



How CFO's Should Tackle Information Management

By Robert P. Green, CPA.CITP

Published by Financial Executive Magazine, December 2007

Consider the strategic value of your business information. Where is it in the hierarchy among your key assets? Is it first or second? Between information and employees, you should have numbers 1 and 2 sewn up!

Businesses win coveted, well-publicized awards for best practices in how they manage their work environment and take care of their employees. Know of a company that's been rewarded for being exemplary at strategically managing and making the most of its information? Likely not. Yet, the practices that manage information, like people management, can have a dramatic impact on the success — or failure — of any business, big or small.

Strategic information management practices and methods, although often considered the responsibility of the chief information officer (CIO), have evolved to a point where they should be evaluated and implemented with the blessing and guidance of the CFO. This is not withstanding the fact that publicly traded companies must involve the CFO in this activity due to the Sarbanes-Oxley Act of 2002.

If your business is like most, it relies on its information technology (IT) department, CIO and/or chief technology officer (CTO) for most anything technological. That's well and good, but, in addition, from a fiduciary perspective, the CFO should be involved in key decisions, and he or she needs to play a driving role in creating an information management (IM) strategy.

'Information Management' and the CFO Role

IM involves mature, executive-sponsored practices to address how information serves a business and how a business serves its information. This is a top-down strategy, seeking to glean the value from IT and not support IT for the sake of IT. It starts with a focus on determining specifically what information is key to the success of a business.

The result is an executable strategic IT plan that addresses how, when and where to capture, store, process, secure and use digital information. Such a plan is a roadmap, with the directions being provided by IM considerations and actions.

Many growing, dynamic businesses don't take time to prepare strategic IT plans, much less consider the valuable "what, how, when and where" considerations. Such planning and related projects are often deemed of minor importance and delegated to the IT staff, and often without input from management.

The lack of priority towards IT planning can be most evident when considering the pervasive lack of disaster recovery and business continuity planning and management surrounding key business information. In the opening question regarding information and employees, surely, Human Resources (HR) departments go to great lengths to provide for the safety of employees in the event of a disaster. But often, similar plans for information protection and business systems resumption following a disaster are far less comprehensive, and not often put to a legitimate test.

The CFO can change or mitigate most all of this, when exercising his or her fiduciary responsibility. Yes, it takes time and money to develop IM practices and strategic IT plans; however, the CFO has the power and insight to characterize the process as more of an opportunity, thereby differentiating the businesses from others. This action can allow the company's information to become the valuable, productive asset it should be.

From the 30,000-foot level, CFOs should consider the digital information present in their businesses in light of the myriad information management and IT planning considerations that impact it.

Ask the following questions: Is digital data well-organized? Is it secured and stored intelligently? Is it reliable? Is it available to those who need it, and in a timely manner? Is it unnecessarily subject to theft by insiders, or outsiders? Can it be found to be bona fide and trusted? Is it subject to manipulation, thereby mitigating its value? Can it really be used to make decisions? Are these decisions made in a timely way, and with confidence? Is it managed in such a way to ensure the growing requirements of regulatory compliance?

Dividends from IM Practices

Businesses that emphasize prudent IM practices can make more effective, informed decisions simply because of the utility and validity of their information. Better access to bona fide information leads to more efficient business processes and a higher likelihood of profitability.

Of high importance in our litigious and competitive business climate, consider the value from executive- and board-level peace of mind that comes from the comfort that a firm's digital information assets are secured, in all respects, from external threats. Further comfort comes from prudent IM practices that mitigate abuses by insiders, principally to avoid theft and manipulation of digital intellectual property and confidential/proprietary information. A recent federal study illustrates that roughly 60 percent of information-based losses come from internal abuses and overall poor management of information.

Also, global pressures for competitiveness can be better managed when business processes are streamlined from information and applications that work in concert, allowing for prudent and efficient retrieval by those that need it, when they need it.

Consider the fulfillment of the promise that IT brought decades ago, with limited success: the promise of making businesses smarter. When properly deployed, business information software allows management to use metrics and other analyses to evaluate the underlying business performance, as well as their own particular areas of measurement.

Metrics, of course, are worthless unless they are tested for validity and are timely, accurate and well-conceived. IM and strategic IT planning involve the selection of application software tools and the design of business processes that produce metrics. Few businesses benefit as much as possible from these — often because they did not originate from the CFO; rather, they were left to more narrowly focused management members or outsiders.

The CFO has a fiduciary role to ensure the information "asset" is efficiently deployed and managed and can be well-suited to evaluate the effectiveness and impact of IM-related practices. There is no reason for a CFO's success to be hindered because he or she may not be IT-savvy.

Specific IM Practices

Practices that safeguard and intelligently manage information are critical to mitigate information-borne business risks. The following practices are critical to the long-term survival of an enterprise and present a level of investment that typically pales in comparison to the cost of combating whatever risks and exposure arise from their absence or exploitation.

- Build a sturdy information systems foundation because digital information without integrity and effective delivery has little value.
- Establish a network infrastructure that's scalable to meet both today's and tomorrow's needs. Emphasize computing speed and devices that allow users to compute efficiently.

□ Secure key information from outsider abuses. Utilize technologies and methods to mitigate the risks of unwanted external-based intrusions that can literally take your business down. Firewalls and other devices, coupled with malicious behavior-fighting software applications, such as anti-virus and intrusion-detection tools, provide responsible protection.

□ Safeguard information from insider abuses such as employee and insider data theft. This requires a combination of IT, HR and legal expertise. Legal and HR practices include creation and enforcement of “acceptable use policies” surrounding what is, and is not, appropriate for employees to do when working on company systems.

IT-oriented tools and practices can reduce the impact of costly data “leakage.” Businesses can manage who has access to data, as well as provide for which kind of devices can connect to the business network, thus alleviating the risks of data theft through copying to external media (e.g., CD or thumb drive). Many companies have increased their monitoring of employee computing behavior, as well as filtering inbound and outbound email content and website use.

The practices mentioned above not only help protect businesses from losing key or sensitive data, they also increase productivity and, thus, profitability. Proactive measures have been proven to save significant costs and residual harm by mitigating theft of intellectual property and other inappropriate employee behaviors.

□ Disaster planning and recovery management: mitigate the risks to critical business information and productivity that arises from disasters to benefit information systems, along with other assets. They need to be easily recoverable so that business resumption is not hindered materially. Preparing and managing a disaster recovery plan is a complex, multi-departmental process; the strategic IT plan should include this area in its purview.

□ Foster an environment where corporate governance over information systems and data is genuine. Bottom line: if the CEO and CFO don’t demonstrate concern about the integrity, efficiency and effectiveness of the computing environment and its staff and practices, information will not serve the business. Nor will systems be well planned, thereby reducing the effectiveness of IT and information.

Businesses benefit from having the CFO and CEO convey the business’s overall objectives, long- and short-term, and then have the strategic IT plan emphasize support of these objectives.

The adage “garbage-in, garbage-out” could not be more applicable than when it refers to the capturing and processing of business information. Clearly, without capturing relevant information, at the right time, in an accurate manner, information systems cannot deliver meaningful reports and analysis.

□ Specific software tools used — such as accounting software, manufacturing management software, customer relationship software and the like — should be selected as part of a strategic IT plan. All too often, businesses rely on non-integrated, poor-performing or simply inappropriate software to process and manage information.

Fortunately, business application software has become increasingly flexible, scalable, powerful and adept, yet less expensive, and can be adapted to successfully manage information in many industries. Gone should be the days of mandatory use of highly customized, risk-intensive software tools for mission-critical computing.

An IM strategy of utilizing more current software tools and databases, delivered through efficient user interfaces such as Web browsers, is something that the CFO can help ensure becomes a reality.

There are several IM practices worthy of consideration by the CFO. For starters, he or she should establish a committee to ensure that the nature and extent of information needed to manage the business is indeed captured, and available. Information should be organized in such a way so as to alleviate duplicity, and for effective sharing by users, without complications from version control challenges.

Although complex and ripe with benefits and detriments, information “retention” policies should be implemented, with the advice of counsel. This typically requires that businesses determine the classifications of information that they possess, followed by establishing rules for retention duration and destruction. Without consistent application of these policies, however, they can be worthless in the event of litigation.

Information ownership should be considered, as to specifically who is responsible for its validity and availability. And, emphasize information practices to enable regulatory compliance with mandated privacy acts and Sarbanes-Oxley, among others. Breaches of private information, as well as material weaknesses in internal control over financial information, can be detrimental as well as costly. IM practices, when supporting a well-conceived strategic IT plan that, in turn, supports business objectives, can lead to more effective decision-making and mitigation of information-borne risks that have become more prevalent with the pervasiveness of business data.

The CFO has a fiduciary responsibility for the successful deployment, safeguarding and management of business information. In concert with IT and other executives, the CFO can ensure that information can serve the business, thereby becoming a valued asset, rather than a costly nuisance.

Robert P. Green, CPA.CITP, is a Partner at SingerLewak, a leading regional Accounting and Consulting firm headquartered in Los Angeles. He can be reached via email at BGreen@SingerLewak.com, or by phone at 818.251.1359.

SingerLewak has offices in Orange County, Woodland Hills, Monterey Park, Inland Empire, San Diego and San Jose. The website is www.singerlewak.com and you can reach the Firms’ headquarters, toll free, at 877.754.4557.

Reprinted with permission of Financial Executive Magazine, a publication of FEI.