CHAPTER

10 Risk Management in IT[1]

Not so long ago, IT-based risk was a fairly low-key activity focused on whether IT could deliver projects successfully and keep its applications up and running (McKeen and Smith 2003). But with the opening up of the organization's boundaries to external partners and service providers, external electronic communications, and online services, managing IT-based risk has morphed into a "bet the company" proposition. Not only is the scope of the job bigger, but also the stakes are much higher. As companies have become more dependent on IT for everything they do, the costs of service disruption have escalated exponentially. Now, when a system goes down, the company effectively stops working and customers cannot be served. And criminals routinely seek ways to wreak havoc with company data, applications, and Web sites. New regulations to protect privacy and increase accountability have also made executives much more sensitive to the consequences of inadequate IT security practices—either internally or from service providers. In addition, the risk of losing or compromising company information has risen steeply. No longer are a company's files locked down and accessible only by company staff. Today, company information can be exposed to the public in literally hundreds of ways. Our increasing mobility, the portability of storage devices, and the growing sophistication of cyber threats are just a few of the more noteworthy means.

Therefore, the job of managing IT-based risk has become much broader and more complex, and it is now widely recognized as an integral part of any technology-based work—no matter how minor. As a result, many IT organizations have been given the responsibility of not only managing risk in their own activities (i.e., project development, operations, and delivering business strategy) but also of managing IT-based risk in all company activities (e.g., mobile computing, file sharing, and online access to information and software). Whereas in the past companies have sought to achieve security

[1] This chapter is based on the authors' previously published article, Smith, H. A., and J. D. McKeen. "A Holistic Approach to Managing IT-Based Risk." *Communications of the Association for Information Systems* 25, no. 41 (December 2009): 519–30. Reproduced by permission of the Association for Information Systems.

through physical or technological means (e.g., locked rooms, virus scanners), understanding is now growing that managing IT-based risk must be a strategic and holistic activity that is not just the responsibility of a small group of IT specialists but also part of the mind-set that extends from partners and suppliers to employees and customers.

This chapter explores how organizations are addressing and coping with increasing IT-based risk. It first looks at the challenges facing IT managers in the arena of risk management and proposes a holistic view of risk. Next it examines some of the characteristics and components needed to develop an effective risk management framework and presents a generic framework for integrating the growing number of elements involved in it. Finally, it describes some successful practices organizations could use for improving their risk management capabilities.

A HOLISTIC VIEW OF IT-BASED RISK

With the explosion in the past decade of new IT-based risks, it is increasingly recognized that risk means more than simply "the possibility of a loss or exposure to loss" (Mogul 2004) or even a hazard, uncertainty, or opportunity (McKeen and Smith 2003). Today, *risk* is a multilayered concept that implies much more is at stake.

> "IT risk has changed. IT risk incidents harm constituencies within and outside companies. They damage corporate reputations and expose weaknesses in companies' management teams. Most importantly, IT risk dampens an organization's ability to compete." (Hunter and Westerman 2007)

As a result, companies are now focused on "enterprise risk management" as a more comprehensive and integrated approach to dealing with risk (Slywotzky and Drzik 2005). Although, not every risk affecting an enterprise will be an IT-based risk, the fact remains that an increasing number of the risks affecting the enterprise have an IT-based component. For example, one firm's IT risk management policy notes that the goal of risk management is to ensure that technology failures or data integrity do not compromise the company's strategic objectives, the company's reputation and stakeholders, or its success and reputation.

But, in spite of the increasing number and complexity of IT-based threats facing organizations and evidence that links risk management with IT project success (Didraga 2013), it remains difficult to get senior executives to devote their attention (and commit the necessary resources) to effectively manage these risks. A recent global survey noted, "while the security community recognizes that information security is part of effective business management, managing information security risk is still overwhelmingly seen as an IT responsibility worldwide" (Berinato 2007). Another study of several organizations found that none had a good view of all key risks and 75 percent had major gaps in their approach to IT-based risk management (Coles and Moulton 2003). In short, while IT has become increasingly central to business success, many enterprises have not yet adjusted their processes to incorporate IT-based risk management (Hunter and Westerman 2007).

Knowing what's at stake, risk management is perennially in the top ten priorities for CIOs (Hunter et al. 2005) and efforts are being made to put effective capabilities and processes in place in IT organizations. However, only 5 percent of firms are at a high level of maturity in this area, and most (80 percent) are still in the initial stages

of this work (Proctor 2007). Addressing risk in a more professional, accountable, and transparent fashion is an evolution from traditional IT security work. At a Gartner symposium the following was pointed out:

> "[T]raditionally, [IT] security has been reactive, ad hoc, and technically-focused.... The shift to risk management requires an acceptance that you can't protect yourself from everything, so you need to measure risk and make good decisions about how far you go in protecting the organization." (Proctor 2007)

Companies in the group largely reflected this transitional state. "Information security is a primary focus of our risk management strategy," said one manager. "It's very, very visible but our business has yet to commit to addressing risk issues." Another stated, "We have a risk management group focused on IT risk, but lots of other groups focus on it too....As a result, there are many different and overlapping views, and we are missing integration of these views." "We are constantly trying to identify gaps in our risk management practices and to close them," said a third.

There is, however, no hesitation about identifying the sources of risk. Every company in the group had its own checklist of risk items, and experts have developed several different frameworks and categorizations that aim to be comprehensive (see Appendix A for some of these). What everyone agrees on is that any approach to dealing with IT-based risk must be holistic—even though it is an "onerous" job to package it as a whole. "Every category of risk has a different vocabulary," explained one focus group manager. "Financial, pandemic, software, information security, disaster recovery planning, governance and legal—each view makes sense, but pulling them together is very hard." Risk is often managed in silos in organizations, resulting in uncoordinated approaches to its management and to decision-making incorporating risk. This is why many organizations, including several in the focus group, are attempting to integrate the wide variety of issues involved into one holistic enterprise risk management strategy that uses a common language to communicate.

The connection among all of the different risk perspectives is the enterprise. Any IT problem that occurs—whether with an application, a network, a new system, a vendor, or a hacker (to name just a few)—has the increasing potential to put the enterprise at risk. Thus, a holistic view of IT-based risk must put the enterprise front and center in any framework or policy. A risk to the enterprise includes anything (either internal or external) that affects its brand, reputation, competitiveness, financial value, or end state (i.e., its overall effectiveness, efficiency, and success).

Figure 10.1 offers an integrated, holistic view of risk from an enterprise perspective. A wide variety of both internal and external IT-based risks can affect the enterprise. Externally, risks can come from the following:

- Third parties, such as partners, software vendors, service providers, suppliers, or customers
- Hazards, such as disasters, pandemics, geopolitical upheavals, or environmental considerations
- Legal and regulatory issues, such as failure to adhere to the laws and regulations affecting the company, including privacy, financial reporting, environmental reporting, and e-discovery

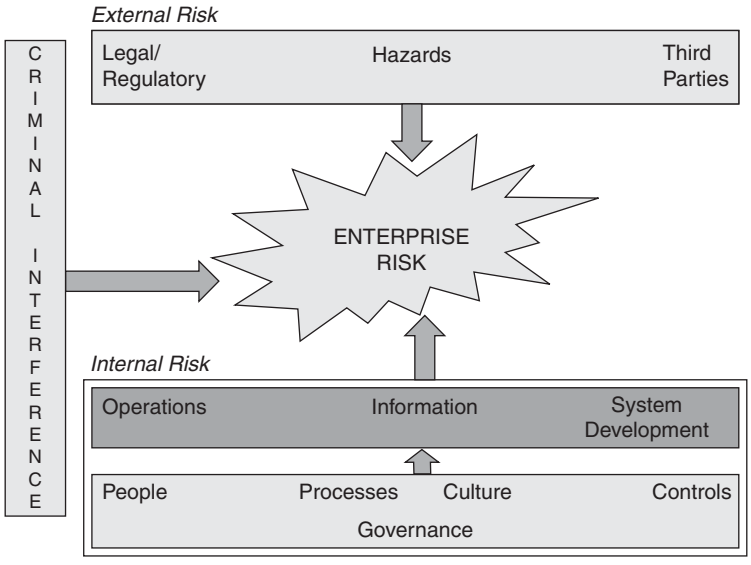

FIGURE 10.1 A Holistic View of IT-Based Risk

Internally, some risks are well known, such as those traditionally associated with IT operations (availability, accessibility) and systems development (not meeting schedules or budgets, or delivering value). Others are newer and, although they must be managed from within the organization, they may include both internal and external components. These include the following:

- Information risks, such as those affecting privacy, quality, accuracy, and protection
- People risks, such as those caused by mistakes or lack of adherence to security protocols
- Process risks, such as problems caused by poorly designed business processes or by failure to adapt business processes to IT-based changes
- Cultural risks, such as risk aversion and lack of risk awareness
- Controls, such as ineffective or inadequate controls to prevent or mitigate risk incidents
- Governance, such as ineffective or inadequate structure, roles, or accountabilities to make appropriate risk-based decisions

Finally, there is the risk of criminal interference, either from inside or outside the organization. Unlike other types of risk, which are typically inadvertent, criminal actions are deliberate attacks on the enterprise, its information, or sometimes its employees or customers. Such threats are certainly not new. Everyone is familiar with viruses and hackers. What is new, however, is that many more groups and individuals are targeting organizations and people. These include other national governments, organized crime, industrial spies, and terrorists. "These people are not trying to bring systems down, like in the past," explained a group member. "They are trying to get information."

HOLISTIC RISK MANAGEMENT: A PORTRAIT

Tackling risk in a holistic fashion is challenging, and building an effective framework for its management is challenging. It is interesting to note that there is much more agreement from the focus group and other researchers about what effective risk management *looks like* than *how* to do it. With this in mind, we outline some of the characteristics and components of an effective, holistic risk management program:

1. ***Focus on what's important.*** "Risks are inevitable," admitted a manager. "The first question we must ask is 'What are we trying to protect?'" said another. "There's no perfect package, and some residual risk must always be taken." A third added "Risks are inevitable, but it's how they're managed—our response, contingency plans, team readiness, and adaptability—that makes the difference." In short, risk is uncertainty that matters, something that can hurt or delay an enterprise from reaching its objectives (Hillson 2008). Although many managers recognize that it's time to take a more strategic view of risk, "[W]e still don't have our hands around what's important and what we should be monitoring and protecting" (Berinato 2007). Risk management is therefore not about anticipating all risks but about attempting to reduce significant risks to a manageable level and knowing how to assess and respond to it (Slywotzky and Drzik 2005). Yet, more than protecting the enterprise, risk management should also enable IT to take more risk in the safest possible way (Caldwell and Mogul 2006). Thus, the focus of effective risk management should not be about saying "no" to a risk, but how to say "yes," thereby building a more agile enterprise (Caldwell and Mogul 2006).
2. ***Expect changes over time.*** Few companies have a good grasp of risk management because IT is a discipline that is evolving rapidly (Proctor 2007). As a result, it would be a mistake to codify risk practices and standards too rapidly, according to the focus group. Efforts to do this have typically resulted in "paperwork without context," said one manager. Within a particular risk category, risk management actions should be "continuous, iterative, and structured," group members agreed. In recognition of this reality, most participant organizations have a mandatory risk assessment at key stages in the system development process to capture the risk picture involved with a particular project at several points in time and many have regular, ongoing reviews of required operational controls on an annual or biannual basis to do the same thing. In addition, when incidents occur, there should always be a process for evaluating what happened, assessing its impact, and determining if controls or other management processes need to be adapted (Coles and Moulton 2003). Finally, organizations should also be continually attempting to simplify and streamline controls wherever possible to minimize their burden. This is a process that is often missed, admitted one manager.

   However, despite the fact that each of these steps is useful, it is also essential to stand back from these initiatives and see how the holistic risk image is developing. It is this more strategic and holistic view that is often missing in organizations and that firms often fail to communicate to their staff. One of the greatest risks to organizations comes from employees themselves, not necessarily through their intentional actions, but because they don't recognize the risks involved in their actions (Berinato 2007). Therefore, many believe it is time to recognize that risk cannot be managed solely through controls, procedures, and technology but

that all employees must understand the concepts and goals of risk management because the enterprise will always need to rely on their judgment to some extent (Symantec Corporation 2007). In the same vein, many managers frequently do not comprehend the size and nature of the risks involved and thus resource their management inappropriately (Coles and Moulton 2003). As a result they tend to delegate many aspects of risk management to lower levels in the organization, thus preventing the development of any longer-term, overall vision (Proctor 2008; Witty 2008).

