CHAPTER **1**

Organizations as Submarines: Why Data Governance Is Imperative

> "Human history is more and more a race between education and catastrophe."
> —H.G. Wells

Until recently, data governance seldom merited serious discussion by corporate Directors. However, as the emergence of digital technologies and the Internet (and the advent of security risks that can have significant consequences) has drawn attention to information security), it caused corporate Boards to begin to raise these issues. Unfortunately, the primary approach has been one that follows the traditional paradigm of Director and Officer response to emerging risks in areas like corporate governance. Issues are targeted and briefed as risks are identified through litigation. This is an effective strategy where the scope of the risks is basically known. When Directors apply such an approach to information security in the use of information technology and the Internet, however, they are apt to focus too narrowly on known risks and to overlook the need to adopt a broader, comprehensive view of their company's data governance.

For the purposes of this Guide, data governance is defined as the "ongoing management of the risk of unauthorized collection, use, disclosure, transfer, modification, and/or destruction of information through physical, procedural, and technical security mechanisms."

Data governance is best understood as a combination of the concerns that emerge in connection with: (1) information security (managed by the chief security officer or CSO), (2) record or document retention (often managed by the Chief Financial Officer), and (3) data privacy (managed by the chief privacy officer).[1] Although "information

security" now appears routinely on Boardroom agendas, often as a high priority item,[2] the outcomes of such discussions can reflect serious misconceptions and misunderstandings about the nature of the risks to individual companies and their Directors. The responsibilities of various personnel with varying levels of technology expertise, different spheres of responsibility, and the tendency to address these issues "piece-meal" at the Boardroom level further contributes to concerns about the integrity and security of company data governance.[3] What is needed at the Board level is a unified approach. Evolving notions of responsible corporate oversight suggest that Directors need, at a minimum, to comprehend certain basic data governance principles, because they can ill-afford to overlook (or only belatedly appreciate) rapidly evolving risks and exposures.[4]

Those Directors who defer or delegate to specialized personnel their understanding and command of data governance will be at increasing risk of incurring personal liability for failing to fulfill their fiduciary duty of care to ensure that their companies comply with rapidly emerging legal requirements concerning deficiencies in data governance.

When corporate information technology systems suffer damage as a result of vulnerabilities or security breakdowns (referred to hereafter as "incidents"), the costs may range from hundreds of thousands to millions of dollars (including disruption and diagnostic costs as well as ruined or irretrievable data).[5] Such incidents may be caused by unauthorized external access, or carelessness by innocent, well-intentioned personnel, or by insiders exploiting unsuspected vulnerabilities or whose correction had been postponed.

The advent of information technology and the Internet (referred to hereafter as the "Digital Era") has brought about profound changes in risk management, asset protection, and internal reporting. Such changes have occurred because companies have relinquished the relatively static, predictable, and easily controlled conditions of hard copy records for the dynamic, less predictable, and more difficult to control conditions of digital or electronic records.[6] Because of these changes, Directors often misunderstand key aspects of data retention and protection. Because many firms "assets" are increasingly indistinguishable from its stored information, the integrity of the mode of storage is an integral part of the preservation of its "value." Failure to be aware of this or sufficiently concerned with the integrity of stored information can leave

the firm's information assets vulnerable to unauthorized access, misappropriation, modification, damage, or destruction.

Today, a failure to provide appropriate data governance can become a crisis that rapidly undermines the integrity and reputation of the organization. In an environment of increased media attention to privacy and security, the magnitude of "headline" risks and the corresponding loss of the goodwill of customers, partners, regulators, and other stakeholders can have an immediate and profound "bottom line." To the extent information security is seen as a component of critical infrastructure protection in a post 9/11 environment, data governance is also increasingly treated as a critical and integral part of national security.

One tenet of this book is that Directors should adopt data governance standards, both for themselves and their organizations, that exceed what a strict reading of the law today appears to require. For risks that change gradually, when Boards have ample time to respond, there is little need or benefit to push an organization's legal compliance "ahead of the curve". This is especially so when organizations struggle to meet minimum compliance requirements and we can empathize with Directors who simply want to do what regulators may now require. Most Boards may well "be happy if they felt that they had, for just one brief shining moment, 'caught up' with accepted, mandatory legal requirements."[7]

Where technological risks evolve at an increasingly rapid pace being "caught up" will leave an organization far "behind the curve", reacting belatedly to problems, incurring high costs in damage control, as well as financial and reputational loss. As many companies have learned from late attempts to comply with Sarbanes Oxley, a prudent, early investment to get "ahead of the curve" would have positioned them to reap substantial savings on "best practices" and spared them the need to disclose in an annual report the existence of "material weaknesses in internal controls."

We believe it "penny wise and pound foolish" for a Board to settle for a narrow reading of laws and accept minimal improvements in compliance in areas where the trend among regulators is to adopt ever-more stringent readings of legal requirements. Any perceived "getting ahead of the curve" now simply means "less catch up" later and the avoidance of risk and/or loss in the interim. Board consideration of "data governance" is only just beginning and addressing framework questions now with foresight and a determination that "best practices" should exceed

minimal legal requirements will ensure Directors fulfill their personal obligations and corporate duties.

This Guide is intended to help Directors fulfill their obligations by providing them with some practical questions for ensuring the management of inherent risks and emerging foreseeable threats.

In Chapter Two, we review the impending "perfect storm" in the information security environment. We identify seven trends that contribute to its formation, its breadth and intensity, and the severity of its consequences for organizations and their Directors. Chapter Two makes the case that data governance must become a high priority for Directors; and Chapter Three explains why data governance will remain a high priority for Directors for the foreseeable future. In Chapter Three, we review the data governance issues that most warrant Directors' attention. We explain changes in digital asset protection and internal reporting that affect Directors' fiduciary duties and create legal obligations that can expose them to increased risks of personal liability. We highlight the applicable requirements (referred to in this Guide as "drivers"), which we believe create positive obligations and which, if not properly addressed, will be a source of potential liability for Directors. Chapter Three concludes with a summary of key points that are synthesized into a recommended list of priority issues that Directors should explore each time they review internal reports on data governance, specifically in relation to reports that assess and attest to internal controls for financial reporting by their organization and its outsource service providers.

Chapter Four proposes key lines of inquiry that Directors should pursue to assure themselves that data governance receives sufficient attention by supervisory personnel within their organizations. Our premise is that Directors cannot simply adopt the reports prepared by technical personnel or executive officers concerning the enterprise's information security without risking fiduciary liability. Evolving case law and legislation reveals a strong trend toward an increasing Director and Officer obligation to know more and toward increasing categories of "duties to know" that are "non-delegable." This Guide adopts the view that Directors both need to ask specific questions and to be less willing to accept on face value initial answers. This will facilitate their moving quickly up the learning curve of what they need to know effectively to supervise their company's data governance.

We emphasize that for an enterprise to succeed at efficient data governance, its Directors must perceive the effort as a continuous process designed not simply to identify imminent risks and to anticipate emerg-

ing threats, but also to avert, wherever feasible and practical, unauthorized access to or misuse of the enterprise's information assets. When incidents occur, as they inevitably will in the best-managed enterprises, it is necessary to detect each promptly, to mitigate damages and prevent their spread, and to improve security to reduce the probability of a reoccurrence. Success in this endeavour is a daunting task for management. And shareholders and enforcement agencies will increasingly scrutinize its oversight by Directors as the information technology transformation continues to mature.

We believe it would be useful for Directors to adopt a dynamic image of their Company that accurately reflects the need to safeguard valuable but highly mutable information assets. Companies are increasingly less like "castles" with their Boardroom's citadels enjoying a clear view of the far horizons and of approaching attackers. In their use of information technology in daily operations, the companies of the 21st century more often resemble a modern submarine, dependent upon computer systems and continuous scanning to protect against incoming threats. The Boardroom is more like a "conning tower" or bridge. Like a sub captain, a Director must develop the expertise to evaluate the information provided by his Company officers in order to clarify the status of the ship.

Changing this paradigm will prepare Directors to treat Company security needs as a high priority and as an on-going concern. It will also permit a well-prepared "damage control" team to identify potential threats quickly, to select the most effective means to contain the damage promptly and to avoid putting the ship and its enterprise in peril. It will help Directors to address the inherent conflict in managing information security—namely that "the compelling desire to achieve [information security] co-exists with an equally compelling desire to enjoy its achievement without further investment of funds or vigilance."[8]