Chapter 1

Governance Overview—How Do We Do It? What Do We Get Out of It?

1.1 WHAT IS IT?

Governance is simply the act of governing. The *Oxford English Dictionary* defines it as "The act or manner of governing, of exercising control or authority over the actions of subjects; a system of regulations."

The relevance of governance to security is not altogether obvious and most managers are still in the dark about the subject. Information security is often seen as fundamentally a technical exercise, purely the purview of information technology (IT). In these cases, the information security manager generally reports directly or indirectly to the CIO but in some cases may report to the CFO or, unfortunately, even to Operations.

In recent years, there has also been an increase in the number of senior risk managers, or CROs, and, in some cases, Information Security reports through that office. Although these organizational structures often work reasonably well in practice, provided the purview of security is primarily technical and the manager is educated in the subject and has considerable influence, in many cases they do not work well and, in any event, these reporting arrangements are fundamentally and structurally deficient. This contention is often subject to considerable controversy even among security professionals. However, analysis of the wide range of activities that must be managed for security to be effective and study of the best security management shows that it requires the scope and authority equivalent to that of any other senior manager. To be effective, security and other assurance activities are regulatory functions and cannot report to the regulated without creating an unten-

Information Security Governance. By Krag Brotby

able structural conflict of interest. Maintaining a distinction between regulatory and operational functions is critical, as each has a very different focus and responsibility. The former is related to safety and the latter to performance, and it is not unusual for tension to exist between them.

Part of the reason that the requirement for separation of security from operational activities is not evident is that the definitions and objectives of security generally lack clarity. Asking the typical security manager what the meaning of security is will elicit the shop-worn response of "ensuring the confidentiality, integrity, and availability of information assets." Pointing out that that is what it is supposed to do, that is its mission, and not what it is, generally elicits a blank stare. Probing further into the objectives of security will usually result in the same answer.

The lack of clarity about what security should specifically provide, how much of it is enough, and knowing when that has been achieved poses a problem and contributes to the confusion over the appropriate organizational structure for security. Lacking clear objectives, a definition of success, and metrics about when it has been achieved begs the question, *What does a security manager actually do*? How is the manager to know when he or she is managing appropriately? What is his or her performance based on? How does anyone know?

In other words, as in any other business endeavor, we manage for defined objectives, for outcomes. Objectives define intent and direction. Performance is based on achieving the objectives. Metrics determine whether or not objectives are being achieved.

1.2 BACK TO BASICS

If there is a lack of clarity looking ahead, reverting to basics may help shed light on the subject. Security fundamentally means safety, or the absence of danger. So in fact, IT or information security is an assurance function, that is, it provides a level of assurance of the safety of IT or information. Of course, it must be recognized that the safety of an organization's information assets typically goes a considerable distance beyond the purview of IT.

IT is by definition technology centric. IT security is by definition the security related to the technology. From a business or management perspective, or, indeed, from a high-level architectural viewpoint, IT is simply a set of mechanisms to process, transport, and store data. Whether this is done by automated machinery or by human processes is not relevant to the value or usefulness of the resultant activities. It should be obvious, therefore, that IT security cannot address the broader issue of information "safety."

Information security (IS) goes further in that it is information centric and is concerned with the "payload," not the method by which it is handled. Studies have clearly shown that the risks of compromise are often greater from the theft of paper than from IT systems being hacked. The loss of sensitive and protected information is five times greater from the theft or loss of laptops and backup tapes than it is from being hacked. These are issues typically outside the scope of IT security. The fact

that the information on these purloined laptops or tapes is infrequently encrypted is not a technology problem either; it is a governance and, therefore, a management problem.

To address the issues of "safety," the scope of information security governance must be considerably broader than either IT security or IS. It must endeavor to initiate a process to integrate the host of functions that in the typical organization are related to the "safety" of the organization. A number of these were mentioned in the Introduction, including:

- Risk management
- BCP/DR
- Project office
- Legal
- Compliance
- CIO
- CISO
- IT security
- CSO
- CTO
- CRO
- Insurance
- Training/awareness
- Quality control/assurance
- Audit

To this list we can add privacy and, perhaps more importantly, facilities. Why facilities? Consider the risks to information "safety" that can occur as a function of how the facility operates: the physical security issues, access controls, fire protection, earthquake safety, air-conditioning, power, telephone, and so on. Yet, risk assessments in most organizations frequently do not consider these elements.

The advantage of using the term "organizational safety" and considering the elements required to "preserve" the organization is that the task of security management becomes clearer. It also becomes obvious that many of the other "assurance" functions that deal with aspects of "safety" must be somehow integrated into the governance framework. It also becomes clear that most attempts to determine risk are woefully inadequate in that they fail to consider the broad array of threats and vulnerabilities that lie beyond IT and, indeed, beyond IS as well.

1.3 ORIGINS OF GOVERNANCE

It may be helpful to consider how the whole issue of governance arose to begin with to understand its relevance to information security. The first instance of the appear-

ance of corporate governance seems to be due to economist and Noble laureate Milton Friedman, who contended that "Corporate Governance is to conduct the business in accordance with owner or shareholders' desires, while conforming to the basic rules of the society embodied in law and ethical custom." This definition was based on his views and the economic concept of market value maximization that underpins shareholder capitalism.

The basis for modern corporate governance is probably a result of the Watergate scandal in the United States during the 1970s, which involved then President Nixon ordering a burglary of the opposition party's headquarters. The ensuing investigations by U.S. regulatory and legislative bodies highlighted organizational control failures that allowed major corporations to make illegal political contributions and to bribe government officials. This led to passage of the U.S. Foreign and Corrupt Practices Act of 1977 that contained specific provisions regarding the establishment, maintenance, and review of systems of internal control

In 1979, the U.S. Securities and Exchange Commission proposed mandatory reporting on internal financial controls. Then, in 1985, after the savings and loan collapse in the United States as a result of aggressive lending, corruption, and poor bookkeeping, among other things, the Treadway Commission was formed to identify main causes of misrepresentation in financial reports and make recommendations. The 1987 Treadway Report highlighted the need for proper control environments, independent audit committees, and objective internal audit functions. It suggested that companies report on the effectiveness of internal controls and that sponsoring organizations develop an integrated set of internal control criteria.

This was followed by the Committee of Sponsoring Organizations (COSO), which was formed and developed the 1992 report stipulating a control framework that was endorsed and refined in four subsequent U.K. reports: Cadbury, Rutteman, Hampel, and Turnbull.

Scandals and corporate collapses in the United Kingdom in the late 1980s and early 1990s led the government to recognize that existing legislation and self-regulation were not working. Companies such as Polly Peck, British & Commonwealth, BCCI, and Robert Maxwell's Mirror Group News International in United Kingdom were some of the high-profile victims of the irrational exuberance of the 1980s and were determined to be primarily a result of poor business practices.

In 1991, the Cadbury Committee drafted a code of practices defining and applying internal controls to limit exposure to financial loss.

Subsequent to the most spectacular failures in recent times of Enron, Worldcom, and numerous other companies in the United States, the draconian Sarbanes–Oxley Act of 2002 required financial disclosure, testing of controls and attestation of their effectiveness, board-level financial oversight, and a number of other stringent control requirements.

In January 2005, the Bank of England, the Treasury, and the Financial Services Authority in the United Kingdom published a joint paper on supervisory convergence addressing many of the same issues as Sarbanes–Oxley.

Currently, the global revolution in high-profile governance regulation has resulted in the following, among others: