Management Online REview

Information Integrity in the Digital Age: A Challenge for the Board

Madhavan Nayar, Eric G Flamholtz

Abstract

For most organizations, the information explosion of the mature Digital Age has made current approaches to Information Integrity (the accuracy, consistency, and reliability of the information) obsolete. This article details extrinsic and intrinsic information errors and their impact, and spells out the need for effective real-time automated information controls. Implications for Boards of Directors include taking on greater responsibility for internal controls in order to achieve Information Integrity.

Keywords: Information integrity, Information explosion, IT, Information controls, Boards of directors.

Introduction

History is replete with examples of technologies which disrupt the existing world order in many fields of endeavor. For example, over the centuries, cavalry had been the source of strategic advantage in warfare. However, in 1939, when the German army invaded Poland, they were met by the Polish cavalry. Proud, skilled and brave horsemen, the Polish cavalry charged the advancing German army, which was armed with tanks with mounted machine guns. The carnage that ensued demolished the Polish cavalry and made clear its obsolescence.

Ever since the advent of the public corporation, Boards of Directors have played the vital role of stewards of the shareholders' interests. In that role, their primary functions are oversight and decision making. The decision making function concerns the formulation of corporate policy, selection of senior management, review of strategic and business plans, and a variety of other matters. The oversight function involves the ongoing monitoring of corporate business and activities, and in particular, compliance with legal obligations and regulations.

The Presumption of Information Integrity

Boards have depended on the information provided, primarily by senior management, to base their decisions and carry out their responsibilities. It has been assumed, for the most part, that such information is dependable and trustworthy, and that management has implemented appropriate controls in the information systems and processes to ensure Information Integrity – the accuracy, consistency and reliability of the information. Additionally, Boards have relied on the system of internal controls, including internal audits, and the external auditors for the assurance of Information Integrity.

In the wake of scandals at Enron, WorldCom and a host of other marquee companies, the Boards of Directors of public corporations are under siege from shareholders and regulators. The information they give the shareholders and regulators has become suspect, and in some instances, been proven to be wrong, misleading or false. The Boards have suffered as a result of the fragmented, *ad hoc* and inadequate approach to Information Integrity that is prevalent in most organizations. The internal control systems aimed at assuring Information Integrity, more often than not, are held together by a patchwork of manual processes, embedded controls and obscure audit trails The Boards of Directors of today's public corporations are fighting a new kind of 'war'. They are fighting the 'Information Integrity war' with antiquated concepts and tools much the same way the Polish cavalry met the German army in World War II!

The thesis of our article is that the coming of age of the Digital Age has made the current approaches to Information Integrity in most organizations obsolete. The Board of Directors should mandate that senior management deploy effective, automated information controls across the enterprise to assure Information Integrity.

We shall examine how the maturing of the Digital Age is creating an 'information explosion' and causing a fundamental shift in the role of information in the modern corporation. Together, these two trends are exacerbating certain inherent risks of information errors and Information Integrity failures for businesses. We shall discuss the impact of information errors, such as increased operational costs, loss of market share, regulatory fines and penalties, loss of reputation, lower market valuation and even business failure. We will discuss the use of effective automated information controls for achieving Information Integrity.

We will conclude the article with a few specific actions that the Board can take to win the 'Information Integrity war'.

The Information Explosion[1]

The fastest increasing quantity on this planet is the amount of information we are generating. It is (and has been) expanding faster than anything else we create or can measure over the scale of decades. Information is accumulating faster than any material or artifact in this world, faster than any by-product of our activities. The rate of growth in information may even be faster than any biological growth at the same scale.

Recently two economists at UC Berkeley calculated our total global information production for one year. In their study "How much information?" researchers Hal Varian and Peter Lyman measured the total production of all information channels in the world for two different years, 2000 and 2003.[2] Varian and Lyman estimate that the total production of new information in 2000 reached 1.5 exabytes. They explain that is about 37,000 times as much information as is in the entire holdings Library of Congress. For one year! Three years later the annual total yielded 3.5 exabytes. That yields a 66% rate of growth in information per year.