3. ***View risk from multiple levels and perspectives.*** Instead of dealing with security "incidents" in a one-at-a-time manner, it is important to do root cause analysis in order to understand risks in a more multifaceted way. To date, risk management has tended to focus largely on the operational and tactical levels and not viewed in a strategic way. One manager explained, "We need to assess risk trends and develop strategies for dealing with them. Tactics for dealing with future threats will then be more effective and easier to put in place." Another noted, "We must aim for redundancy of protection—that is, multiple layers, to ensure that if one layer fails, others will catch any problems."

   Furthermore, risk, security, and compliance are often intermixed in people's minds. Each of these is a valid and unique lens through which to view risk and should not be seen as being the same. For example, one expert noted that 70 percent of a typical "security" budget is spent on compliance matters, not on protecting and defending the organization (Society for Information Management 2008), and this imbalance means that overall spending in many firms is skewed. One firm uses the "prudent man" rule to deal with risk, which recommends a diversity of approaches—being proactive, prevention, due diligence, credibility, and promoting awareness—to ensure that it is adequately covered and that all stakeholders are properly protected. Monitoring and adapting to new international standards and laws, completing overall health checks, and analysis of potential risks are other new dimensions of risk that should be incorporated into a firm's overall approach to risk management.

DEVELOPING A RISK MANAGEMENT FRAMEWORK

With a holistic picture in mind, organizations can begin to develop a framework for filling in the details. The objective of a risk management framework (RMF) is to create a common understanding of risk, to ensure the right risks are being addressed at the right levels, and to involve the right people in making risk decisions. An RMF also serves to guide the development of risk policies and integrate appropriate risk standards and processes into existing practices (e.g., the SDLC). No company in the focus group had yet developed a comprehensive framework for addressing IT-based risk, although many had significant pieces in place or in development. In this section, we attempt to piece these together to sketch out what an RMF might contain.

An RMF should serve as a high-level overview of how risk is to be managed in an enterprise and can also act as a structure for reporting on risk at various levels of detail. Currently, many companies have created risk management policies and require all staff to read and sign them. Unfortunately, such policies are typically so long and complex as

to be overwhelming and ineffective. "Our security policy alone is two hundred pages. How enforceable is it?" complained a manger. Another noted that the language in his company's policy was highly technical. As a result, user noncompliance in following the recommended best practices was considerable. Furthermore, a plethora of committees, review boards, councils, and control centers are often designed to deal with one or more aspects of risk management, but they actually contribute to the general complexity of managing IT-based risk in an organization.

It should not be surprising that this situation exists, given the rapidity with which technologies, interfaces, external relationships, and dependencies have developed within the past decade. Organizations have struggled to simply keep up with the waves of legislation, regulation, globalization, standards, and transformation that seem to continually threaten to engulf them. An RMF is thus a starting point for providing an integrated, top-down view of risk, defining it, identifying those responsible for making key decisions about it, and mapping which policies and standards apply to each area. Fortunately, current technology makes it easy to offer multiple views and multiple levels of this information, enabling different groups or individuals to understand their responsibilities and specific policies in detail and see links to specific tools, practices, and templates, while facilitating different types of reporting to different stakeholders at different levels. By mapping existing groups, policies, and guidelines into an RMF, it is easier to see where gaps exist and where complexities in processes should be streamlined.

A basic RMF includes the following:

- ***Risk category.*** The general area of enterprise risk involved (e.g., criminal, operations, third party).
- ***Policies and standards.*** These state, at a high level, the general principles for guiding risk decisions, and they identify any formal corporate, industry, national, or international standards that should apply to each risk category.[2] For example, one company's policy regarding people states the following, in part:

  > Protecting the integrity and security of client and corporate information is the responsibility of every employee. Timely and effective reporting of actual and suspected privacy incidents is a key component of meeting this responsibility. Management relies on the collective experience and judgment of its employees.

  Another company policy regarding culture states, "We need to embed a risk management focus and awareness into all processes, functions, jobs, and individuals."

- ***Risk type.*** Each type of risk associated with each category (e.g., loss of information, failure to comply with specific laws, inability to work due to system outages) needs to be identified. Each type should have a generic name and definition, ideally linked to a business impact. Identifying all risk types will take

[2] Some international standards include Committee of Sponsoring Organizations (COSO) of the Treadway Commission, www.coso.org; SAI Global, www.saiglobal.com; and the Office of Government Commerce's Management of Risk (M_o_r) (www.ogc.gov.uk/guidance_management_of_risk.asp).

time and probably require much iteration as "there are an incredible variety of specific risks" (Mogul 2004). However, developing lists and definitions is a good first step (Baccarini et al. 2004; Hillson 2008; McKeen and Smith 2003) and is already a common practice among the focus group companies, at least for certain categories of risk.

- ***Risk ownership.*** Each type of risk should have an owner, either in IT or in the business. As well, there will likely be several stakeholders who will be affected by risk-based decisions. For example, the principal business sponsor could be the owner of risk decisions associated with the development or purchase of a new IT system, but IT operations and architecture as well as the project manager will clearly be key stakeholders. In addition to specialized IT functions, such as IT security, audit and privacy functions in the business will likely be involved in many IT risk-based decisions. Owners and stakeholders should have clear responsibilities and accountabilities. In the focus group, some major risk types were owned by committees, such as an enterprise risk committee, or the internal audit, social responsibility and risk governance committee, or the project risk review council on which stakeholder groups were represented.
- ***Risk mitigation.*** As an RMF is developed, each type of risk should be associated with controls, practices, and tools for addressing it effectively. These fall into one of two categories: compulsory and optional. Group members stressed that overemphasis on mitigation can lead to organizational paralysis or hyper-risk sensitivity. Instead participants stressed the role of judgment in right sizing mitigation activities wherever possible. "Our technology development framework does not tell you what you have to do, but it does give you things to consider in each phase," said one manager. "We look first at the overall enterprise risk presented by a project," said another, "and develop controls based on our evaluation of the level and types of risk involved." The goal, everyone agreed, is to provide a means by which risks can be managed consistently, effectively, and appropriately.[3]
- ***Risk reporting and monitoring.*** This was a rather controversial topic in the focus group. Although everyone agreed it is important to make risk and its management more visible in the organization, tracking and reporting on risk have a tendency to make management highly risk averse. One manager said:

> *We spent a year trying to quantify risks and developing a roll-up report, but we threw it away because audit didn't understand it and saw only one big risk. This led to endless discussion and no confidence that IT was handling risk well. Now we use a very simple reporting framework presenting risk as high, medium, or low. This is language we all understand.*

There are definitely pressures to improve risk measurement (Proctor 2007), but clearly care must be taken in how these metrics are reported. For example, one company

[3] "Risk Management Guide for Information Technology Systems" (csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf), the National Institute of Standards and Technology's Special Publication 800-30, provides guidance on specific risk mitigation strategies.

uses a variety of self-assessments to ensure that risks have been properly identified and appropriate controls put in place. However, as risk management procedures become better understood and more codified, risk reporting can also become more formalized. This is particularly the case at present with operational process controls and fundamental IT security, such as virus or intrusion detection.

