security is an issue only slows down the speed with which online banking, financial services and other e-commerce applications develop, but the final outcome is not in doubt. The Internet does enable small businesses everywhere to compete with larger ones, globally; digital communication speeds up outsourcing, customer awareness and reputation destruction. Instant messaging, voice over IP, spyware and sequential auto-responders are technologies as disruptive as CRM (Customer Response Management), HRM (Human Resource Management) and ERP (Enterprise Resource Planning) systems were in their day. OF course, the Internet doesn't replace the need for a real business strategy, or for generating real economic returns for shareholders; it just transforms the environment within which the board has to create and execute strategy.

Guideline for Directors: *The board must ensure the organization's information strategy, IT systems and IT infrastructure are appropriate for its business model and strategic goals. A board which is not aware of how technology is transforming its business space, and which is not actively investigating how it can use technology to transform its own business (cannibalizing existing activities if appropriate) is a business for which some other organization is already creating a silver bullet.*[19]

---

[18] '[The term 'business model'] seems to refer to a loose conception of how a company does business and generates revenue. Yet simply having a business model is an exceedingly low bar to set for building a company. Generating revenue is a far cry from creating economic value, and no business model can be evaluated independently of industry structure. The business model approach to management becomes an invitation for faulty thinking and self-delusion.' Michael E Porter, 'Strategy and the Internet,' HBR, March 2001

[19] See *Leading the Revolution*, Gary Hamel, 2000

corporate governance have been adopted, mostly since 2002. These include Australia (2003), Austria (2002), Canada (2002), France (2002), Germany (*Kodex* – 2003), Italy (2002), Japan (2001), Netherlands (*Tabaksblatt*, 2003), and Switzerland (2002). These codes are all very recent, are all on a 'comply or explain basis' and, within a varied legal and cultural climate for compliance, there are widely varying levels of compliance.

The OECD principles were revised, following extensive consultation, and re-issued in April 2004. They identified six key areas in which a corporate governance framework should operate, including the protection of shareholders' rights, the timely and accurate disclosure of all material matters regarding the corporation, and that the board should be accountable to the company and the shareholders for providing strategic guidance and effective monitoring of management. The board should 'focus on long-term issues, such as assessing corporate strategy, and activities that might involve a change in the nature and direction of the company'.[33]

Guideline for Directors*: the board cannot meet this obligation without extending its corporate governance responsibilities to explicitly include information and IT.*

BIS and Basel 2

Banking failure can be more catastrophic than any other failure. Banking organizations need, for that reason, to go further in risk management terms than other commercial entities. In the banking world, an international accounting and risk management framework, driven by the Bank of International Settlements (BIS) has already emerged. BIS is the central banks' central bank. It exclusively serves central banks and other international organizations and its declared aim is to 'foster cooperation among central banks and other agencies in pursuit of monetary and financial stability'. In June 2004, the Bank's Basel Committee on Banking Supervision published its 'International Convergence of Capital Measurement and Capital Standards: a Revised Framework', which has become known as

[33] 'The OECD Principles of Corporate Governance'; policy brief, April 2004