The information explosion has important implications. As a society, we are doubling the total volume of information every two years. The quantity of information that businesses are capturing, processing, storing and sharing is growing exponentially as well. Unfortunately, the integrity of much, if not most, of that information is unknown, if not suspect.

The Changing Role of Information

With the advent of the first Industrial Revolution, some 200 years ago, it became necessary to establish a system of controls to monitor and report business activity. The resources of the industrial age were tangible things that could be mined, processed, bought, sold, managed and easily understood,[3] and the 'physical' organization and operation – customers, suppliers, people, processes and resources – were visible, identifiable and accessible. The task of monitoring and reporting was comparatively simple and straightforward. It was possible to establish internal control systems to physically observe and manually verify the veracity of the information presented by management.

The global economy is currently in the midst of a *second* Industrial Revolution. This second Industrial Revolution has spawned the Digital Age. It is built on electronic software and hardware, widespread access to the Internet, and the electronic exchange of information for a variety of purposes. It is now possible to process and store immense quantities of data at ever faster rates. This has allowed the gathering of a previously unimaginable amount of detail data about every aspect of the business.

In this environment, the 'physical' organization and operation – customers, suppliers, people, processes and resources – are becoming less and less visible, identifiable and accessible. Instead, they are represented by the information in data warehouses, ERP systems, corporate intranets and spreadsheets. Consequently, the business has to be defined, analyzed and assessed through an "information proxy," the representation of the physical environment in the information environment. Thus information is rapidly becoming a surrogate for the real tangible world.

Information is becoming a virtual world unto itself. This poses new and unique challenges and requirements. This means that decisions must be based upon information rather than observable tangible phenomena. It also means that if and when errors in information occur their significance is magnified.

Information Errors: An Inherent Risk for Every Enterprise

We are all familiar with the phenomenon of information errors. On a personal level, we may have experienced it at the bank, in the supermarket or in dealing with the insurance company. Occasionally we come across headlines in the newspapers and stories in the media. However, reports in the media only reveal the "tip of the iceberg" of all the errors that occur. Only a small fraction of the failures that actually happen are reported. No company or organization wants its name associated with a mistake. For every error reported, there probably are hundreds more that are detected and corrected. And for every error detected, there are many more that go undetected.

Information errors are a pervasive phenomenon in business because every enterprise is inherently exposed to certain extrinsic and intrinsic information-related risk factors.

The extrinsic risk factors are *change, complexity, communication, conversion and corruption.*

1. **Change.** No organization is immune to changes in, organizational structure, regulations, hardware and software and people. All such changes increase the probability of system failures and information errors.
2. **Complexity.** Information environments in organizations are becoming more complex due to increasing data volumes and processing speeds, distributed software and system interfaces and new functions and features demanded by business and regulatory imperatives. Complexity, by definition, introduces the potential for failure. Increased complexity increases the probability of information errors.

3. **Communication.** Widespread deployment of the internet and distributed processing and the availability of high-speed, high bandwidth communication links require the information environments of most organizations to share data across the enterprise and with partners. All such communications are susceptible to failed, incomplete or duplicate transfer of information and therefore information errors.
4. **Conversion.** Conversion of data from one format to another, from one medium to another or one system to another is an integral aspect of every information environment. As such, conversions are susceptible to information errors due to deficiencies and defects in software and processes.
5. **Corruption.** Errors are introduced due to accidental system and process failures as well as deliberate and fraudulent alteration or tampering of systems, processes and data. All information environments are prone to accidental failures. Many are susceptible to fraudulent intrusions. Hence information error due to corruption is an inherent risk.

The intrinsic risk factors are *Design Errors, Development Errors, Deployment Errors, Detection Errors and Data Errors*.

1. **Design Errors**: Design errors are caused by incomplete or incorrect specification of requirements, faulty design reviews and walkthroughs and environmental or other changes during the development and deployment.
2. **Development Errors**: Development errors are caused by poor development methodologies and incomplete or incorrect testing.
3. **Deployment Errors**: Deployment errors are caused by inadequate or incomplete controls.
4. **Detection Errors**: Detection errors are caused by failure in manual or automated controls to detect information errors or wrongly identify errors when they do not exist.
5. **Data Errors**: Data errors are caused by erroneous input and incorrect or incomplete edit and validation controls.