However, risk monitoring is an ongoing process because levels and types of risk are changing continually. Thus, an RMF should be a dynamic document as new types of risk are identified, business impacts are better understood, and mitigation practices evolve. "We need to continually monitor all categories of risk and ask our executives if the levels of risk are still the same," said a focus group member. It is clear that failure to understand how risks are changing is a significant risk in itself (Proctor 2007). It is therefore especially important to have a process in place to analyze what happens when an unforeseen risk occurs. Unless efforts are made to understand the root causes of a problem, it is unlikely that effective mitigation practices can be put in place.

IMPROVING RISK MANAGEMENT CAPABILITIES

Risk management in most areas does not yet have well-documented best practices or standards in place. However, the focus group identified several actions that could lead to the development of effective risk management capabilities:

- ***Look beyond technical risk.*** One of the biggest inhibitors of effective risk management is too tight a focus on technical risk, rather than on business risk (Coles and Moulton 2003). A traditional security approach, for example, tends to focus only on technical threats or specific systems or platforms.
- ***Develop a common language of risk.*** A clearer understanding of business risk requires all stakeholders—IT, audit, privacy, legal, business managers—to speak the same language and use comparable metrics—at least at the highest levels of analysis where the different types of risk need to be integrated.
- ***Simplify the presentation.*** Having a common approach to discussing or describing risk is very effective, said several focus group members. While the work that is behind a simple presentation may be complex, presenting too much complexity can be counterproductive. The most effective approaches are simple: a narrative, a dashboard, a "stoplight" report, or another graphic style of report.
- ***Right size.*** Risk management should be appropriate for the level of risk involved. More effective practices allow for the adaptation of controls while ensuring that the decisions made are visible and the rationale is communicated.
- ***Standardize the technology base.*** This is one of the most effective ways to reduce risk, according to the research, but it is also one of the most expensive (Hunter et al. 2005).
- ***Rehearse.*** Many firms now have an emergency response team in place to rapidly deal with key hazards. However, it is less common that this team actually rehearses its disaster recovery, business continuity, or other types of risk mitigation plans.

One manager noted that live rehearsals are essential to reveal gaps in plans and unexpected risk factors.

- ***Clarify roles and responsibilities.*** With so many groups in the organization now involved in managing risk in some way, it is critical that roles and responsibilities be documented and communicated. Ideally, this should be in the context of an RMF. However, even if an RMF is not in place, efforts should be made to document which groups in the organization are responsible for which types of enterprise risk.
- ***Automate where appropriate.*** As risk management practices become standardized and streamlined, automated controls begin to make sense. Some tools can be very effective, noted the focus group, provided they are applied in ways that facilitate risk management, rather than becoming an obstacle to productivity.
- ***Educate and communicate.*** Each organization has its own culture, and most need to work with staff, business managers, and executives to make them more aware of risks and the need to invest in appropriate management. However, some organizations, like one insurance company in the focus group, are so risk-phobic that they need education to enable them to take on more risk. Such companies could benefit from better understanding their "risk portfolio" of projects (Day 2007). Such an approach can often help encourage companies to undertake more risky innovation initiatives with more confidence.

Conclusion

Organizations are more sensitized to risk than ever before. The economy, regulatory, and legal environment; business complexity; the increasing openness of business relationships; and rapidly changing technology have all combined to drive managers to seek a more comprehensive understanding of risk and its management. Whereas in the past, risk was managed in isolated pockets by such functions as IT security, internal audit, and legal, today recognition is growing that these arenas intersect and affect each other. And IT risk is clearly involved in many types of business risk these days. Criminal activity, legal responsibilities, privacy, innovation, and operational productivity, to name just a few, all have IT risk implications. As a result, organizations need a new approach to risk—one that is more holistic in nature and that provides an integrative framework for understanding risk and making decisions associated with it. Accomplishing this is no simple task, so developing such a framework will likely be an ongoing activity, as experts in IT and others begin to grapple with how to approach such a complex and multidimensional activity. This chapter has therefore not tried to present a definitive approach to risk management. There is general agreement that organizations are not ready for this. Instead, it has tried to sketch an impression of how to approach risk management and what an effective risk management program might look like. IT managers and others have been left to fill in the details and complete the portrait in their own organizations.

References

Baccarini, D., G. Salm, and P. Love. "Management of Risks in Information Technology Projects." *Industrial Management + Data Systems* 104, no. 3–4 (2004): 286–95.

Berinato, S. "The Fifth Annual Global State of Information Security." *CIO Magazine,* August 28, 2007.

Caldwell, F., and R. Mogul. "Risk Management and Business Performance Are Compatible." Gartner Inc., ID Number: G00140802, October 18, 2006.

Coles, R., and R. Moulton. "Operationalizing IT Risk Management." *Computers and Security* 22, no. 6 (2003): 487–92.

Day, G. "Is It Real? Can We Win? Is It Worth Doing? Managing Risk and Reward in an Innovation Portfolio." *Harvard Business Review,* December 2007.

Didraga, O. "The Role and the Effects of Risk Management in IT Projects Success." *Informatica Economica* 17, no. 1 (2013): 86–98.

Hillson, D. "Danger Ahead." *PM Network,* March 2008.

Hunter, R., and G. Westerman. *IT Risk: Turning Business Threats into Competitive Advantage.* Boston: Harvard Business School Press, 2007.

Hunter, R., G. Westerman, and D. Aron. "IT Risk Management: A Little Bit More Is a Whole Lot Better." *Gartner EXPCIO Signature Report,* February 2005.

McKeen, J., and H. Smith. *Making IT Happen: Critical Issues in IT Management*. Chichester, England: John Wiley & Sons, 2003.

Mogul, R. "Gartner's Simple Enterprise Risk Management Framework." Gartner Inc., ID Number: G00125380, December 10, 2004.

Proctor, P. IT "Risk Management for the Inexperienced: A CIO's Travel Guide to IT 'Securistan.'" Presentation to Gartner Symposium ITxpo 2007 Emerging Trends, San Francisco, CA, April 22–26, 2007.

Proctor, P. "Key Issues for the Risk and Security Roles, 2008." Gartner Inc., ID Number: G00155764, March 27, 2008.

Rasmussen, M. "Identifying and Selecting the Right Risk Consultant." Forrester Research Teleconference, July 12, 2007.

Slywotzky, A., and J. Drzik. "Countering the Biggest Risk of All." *Harvard Business Review,* April 2005.

Society for Information Management. "Executive IT security." Private presentation to the SIM Advanced Practices Council, May 2008.

Symantec Corporation. "Trends for July–December 2006." *Symantec Internet Security Threat Report* XI (March 2007).

Witty, R. "Findings: IT Disaster Recovery Can Upsell Business Continuity Management." Gartner Inc., ID Number: G00155402, February 19, 2008.

APPENDIX A

A Selection of Risk Classification Schemes

MCKEEN AND SMITH (2003)

- Financial risk
- Technology risk
- Security
- Information and people
- Business process
- Management
- External
- Risk of success

BACCARINI, SALM, AND LOVE (2004)

- Commercial risk
- Economic circumstances
- Human behavior
- Political circumstances
- Technology and technical issues
- Management activities and controls
- Individual activities

JORDAN AND SILCOCKS (2005)

- Project risk
- IT services
- Information assets
- IT service providers and vendors
- Applications
- Infrastructure
- Strategic
- Emergent

RASMUSSEN (2007)

- Information security risk
- Policy and compliance
- Information asset management
- Business continuity and disaster recovery
- Incident and threat management
- Physical and environment
- Systems development and operations management

COMBINED FOCUS GROUP CATEGORIES

- Project
- Operations
- Strategic
- Enterprise
- Disaster recovery
- Information
- External
- Reputation
- Competitive
- Compliance and regulatory
- Forensic
- Opportunity
- Ethical
- Physical
- Business continuity
- Business process

CHAPTER

11 Information Management: Stages and Issues[1]

More than ever before, we are living in an information age. Yet until very recently, information and its sibling, knowledge, were given very little attention in IT organizations. Data ruled. And information proliferated quietly in various corners of the business—file cabinets, PCs, databases, microfiche, e-mail, and libraries. Then along came the Internet and social media, and the business began to understand the power and the potential of information. For the past few years, businesses have been clamoring for IT to deliver more and better information to them (IBM 2012; Smith and McKeen 2005c). As a result, information delivery has become an important part of IT's job.

Now that businesses recognize the value of improved information, IT is facing huge challenges delivering it:

> Not only does effective information delivery require IT to implement new technologies, it also means that IT must develop new internal nontechnical and analytic capabilities. Information delivery makes IT work much more visible in the organization. Developing standard data models, integrating information into work processes, and forcing (encouraging) business managers to put the customer/employee/supplier first in their decision making involves IT practitioners in organizational and political conflicts that most would likely prefer to avoid. Unfortunately, the days of hiding in the "glass house" are now completely over and IT managers are front and center of an information revolution that will completely transform how organizations operate. (Smith and McKeen 2005a)

This points out a truth that is only just beginning to sink into the organization's collective consciousness. That is, although information *delivery* may be the responsibility

[1] This chapter is based on the authors' previously published article, Smith, H. A., and J. D. McKeen. "Information Management: The Nexus of Business and IT." *Communications of the Association for Information Systems* 19, no. 3 (January 2007): 34–46. Reproduced by permission of the Association for Information Systems.

of IT, information *management* (IM) requires a true partnership between IT and the business. IT is *involved* with almost every aspect of IM, but information is the heart and soul of the business, and its management cannot be delegated or abdicated to IT. Thus, IM represents the true nexus of the business and IT. Because of this, IM has all the hallmarks of an emerging discipline—the offspring of a committed, long-term relationship between the business and IT. It requires new skills and competencies, new frames of reference, and new processes. As is often the case, IT workers are further advanced in their understanding of this new discipline, but many business leaders are also recognizing their responsibilities in this field. In some organizations, notably government, IM is now a separate organizational entity, distinct from IT.

This chapter explores the nature and dimensions of IM and its implications for IT, looking at IM from the enterprise point of view. Information delivery can be viewed from a purely IT perspective, whereas information management addresses the business *and* IT issues and challenges in managing information effectively. The first section examines the scope and nature of IM and how it is being conceptualized in organizations. The next presents a framework for the comprehensive management of information. Then the key issues currently facing organizations in implementing an effective IM program are addressed. Finally, the chapter presents some recommendations for getting started in IM.

INFORMATION MANAGEMENT: HOW DOES IT FIT?

Information management is an idea whose time has come for a number of reasons. One focus group member explained it in this way:

> *In today's business environment, it is a given that we must know who our customer is and ensure our organization's information enables us to make the right business decisions. As well, emerging regulations are starting to shape the IM requirements of all companies. These include privacy and security safeguards on customer information, long-term storage of historical records, and stronger auditability. We are now being held legally accountable for our information*.

Thus, IM has three distinct but related drivers: (1) compliance, (2) operational effectiveness and efficiency, and (3) strategy.

Information, as we are now recognizing, is a key organizational resource, along with human and financial capital. Captured and used in the right way, many believe information is a different form of capital, known as *structural capital* (Stewart 1999). However, unlike human and financial capital, information is not finite. It cannot be used up, nor can it walk out the door. Furthermore, information capabilities—that is, the ability to capture, organize, use, and maintain information—have been shown to contribute to IT effectiveness, individual effectiveness, and overall business performance (Kettinger and Marchand 2005; Marchand et al. 2000; Perez-Lopez and Alegre 2012). Therefore, many companies now believe that creating useful structural capital is a strategic priority (IBM 2012; Kettinger and Marchand 2005).

Unlike information technology, which provides the technology, tools, and processes with which to *capture, store, and manipulate data,* or knowledge management

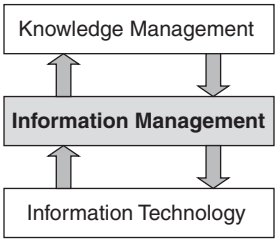

FIGURE 11.1 IM is Fundamental to Organizational Success—Both IT Effectiveness and Individual Performance

(KM), which focuses on how best to leverage the know-how and *intangible experience* of the organization's human capital, IM provides the mechanisms for managing enterprise information itself. IM represents the "meat" in the data–information–knowledge continuum and provides a foundation that can be used by both IT and KM to create business value (see Figure 11.1).

As noted earlier, organizations today are beset with demands for more and better information and more controls over it. IM is the means to get above the fray and clarify how the enterprise will manage information as an integrated resource. In theory, it covers all forms of information needed and produced by the business, both structured and unstructured, including the following:

- Customer information
- Financial information
- Operational information
- Product information
- HR information
- Documents
- E-mail and instant messages
- Customer feedback
- Images and multimedia materials
- Business intelligence
- Relationship information (e.g., suppliers, partners)
- Information about physical objects (i.e., the internet of things)
- Externally generated information (e.g., government records, weather information)
- Geolocation information

In practice, some of these forms will be more thoroughly managed than others, depending on the organization involved.

The "IM function" is also responsible for the complete information life cycle: acquisition or creation, organization, navigation, access, security, administration, storage, and retention. Because IM falls into the gray area between the business and IT and is not yet a separate organizational entity, many organizations are finding it is essential to develop an enterprisewide framework that clarifies the policies, principles, roles, responsibilities and accountabilities, and practices for IM in both groups.

A FRAMEWORK FOR IM

Because much information use crosses traditional functional boundaries, organizations must take an enterprise perspective on IM for it to be effective. A framework for implementing IM involves several stages that move from general principles to specific applications. Although these are presented as distinct activities, in practice they will likely evolve iteratively as the organization and its management learn by doing. For example, one company developed and implemented its privacy policy first then recognized the need for an information security policy. As this was being implemented, it created a more generic IM policy that incorporated the other two in its principles.

Stage One: Develop an IM Policy

A policy outlines the terms of reference for making decisions about information. It provides the basis for corporate directives and for developing the processes, standards, and guidelines needed to manage information assets well throughout the enterprise. Because information is a corporate asset, an IM policy needs to be established at a very senior management level and approved by the board of directors. This policy should provide guidance for more detailed directives on accountabilities, quality, security, privacy, risk tolerances, and prioritization of effort.

Because of the number of business functions affected by information, a draft policy should be developed by a multidisciplinary team. At minimum, IT, the privacy office, legal, HR, corporate audit, and key lines of business should be involved. "We had lots of support for this from our audit people," said one manager. "They recognize that an IM policy will help improve the traceability of information and its transformations, and this makes their jobs easier." Another recommended reviewing the draft policy with many executives and ensuring that all business partners are identified. "Ideally, the policy should also link to existing IM processes such as security classifications," stated another. "It's less threatening if people are familiar with what it implies, and this also helps identify gaps in practices that need to be addressed."

Stage Two: Articulate the Operational Components

The operational components describe what needs to be in place in order to put the corporate IM policy into practice across the organization (see Figure 11.2). In turn, each component will have several "elements." These could vary according to what different organizations deem important. For example, the strategy component at one company has six elements: (1) interacting with the external environment, (2) strategic planning, (3) information life cycle, (4) general planning, (5) program integration, and (6) performance monitoring (for a description of the elements identified by this firm, see Appendix A). Together, the operational components act as a context to describe current IM practices in the organization and reference existing best practices in each area. "This is a living document, and you should expect it to be continually refined," noted a focus group member.

The IM framework's operational components and individual elements act as a discussion document to position IM in the business and to illustrate its breadth and scope. "There's a danger of IM being perceived as a 'technology thing,'" stated a manager.

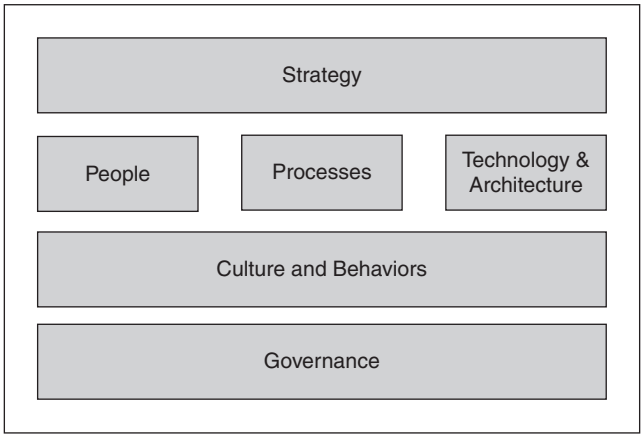

FIGURE 11.2 Operational Components of an IM Framework

Although it is often IT groups that spearhead the IM effort, they recognize that it shouldn't necessarily be located in IT permanently. "Ideally, we need a corporate information office that cuts across lines of business and corporate groups, just like IT," said another manager.

Stage Three: Establish Information Stewardship

Many roles and responsibilities associated with IM need to be clearly articulated. These are especially important to clarify because of the boundary-spanning nature of information. Both political and practical issues arise when certain questions are asked: Who is responsible for the quality of our customer data? Whose version of name and address do we use? Who must sign off on the accuracy of our financial information? Ideally, most organizations would like to have a single version of each of their key information subjects (e.g., customer, product, employees) that all lines of business and systems would use. This would enable proper protections and controls to be put in place. And this is clearly a long-term IM goal for most. However, legacy environments, politics, and tight budgets mean that the reality is somewhat less perfect with duplicate versions of the same information and several variants being used by parts of the business.

Information stewards are businesspeople. They should be responsible for determining the meaning of information "chunks" (e.g., customer name and address) and their business rules and contextual use. They should be responsible for the accuracy, timeliness, consistency, validity, completeness, and redundancy of information. Stewards also determine who may access information according to privacy and security policies and provide guidance for the retention and deletion of information in accordance with regulatory and legal requirements. In addition, stewards make the information's characteristics available to a broad audience through the organization's metadata.

Stewardship, like IM, is an evolving role that few understand fully. Ideally, there should be one steward for each key information subject, but this is nowhere near the reality in most organizations. One organization has established a working group for each of its major subjects, with representatives from all affected stakeholder groups as well as IT. The working groups' goals are to reduce duplicate records, correct information,

simplify processes, and close "back doors." In the longer term, these groups hope to develop standard definitions and a formal stewardship process and ultimately use these to retool IT's data infrastructure.

