

# Information

A COMPANY'S MOST VALUABLE, YET MISMANAGED, ASSET

BY ROBERT GREEN, CPA, CITP & SCOTT COOPER, CMC



> **Any business that** wants to succeed understands the importance of caring for, and safeguarding, its most valuable asset—its employees—and rightfully so. Yet, shouldn't the next most valuable asset—business information—be treated with nearly the same level of care?

Reality is that the majority of businesses are woefully guilty of putting their enterprises at risk by not prudently managing their information. "Information" includes many things: client data, inventory procurement data, time and billing transactions, sales figures and marketing projections, and each is essential to the company's success.

Most consider information management, a broad term used to describe activities that provide for data processing, storage and safeguarding, to be a low priority, if not a nuisance. Too many businesses believe it's easy to ignore implementing information management best practices. It takes time and money to develop such practices, after all.

This mindset, however, can have dreadful consequences including sub-optimal

corporate performance, higher exposure to information-related risks and excessive costs from the risks that become exploited.

## IMPROVED DECISION MAKING

CEOs should recognize that they have a fiduciary responsibility to oversee the management of their company's information. They need to be aware of the kind of information the company owns, where it lives, who uses it, how it is protected, what is allowed to come in and go out, and how it is processed. Why?

Because they realize that prudently managed information enables sound and well-informed business decisions, which, in turn, lead to better

business practices and profits.

These decisions rely greatly on the use of relevant, bona fide, accurate, available and timely information.

**The reality is that the majority of businesses are woefully guilty of putting their enterprises at risk by not prudently managing their information.**

Some information management best practices include:

### *The Value of Reliable Metrics*

Business schools, executives and advisers stress the importance of using performance

indicators, or metrics, to allow managers to more effectively run their businesses.

Metrics often are computed using a combination of financial and non-financial information, and typically are delivered to their audience in the form of computer-generated reports, or in the form of "digital dashboards" which appear as electronic views of data on a desktop or home page.

Consider Gen-X Jeans, a fictitious company. Sample metrics for Gen-X Jeans, and their likely source of the underlying prudently managed information, are:

**Metric:** The level of returns—measured in units, style number or dollars—attributable to each retailer that purchases jeans from Gen-X Jeans, by month and rolling 12-month periods.

**Source:** Information gleaned from Gen-X's accounting software, including data captured for each customer account, sales order and return merchandise authorization.

**Metric:** All jean styles for which samples will not be ready for review by customers at an upcoming seasonal sales event, accompanied by the reason for their delay.

**Source:** Information gleaned from data processed in the "product lifecycle management" software that Gen-X Jeans uses. The information captured in the software is sufficiently thorough to allow for such metrics, and Gen-X Jeans has trained its employees to appropriately use and maintain this software.

### *Advantages of Organized, Accurate and Relevant Information*

The task of managing information goes far beyond metrics and measurement. Bad decisions can be avoided by ensuring that information is easily found and, thus, organized in a centralized, easily navigated and single-instance manner.

Among the ways to accomplish this are to implement robust document management software. This software allows for the management of revisions and versions of documents, the checking in/out of current versions of a particular file, and

## INFORMATION: A MOST VALUABLE, YET MIS

the ability to use knowledge-base search functions for information pertaining to a particular attribute (such as a case number, client, jeans style, etc.)

Similarly, when information is captured by software, it should be error-free and sufficient for use in prospective reporting, operations and analysis. These requirements can be accomplished by making sure that software implementations are performed competently to ensure the capture of bona fide, relevant and sufficient information in a timely manner, and that users are well trained.

Also, although often overlooked, network infrastructures should be organized to allow for rapid, consistent and intuitive means of finding files and folders. File and folder naming conventions and well-conceived folder “trees” can bring this to reality.

Information management practices surrounding data organization are successful when software, databases and processes work in harmony, such that people who need information know that it indeed exists, and know how (and are granted permission) to access it.

These practices are feasible if embraced by management.

#### *Impact of Information Ownership*

Information management also extends to the concept of data ownership. It should be clear exactly who in an organization is responsible for the accuracy and completeness of each kind of information, such as customer information, digital versions of engineering or design drawings, or bills of material.

Absent a chief information officer, a department manager is often designated as the owner of that department’s information, and the software selected to process the department’s transactions and business activities.

For example, a purchasing department manager should be responsible for ensuring that the software used by that department allows only valid, accurate information to be processed (and later stored and referenced) in a software prod-

uct deemed suitable for the processes in that department.

This owner can ensure the information is appropriately shared with business users. Also, care should be taken to avoid the common practices of having independent, rogue software deployments among a business’ many departments.



CEOs should recognize that they have a fiduciary responsibility to oversee the management of their company's information.

For the sake of the decision-making and operational effectiveness, a business must have a thorough understanding and companywide view of the various software products in use, what purpose they serve and what kind of information is processed. Establishing information and software ownership practices can help keep information effective, and available.

#### MITIGATION OF RISKS, COSTS AND REGULATORY EXPOSURE

Information practices that safeguard and intelligently manage information are critical to mitigate exposure risks. Not only do the following represent areas of information management that are critical to the survival of an enterprise, they also carry a level of investment that typically pales in comparison to the cost of combating whatever risks and exposure arise from their absence or exploitation.

