Harvard Business Review

- ***Richard Nolan*** *(rnolan@hbs.edu) is an emeritus professor of business at Harvard Business School in Boston and a professor of management and organization at the University of Washington Business School in Seattle.*
F. Warren McFarlan *(fmcfarlan@hbs.edu) is a Baker Foundation Professor and the Albert H. Gordon Professor of Business Administration emeritus at Harvard Business School.*

Information Technology and the Board of Directors

Board practices for monitoring technology investments vary widely and often wildly. As technology's cost, complexity, and consequences grow, directors need a framework to develop IT policies that fit the companies they oversee.

by Richard Nolan and F. Warren McFarlan

Ever since the Y2K scare, boards have grown increasingly nervous about corporate dependence on information technology. Since then, computer crashes, denial of service attacks, competitive pressures, and the need to automate compliance with government regulations have heightened board sensitivity to IT risk. Unfortunately, most boards remain largely in the dark when it comes to IT spending and strategy. Despite the fact that corporate information assets can account for more than 50% of capital spending, most boards fall into the default mode of applying a set of tacit or explicit rules cobbled together from the best practices of other firms. Few understand the full degree of their operational dependence on computer systems or the extent to which IT plays a role in shaping their firms' strategies.

This state of affairs may seem excusable because to date there have been no standards for IT governance. Certainly, board committees understand their roles with regard to other areas of corporate control. In the U.S., the audit committee's task, for example, is codified in a set of Generally Accepted Accounting Principles and processes and underscored by regulations such as those of the New York Stock Exchange and Securities and Exchange Commission. Likewise, the compensation committee acts according to generally understood principles, employing compensation consulting firms to verify its findings and help explain its decisions to shareholders. The governance committee, too, has a clear mission: to look at the composition of the board and recommend improvements to its processes. To be sure, boards often fail to reach set standards, but at least there are standards.

Because there has been no comparable body of knowledge and best practice, IT governance doesn't exist per se. Indeed, board members frequently lack the fundamental knowledge needed to ask intelligent questions about not only IT risk and expense but also competitive risk. This leaves the CIOs, who manage critical corporate information assets, pretty much on their own. A lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would.

Understanding this, a small group of companies has taken matters into its own hands and established rigorous IT governance committees. Mellon Financial, Novell, Home Depot, Procter & Gamble, Wal-Mart, and FedEx, among others, have taken this step, creating board-level IT committees that are on a par with their audit, compensation, and governance committees. When the IT governance committee in one of these companies assists the CEO, the CIO, senior management, and the board in driving technology decisions, costly projects tend to remain under control, and the firm can carve out competitive advantage.

The question is no longer whether the board should be involved in IT decisions; the question is, how? Having observed the ever-changing IT strategies of hundreds of firms for over 40 years, we've found that there is no one-size-fits-all model for board supervision of a company's IT operations. The correct IT approach depends on a host of factors, including a company's history, industry, competitive situation, financial position, and quality of IT management. A strategy that works well for a clothing retailer is not appropriate for a large airline; the strategy that works for eBay can't work for a cement company. Creating a board-level committee is not, however, a best practice all companies should adopt. For many firms—consulting firms, small retailers, and book publishers, for instance—it would be a waste of time.

In this article, we show board members how to recognize their firms' positions and decide whether they should take a more aggressive stance. We illustrate the conditions under which boards should be less or more involved in IT decisions. We delineate what an IT governance committee should look like in terms of charter, membership, duties, and overall agenda. We offer recommendations for developing IT governance policies that take into account an organization's operational and strategic needs, as well as suggest what to do when those needs change. As we demonstrate in the following pages, appropriate board governance can go a long way toward helping a company avoid unnecessary risk and improve its competitive position.

The Four Modes

We've found it helpful to define the board's involvement according to two strategic issues: The first is how much the company relies on cost-effective, uninterrupted, secure, smoothly operating technology systems (what we refer to as "defensive" IT). The second is how much the company relies on IT for its competitive edge through systems that provide new value-added services and products or high responsiveness to customers ("offensive" IT). Depending on where companies locate themselves on a matrix we call "The IT Strategic Impact Grid" (see exhibit), technology governance may be a routine matter best handled by the existing audit committee or a vital asset that requires intense board-level scrutiny and assistance.


The IT Strategic Impact Grid

Defensive IT is about operational reliability. Keeping IT systems up and running is more important in the company's current incarnation than leapfrogging the competition through the clever use of emerging technology. One famously defensive firm is American Airlines, which developed the SABRE reservation system in the late 1960s. Once a source of innovation and strategic advantage, the SABRE system is now the absolute backbone of American's operations: When the system goes down, the airline grinds to a complete halt. Boards of firms like this need assurance that the technology systems are totally protected against potential operational disasters—computer bugs, power interruptions, hacking, and so on—and that costs remain under control.