Impact of Information errors

We know anecdotally that the economic impact of information errors is huge. However, there have been few in-depth studies or reports about the economic impact of information errors. Some illustrations of the consequences of information errors include:

- When public companies have to issue revised financial reports to correct information errors, we often observe dramatic drops in the share price and market capitalization of the companies involved.

- Many person hours and positions are dedicated to verifying the accuracy and completeness of information before it is reported to the public. Systems of checks and balances are dedicated to monitoring and detecting information errors.

- When errors occur, companies often have to incur expensive research costs to identify the cause of the error and correct the problem.

An Example of the Cost of Information Errors: The Telephone Industry

The types of costs that businesses incur from information errors can be illustrated by the telephone industry. This problem is so pervasive that industry has a name for revenue lost due to missing or erroneous data: "revenue leakage." In fact, most phone companies have vice presidents and departments for revenue assurance. It has been conservatively estimated that phone companies lose 5-10% of their revenue due to information leakage.[4]

This problem is broader than just the telephone industry. The Information Integrity Coalition, a non-profit organization, estimates that, on average, organizations spend between 1-5% of their revenue in resources and activities aimed at preventing, monitoring, and verifying, detecting and correcting errors.[5] If these estimates are correct, it means that Citigroup, for example, may be spending between 1 and 5 billion dollars, Wal-Mart between 1.9 and 9.5 billion dollars, the US Government between 20 and 100 billion dollars, and the Fortune 1000 as a whole between 80 and 400 billion dollars as the opportunity cost of information integrity errors.

Inadequacies of the Current Approach

Our current approach to dealing with information errors is fragmented, *ad hoc*, and unscientific. We currently approach information errors as security, audit and controls issues. We assume software engineering will solve the problem. We invest in hardware, software, people and time for backup and recovery of our data and systems. We have almost everyone manually verifying all kinds of information. When errors do happen, we often blame it on human failure.

Since the beginning of the so-called Information Revolution, much of the focus has been on *technology* rather than information. Shouldn't the Information Revolution be more about information than about technology? Our knowledge of what makes information trustworthy and dependable does not seem to be based on science and theory . We don't even have a common language to describe or discuss the problem, let alone the solution. For example, we use the terms "data" and "information" interchangeably. We refer to information quality, accuracy, integrity, consistency and reliability as if they are all the same. During the past decade there has been increasing attention to this problem. This has led to a new framework for understanding and viewing Informational Integrity. Although an in-depth discussion of this framework is beyond the scope of this article, one of the key ideas is the need for real time automated information controls.

Automated Information Controls

Modern enterprises are becoming "information refineries" A refinery receives various types of raw materials, processes them, stores the outputs and delivers the refined products to its customers. An information refinery receives various types of data, processes the data, stores the outputs and delivers the results to a variety of internal and external stakeholders. The operation of a refinery and the quality of its inputs, processes and outputs are continuously monitored by an integrated system of automated controls. The information refinery should similarly have a system of automated information controls. What is required is a system of real-time information controls that automatically monitor and verify information throughout its lifecycle, and detect and manage information errors when they do occur. Some of these solutions already exist, while others require development.

Effective real-time automated information controls can prevent information errors, ensure Information Integrity and yield many important benefits to the enterprise such as:

1. **Increased Operational Efficiency**: Automation of manual verification, standardization of information controls and elimination of unnecessary delays in processes increase operational efficiency which translates to better resource use, reduced cycle time, and increased customer satisfaction.
2. **Increased Profitability**: Automated information controls increase profitability by reducing operational costs in many different ways: elimination of manual labor, prompt detection of errors, faster resolution of errors, and lower refunds and write-offs. Profitability is also

increased by protecting an organization's revenue through prompt detection and prevention of revenue leakage and the capture of unbilled revenue.

3. **Regulatory Compliance**: Automated information controls, because they are consistent, standardized and verifiable, simplify and speed up internal and external audits. They also ensure that the information provided to the regulators is accurate, consistent, and reliable.
4. **Protection of Reputation**: Some information errors can be catastrophic because they can result in damaging headlines in the media, severe penalties from the regulators or significant erosion of the market value of the business. Automated information controls help detect and prevent catastrophic Information Integrity failures.