"We are struggling with this concept," admitted a manager. "This is not a simple task, and no one in our business wants to take accountability as yet." Stewardship also takes time, and many business units are not yet prepared to allocate resources to it. "At present, we are hitching our wagons to other projects and hoping to make some progress in this way," said another manager. "Every area is taking some steps, but they're all at different levels of maturity. This can be frustrating because progress is so slow." All agreed that the role of information steward needs to be better defined and incorporated into organizational and HR models. New performance metrics also need to be established to monitor progress against these goals in ways that link IM activities to key business objectives.

Stage Four: Build Information Standards

Standards help ensure that quality, accuracy, and control goals can be met. When all parts of an organization follow the same standards, it is relatively easy to simplify the processes and technology that use a piece of information, said the focus group. Conversely, different information standards used by different business groups will inhibit effective IM. *Setting* information standards can be challenging, and it's even harder to actually *implement* them, participants noted. The latter is partly due to the large number of legacy applications in most organizations and also because it is difficult to get funding for this work.

Not all information needs to be standardized, however—only that which is used by more than one business unit. When information *is* used more broadly, a standard needs to be established. A metadata repository is useful for this. This repository stores information definitions; standards for use and change; and provides cross-references for all models, processes, and programs using a particular piece of information. A metadata repository can be jointly used by the business, when beginning a new project, and IT, when developing or modifying applications. It can be invaluable to both groups (and the enterprise) in helping them to understand how their work will affect others, thus preventing potential problems.

Typically, cross-functional working groups composed of business and IT staff establish standards. "Metadata is really where the rubber meets the road," said one manager. "It can be a very powerful tool to prevent the duplication of data in the organization." However, it is a huge undertaking and takes time to show value. "You need strong IT executive support for this," he said. "It is not something that those outside of IT initially understand." The focus group recommended starting with what exists currently (e.g., a data warehouse), then growing from there. One firm initially established a procedure that any changes to production systems had to update the metadata repository first. "We weren't prepared for the demand this created," stated the manager involved. "It's much better to incorporate this step in front-end analysis than at the end of development."

Finally, education and awareness play an essential role at this stage. "We always underestimate the importance of awareness," said a participant. "We must make sure that no project starts in the organization that doesn't use standards. The only way to

Standards require . . .

- A unique name and definition
- Data elements, examples, and character length (e.g., name prefix)
- Relationship rules
- Implementation requirements
- Spacing and order

do this is to keep this issue continually in front of our business executives." The other group members agreed. "Standards are the cornerstone of IM," said one. "If they are followed, they will ensure we don't add further layers of complexity and new steps."

ISSUES IN IM

As with anything new, those involved with IM in their organizations face a host of challenges and opportunities as they try to implement more effective processes and practices around information. Some of these can be mixed blessings in that they are both drivers of IM and complications (e.g., legislation). Others are simply new ways of looking at information and new perspectives on the way organizations work. Still others are genuinely new problems that must be addressed. When combined with the fact that IM "belongs" exclusively to neither IT nor the business, these add up to a huge organizational headache, especially for IT. "Sometimes the businesspeople are not ready for the disciplines associated with IM," said one manager. "If they're not ready, we move on to an area that is." Another said, "Sometimes it's more trouble than it's worth to involve the business, and we just do the work ourselves."

Culture and Behavior

In the longer term, however, the focus group agreed that IM is something that all parts of the organization will have to better understand and participate in. One of the most comprehensive challenges is changing the culture and behavior surrounding information. Marchand et al. (2000) suggest that six interdependent beliefs and behaviors are needed by all staff to support a positive "information orientation." These have been strongly correlated to organizational performance when they are present with strong IT and IM practices:

1. ***Integrity.*** Integrity "defines both the boundaries beyond which people in an organization should not go in using information and the 'space' in which people can trust their colleagues to do with information what they would do themselves" (Marchand et al. 2000). Where integrity exists, people will have confidence that information will not be used inappropriately.
2. ***Formality.*** Formality is the ability to trust formal sources of information (as opposed to informal ones). Formality enables an organization to provide accurate and consistent information about the business and establish formal processes and information flows that can be used to improve performance and provide services to customers.

3. ***Control.*** Once formal information is trusted, it can be used to develop integrated performance criteria and measures for all levels of the company. In time, these will enable monitoring and performance improvement at the individual and work unit levels and can be linked to compensation and rewards.
4. ***Transparency.*** Transparency describes a level of trust among members of an organization that enables them to speak about errors or failures "in an open and constructive manner without fear of unfair repercussions" (Marchand et al. 2000). Transparency is necessary to identify and respond effectively to problems and for learning to take place.
5. ***Sharing.*** At this level, both sensitive and nonsensitive information is freely shared among individuals and across functional boundaries. Information exchanges are both initiated by employees and formally promoted through programs and forums.[2]
6. ***Proactiveness.*** Ultimately, every member of an organization should be proactive about acquiring new information about business conditions and testing new concepts.

Information Risk Management

The increasing breadth and scope of IT, combined with greater use of outsourcing and mobility, has made information more vulnerable to both internal and external fraud and has raised the level of risk associated with it. Management must, therefore, take proactive measures to determine an appropriate risk/return trade-off for information security. Costs are associated with information security mechanisms, and the business must be educated about them. In some cases these mechanisms are "table stakes"—that is, they must be taken if the company wants to "be in the game." Other risks in information security include internal and external interdependencies, implications for corporate governance, and impact on the value proposition. Risk exposures can also change over time and with outsourcing, mobile applications, and cloud computing.

The focus group agreed that security is essential in the new world of IM. Today most organizations have basic information protection, such as virus scanners, firewalls, and virtual private networks. Many are also working on the next level of security, which includes real-time response, intrusion detection and monitoring, and vulnerability analysis. Soon, however, information security will need to include role-based identity and access management. An effective information-security strategy includes several components:

- An information protection center, which classifies data, analyzes vulnerabilities, and issues alerts
- Risk management
- Identity management, including access management, digital rights management, and encryption technology
- Education and awareness
- Establishment of priorities, standards, and resource requirements
- Compliance reviews and audits

[2] Privacy laws in many countries inhibit the sharing of personal information for any purpose other than that for which it was collected. Customer information can, therefore, be shared only with consent.

Many of the decisions involved must be made by the lines of business, not IT, as only the business can determine access rules for content and the other controls that will facilitate identity and access management.

Information Value

At present, the economics of information have not yet been established in most organizations. It is, therefore, often hard to make the case for IM investments not only because the benefits are difficult to quantify but also because of the large number of variables involved. A value proposition for IM should address its strategic, tactical, and operational value and how it will lower risk and develop new capabilities. Furthermore, an effort should be made to quantify the value of the organization's existing information assets and to recognize their importance to its products and services.