##### *Electronic Data Retention Policies*

Along with the challenge of defining what information to capture and keep, management also must decide when is the right time to dispose of certain information. This is critical in the litigation preparedness arena and also represents sound business practices.

In developing appropriate document retention policies, it is recommended to include the advice of counsel, regardless of whether or not a business is involved in litigation, to determine just how long to maintain, and backup, various types of information. This is because regulatory bodies may mandate certain “lives” for key information, in both electronic and paper form.

For example, it may be best that all contractual documents/files and related working revisions be kept available to authorized users for a period of years and destroyed at a certain time. Other documents, such as digital engineering drawings, might be appropriately maintained and backed up indefinitely. E-mails, perhaps, would be given a shorter life span, for both active reference and backup purposes. Non-final versions of key electronic/digital documents also present a retention challenge.

Whatever the policy, it should be documented, managed, updated—and consistently maintained.

##### *IT-oriented Disaster Preparedness and Business Continuity*

Sound information management practices have a profound impact on the process of preparing for an unexpected loss from a

With  
prudent &  
sustained  
information  
management  
practices, the  
risk of making  
bad decisions  
is mitigated.

disaster. Although information is only one business component that requires disaster planning and recovery management, it can be among the most easily recoverable functions of the enterprise, and perhaps the most valuable to getting the business running again.

Not preparing for the resumption of information systems in the event of a disaster is not only irresponsible, but can lead to devastating costs, and possibly spell the end of the business. Preparing a disaster recovery plan is extensive, but achievable, for all businesses. It involves multiple departments, extensive collaboration, a broad approach that considers people, information, customers and operations, and, above all, requires a strong commitment by management.

Information systems personnel must be involved, or the loss of a most valued asset can occur. One should consider, for example, what kind of disaster or loss should be prepared for, as well as the nature of operations after a disaster occurs.

Say a business chooses to plan for a loss of headquarters due to fire. The planning process should include, among other features, the ability to have all critical software and current data restored and readily functional, allow for continuity of e-commerce transactions where applicable, and provide for temporary work facilities in which to conduct a reasonable level of operations.

#### *IT-oriented Regulatory Compliance*

Governmental regulations surrounding privacy of personal information, such as HIPAA, Gramm-Leach Bliley and state-specific regs, mandate businesses to protect and manage information of a confidential and personal nature. Other regulations, such as the Federal Rules of Civil Procedure, now more stringently emphasize the need to organize and manage digital information (specifically referred to as “electronically stored information”) to allow for more effective, relevant use in the litigation process.

Some mandates include the need to encrypt information for privacy and added security, as well as require the physical separation of certain kinds of digital information within an organization. Other

regulations require that in the event of a breach of security, which could result in personal information being available to individuals outside of the custodian company’s environment, the company must notify any number of its constituents and regulatory agencies about the breach, pay fines and take steps to ensure breaches are not reasonably repeatable.

Yet, despite these requirements, it is very common that they are not even known, or complied with, by businesses.

Lastly, recognize that Sarbanes-Oxley has given some legs to the requirements of maintaining sound information management practices, including the assessment and prioritization of corporate governance surrounding information technology and related internal controls of financial reporting.

Sound guidance on this topic, and other intelligent information management practices have been published by a number of agencies, including the IT Governance Institute, [www.ITGI.org](http://www.ITGI.org).

#### *Internal, External Threats to Information*

The annual financial and intangible cost of remediation and recovery from information loss, theft and manipulation is staggering, amounting to billions of dollars, according to studies.

These challenges result from threats from inside the business—and outside. Simple information management practices can be implemented to mitigate these costs, yet, again, these measures are often ignored, usually because management chooses to spend resources elsewhere or assumes that nothing devastating will happen to the company.

Practices to combat internal threats to information include the design and main-


tenance of network environments, user and group security/access controls, software application security and configurations, and the deployment of more recent tools that limit employee behavior, such as copying information to portable flash or hard drives.

Also, software can be implemented to monitor the kind of information “leakage” that occurs, specifically, isolating incidents where valuable information is inappropriately removed or copied from a business’ information systems.

Monitoring of e-mail content, both inbound and outbound, is common, as is monitoring employee internet activity. Some of these proactive measures have been demonstrated to save significant sums in the mitigation of losses from theft of intellectual property, and inappropriate employee behavior.

External threats to information are those that arise from activities outside the business, and include viruses, spyware and hackers. Most can be mitigated through security devices, software, management practices and policies. Firewalls, anti-virus software, e-mail content-filtering software and well-conceived IT-specific Acceptable Use Policies, which stipulate the rules and use of the internet and e-mail in a business, represent a few such tools and practices.

#### **WORTH THE INVESTMENT**

With prudent and sustained information management practices in place, the risk of making bad decisions is mitigated, and efficiencies are gained. Data is secure, effectively used and a strategic asset is treated with efforts that match its value. Gone are pains of excessive manual analysis, costly custom report writing exercises, embarrassing errors from bad data given to third parties and other symptoms of poor information management. 

**Robert “Bob” Green, CPA, CITP, and Scott Cooper, CMC**, are the managing directors of *INSYNC Consulting Group, Inc.*, which provides information management, strategic and tactical IT advisory services as well as forensic computing consulting. You can reach them at [Bob@INSYNCCusa.com](mailto:Bob@INSYNCCusa.com) and [Scott@INSYNCCusa.com](mailto:Scott@INSYNCCusa.com).