Conclusion

What does all this mean to the Board of Directors? The Board of Directors has two major functions: 1) oversight (governance) and 2) decision-making. The decision making function concerns the formulation of corporate policy, selection of senior management, review of strategic and business plans, and a variety of other matters. The oversight function involves the ongoing monitoring of corporate business and activities, and in particular compliance with legal obligations and corporate policies.

In the wake of the scandals at Enron and other companies, where shareholders lost many millions of dollars, the U.S, Congress passed the Sarbanes-Oxley Act of 2002[5]. As directed by this legislation, the SEC adopted rules that require conformance with specific sections of the Act. Under Sarbanes-Oxley, the chief executive officer and chief financial officer of public companies are required to review, and based upon their knowledge, certify that quarterly and annual reports are materially accurate and complete. In addition, quarterly assessments of the disclosure controls and procedures as well as annual assessments of internal controls over financial reporting are also required.

Given current trends towards increased demands of corporate governance, Sarbanes-Oxley and the tenor of the times, the role of the Board of Directors needs to change to require even more emphasis on anything to do with internal control. Specifically, Eisenberg has proposed that the role of the Board be changed from a "monitoring model" to one that takes greater responsibility for internal controls.[6] At the very least, the Board needs to exercise its oversight function by serving as a catalyst for management to perform assessments of the disclosure controls and procedures as well as annual assessments of internal controls over financial reporting to ensure that information integrity has been achieved. This, in turn, will require new tools for the continuous validation of electronic information.

What is the bottom line of this paper for the Board? In brief, the implications for the Board are:

1. The Digital Age is causing an unprecedented explosion in information with serious consequences;
2. Information is rapidly becoming a surrogate for the physical enterprise and its activity;
3. Absent effective enterprise-wide measures to ensure Information Integrity, the Board may be making assessments and decisions based on erroneous, misleading or deliberately false representations from senior management;
4. The onus for mandating the assurance of Information Integrity rests with the Board; and
5. Senior management should be tasked with the deployment of a comprehensive system of independent, real-time automated information controls throughout the enterprise.

If we do not re-arm ourselves with tools suitable for today's digital information environment, the results of the Information Integrity War is destined to be the same as the fate of the Polish cavalry.

We are hopeful that public corporations will respond to this challenge, with the charge led by their Boards of Directors.

References / Footnotes:

[1] Kelly, Kevin, "The Technium." http://www.kk.org/thetechnium/archives/2006/02/the_speed_of_in.php
[2] Lyman, Peter and Hal R. Varian, "How Much Information," 2003. Retrieved from http://www.sims.berkeley.edu/how-much-info-2003 on 11/10/06.
[3] Cleveland, Harlan, "Information as a Resource." Futurist. December 1982.
[4] Deloitte & Touche, 1998, *First Revenue Assurance Survey.*
[5] Information Integrity Coalition, *www.informationintegrity.org*
[6] Melvin A. Eisenberg, "The Board of Directors and Internal Control," Cardozo Law Review, Vol. 19, Nos. 1-2, Sept-Nov. 1997, pp. 237-264.

MADHAVAN NAYAR
Infogix Inc., 1240, East Diehl Road, Suite 300, Naperville, Illinois, 60563, USA.
e-mail: Mnayar@infogix.com

Madhavan Nayar is Founder and Company Leader of Infogix (formerly Unitech Systems), a leading provider of Information Integrity solutions. He has taught at graduate business schools such as Kellogg, and holds annual prizes for Entrepreneurship and Information Systems.

ERIC G FLAMHOLTZ
Anderson Graduate School of Management, UCLA, 405 Hilgard Avenue, Los Angeles, CA 90024-1481, USA.

Dr Eric G Flamholtz is Professor of Management at UCLA and President of Management Systems Consulting Corporation which he founded in 1978. A prolific author, his latest book is Leading Strategic and Organizational Change, *Cambridge University Press (forthcoming).*