University of Dayton
eCommons

Accounting Faculty Publications

Department of Accounting

2-1-2013

The Importance of Information Integrity: In a Data-Driven World, Unreliable and Inaccurate Information Can Lead to Bad Decision-Making

Sridhar Ramamoorti
University of Dayton, sramamoorti1@udayton.edu

Madhavan K. Nayar

Follow this and additional works at: https://ecommons.udayton.edu/acc_fac_pub

Part of the Accounting Commons, Business Administration, Management, and Operations Commons, Business Law, Public Responsibility, and Ethics Commons, Corporate Finance Commons, and the Nonprofit Administration and Management Commons

The Importance of Information Integrity

In a data-driven world, unreliable and
inaccurate information can lead to bad decision-making.

Sridhar Ramamoorti and Madhavan K. Nayar

What is information integrity? It is the trustworthiness and dependability of information. The credibility of information depends on whether we are getting it from sources we can trust. After all, the value of information to the decision-maker and problem-solver consists first in its integrity, and then in its usefulness and usability. Why? Because, even the best chef knows that you can't make a good omelet out of bad eggs!

Consider the emerging trend of big data (see "Big Data" on page 34). According to IBM, people create 2.5 quintillion bytes of data every day (a quintillion is 1 followed by 18 zeroes), and research from International Data Corp. suggests that the world's data volume is doubling every two years. So what are organizations going to do about this unfathomable data accumulation? Many have started performing comprehensive data mapping but have encountered boundary problems such as the complexity of a "bring your own device" environment and accounting for data resident in legacy systems, laptops, and USB drives.

Given today's digital information environment, the understanding, definition, and analysis of information integrity can be challenging and complex. Organizations may be rapidly approaching a point at which they will be creating, processing, storing, sharing, and using so much data so fast that it will be impossible to prevent massive information integrity failures in sufficient time. Undetected and uncontrolled, such failures are likely to create information errors, disrupt processes and systems, and pollute the information environment. Clearly, there is an urgent need to establish standards for information integrity and to form interdisciplinary teams to develop effective means to apply those standards.

Internal auditors can be an important part of such interdisciplinary and cross-functional initiatives. Their familiarity with the progress of these initiatives positions them to evaluate the adequacy of internal controls pertaining to information integrity risks. Moreover, their involvement in the broadly defined governance, risk management, controls, and compliance mandate allows them to be the ideal vehicle for educating people throughout the organization about information integrity risks.

Integrity Failures

Corporate governance failures can be viewed through the prism of information integrity, as executives and boards use information to make decisions. Information failures can be traced back to information errors, ethical lapses, integrity failures,
or a combination of these factors. Information errors arise due to decision-makers receiving or using incomplete or unreliable information; decision-relevant information being unavailable;

available information being irrelevant, non-actionable, or non-understandable; or reliance on stale information arising through a variety of inadvertent, process-based causes. Also falling into this category would be the law of unintended consequences, whereby the right information is not available when it is supposed to be. Integrity failures also occur whenever information ends up being massaged or manipulated deliberately, bias is introduced purposefully, and people act unethically or fraudulently to shade information or make outright misrepresentations or fabrications. Given this backdrop, a careful root-cause analysis of any corporate governance failure — frequently involving fraud allegations — will lead to the inevitable diagnosis: information errors, integrity lapses, or both.

Two key observations can be asserted with reference to a framework for ensuring the integrity of information:

- An information problem may or may not be an integrity problem; nevertheless, depending on its size and other ripple effects, it could lead to an information integrity failure. The significance of the information error generally is measured quantitatively: It is a question of the magnitude of the error (i.e., by what order of magnitude are the estimates wrong? What is the margin of error?). There could be qualitative considerations, too. Thus, decisions based on faulty economic and market assessments about the pricing and sales of a product in a foreign jurisdiction could jeopardize the entire operation in that location, for example.
- An integrity problem will almost always result in an information problem, and thus, sooner or later will lead to an information integrity failure. It is not a question of if, but when, a person with questionable ethics will choose to misrepresent something. With respect to the recent wave of insider trading prosecutions, consider that the individuals prosecuted were simply waiting for the opportunities to exploit non-public, market-moving information to their advantage. The significance of behavioral and integrity risks is mostly a qualitative judgment, for one cannot trust somebody who is honest only 99 percent of the time. What if your transaction is the one out of 100 in which the counterparty acts in bad faith?

Accounting and audit standards have used the terms *relevance*, *reliability*, and *timeliness* of information when considering internal control systems. These are a subset of an evaluation of information error characteristics. However, considering recent ethics and integrity lapses in the C-suite and among managers, internal auditors also must pay equal, if not greater, attention to behavioral and integrity risks. Internal controls cannot remain "people-neutral" in such a context; they must explicitly factor in the risk of a manager exploiting a conflict of interest or colluding with an outside third party to defraud the organization. Internal auditors also can advise management and the board on the nature, scope, and potential significance and impact of such information integrity risks.

What Are the Implications?

In the final analysis, internal control frameworks primarily are designed to address information integrity risk and reduce it to an acceptable level. While most of these are excellent process-

based frameworks, they can be embellished further by considering behavioral/integrity risks. People-neutral internal controls stand little chance of stopping a well-motivated fraudster; the universe of irregularities is far greater than the controls organizations can conceive of and implement beforehand, so auditors are always playing "catch up."

The concept of information integrity provides a comprehensive framework and foundation for internal auditors to recognize how best to characterize this important risk. Once the sources of information integrity risk are understood, internal auditors can evaluate better the adequacy of internal control systems within their respective organizations. Information integrity risk has relevance to preventive, detective, and corrective controls. In the long run, internal control systems that have been designed and implemented using the concept of information integrity are much more likely to be robust and effective, as they would incorporate both the "information" and the "people" dimensions of decision-making.

Sridhar Ramamoorti, PHD, CIA, CPA, CFE, is associate professor of accountancy and director– Board Culture & Behavioral Dynamics at the Corporate Governance Center at Kennesaw State University in Georgia.

Madhavan K. Nayar is president at E-Prairie LLC in Naperville, Ill., which supports and invests in ventures focused on sustainable information ecosystems.