Determining "value" is a highly subjective assessment. Thus, different companies and even different executives will define it differently. Most businesses define *value* broadly and loosely, not simply as a financial concept (Ginzberg 2001). However, because there is no single, agreed-on measure of information value, misunderstandings about its definition can easily arise (Beath et al. 2012). Therefore, it is essential that everyone involved in IM activities agree on what value they are trying to deliver and how they will recognize it. Furthermore, value has a time dimension. It takes time for an IM investment to pay off and become apparent. This also must be recognized by all concerned.

Privacy

Concern for the privacy of personal information has been raised to new levels, thanks to legislation being enacted around the world. All companies need enterprisewide privacy policies that address the highest privacy standards required in their working environments. For example, if they operate globally, policies and practices should satisfy all legislation worldwide. Privacy clearly should be both part of any long-term IM initiatives, and also what an organization is doing *currently.* As such, it is both an IM issue and an initiative in its own right. Both existing processes and staff behavior will be affected by privacy considerations. "Privacy is about respect for personal information and fair and ethical information practices. Training should start with all new employees and then be extended to all employees," said a manager. Many countries now require organizations to have a chief privacy officer. If so, this person should be a key stakeholder in ensuring that the organization's IM practices for data quality and accuracy, retention, information stewardship, and security are also in keeping with all privacy standards and legislation.

As with other IM initiatives, it is important that senior management understand and support the changes needed to improve privacy practices over time. "Good practices take time to surface," said a manager. "It takes time and resources to ensure all our frontline staff and our information collection and management processes are compliant." Accountabilities should be clearly defined as well. Ideally, IM policy and stewards set the standards in this area with privacy specialists and operational staff (in both IT and the business) responsible for implementing them. With the increase in outsourcing, particularly to offshore companies, all contracts and subcontracting

arrangements must be reviewed for compliance in this area. "Our company is still liable for privacy breaches if they occur in one of our vendor firms," noted a group member.

Knowledge Management

Although many organizations have been soured on knowledge management (KM) because of its "soft and fuzzy" nature (Smith and McKeen 2004), the fact remains that IM provides a solid foundation that will enable the organization to do more with what it knows (see Figure 11.1). Even firms that do not have a separate KM function recognize that better IM will help them build valuable structural capital. There are many levels at which IM can be improved. At the most elementary, data warehouses can be built and the information in them can be analyzed for trends and patterns. One company is working on identifying its "single points of knowledge" (i.e., those staff members who have specialized knowledge in an important area) and capturing this knowledge in a formal way (e.g., in business processes or metadata). Many firms are making customer information management a priority so they can use this information to both serve their customers better and to learn more about them.[3] This clearly cannot be done unless information is integrated across processes and accessible in a usable format (Beath et al. 2012; Smith and McKeen 2005b). Finally, information can be aggregated and synthesized to create new and useful knowledge. For example, Wal-Mart takes transaction-level information from its sales process and aggregates and analyzes it to make it useful both to the sales process and to other areas of the business. It identifies trends and opportunities based on this analysis and enables information to be viewed in different ways, leading to new insights.

The Knowing–Doing Gap

Most organizations assume that better information will lead to better decisions and actions, but research shows that this is not always (or even often) the case. All too often companies do not utilize the information they have. One problem is that we really understand very little about how organizations and groups actually use information in their work (Beath et al. 2012; Pfeffer and Sutton 2000). Some organizations do not make clear links between desired actions and the acquisition and packaging of specific information. Although this may seem like common sense, the focus group agreed that the complex connections between decisions and actions are not always well understood. Effective technology, strong IM practices, and appropriate behaviors and values are *all* necessary to ensure the information–action connection is made (Smith et al. 2006).

GETTING STARTED IN IM

Although IM is not IT, the fact remains that IT is still largely driving IM in most organizations. Whether this will be the case in the longer term remains to be seen. Most members would like to see the situation reversed, with the business driving the effort to

[3] Customer information is particularly sensitive and may be analyzed only with a customer's consent in many countries. The need to monitor consents adds a further layer of complexity to this already challenging activity.

establish appropriate IM policies, procedures, stewardship, and standards and IT supporting IM with software, data custodianship, security and access controls, information applications and administration, and integrated systems. In the shorter term, however, IT is working hard to get IM the attention it deserves in the business.

Focus group participants had several recommendations for others wishing to get started in IM:

- ***Start with what you have.*** "Doing IM is like trying to solve world hunger," said one manager. "It just gets bigger and bigger the longer you look at it." Even just listing all of the information types and locations in the organization can be a daunting task, and the job will probably never be fully complete. The group, therefore, recommended doing an inventory of what practices, processes, standards, groups, and repositories already exist in the organization and trying to grow IM from there. It is most important to get the key information needed to achieve business objectives under control first. For many companies, this may be customer information; for others, it may be product or financial information. "It's really important to prioritize in IM," said a manager. "We need to focus on the right information that's going to have the biggest return." It may help to try to quantify the value of company information in some way. Despite the fact that there is no accepted accounting method for doing so as yet, some firms are adapting the value assessment methodologies used for other assets. "When you really look at the value of information, it's worth a staggering amount of money. This really gets senior management attention and support," noted a focus group member.

  A top-down approach is ideal, yet it may not always be practical. "It took us over a year to get an information policy in place," said a participant. "In the meantime, there are significant savings that can be realized by taking a bottom-up approach and cleaning up some of the worst problems." Harnessing existing compliance efforts around privacy, security, and the other types of regulation is also effective. At minimum, these will affect information architecture, access to data, document retention, and data administration for financial and personal information (Smith and McKeen 2006). "We can take either an opportunity or a fear mindset toward regulation," said a manager. Companies that see compliance from a purely tactical perspective will likely not see the value of increased controls. If, however, they see regulation as a chance to streamline and revamp business processes and the information they use, their compliance investments will likely pay off. Those interested in IM can also take advantage of the dramatically elevated attention levels of the board and executives to compliance matters.
- ***Ensure cross-functional coordination among all stakeholders.*** Business involvement in IT initiatives is always desirable, and it is impossible to do IM without it. "No IM effort should go ahead without fully identifying all areas that are affected," stated one manager. Typically, legal, audit, and the privacy office will have a keen interest in this area. Equally typical, many of the business units affected will not be interested in it. For operational groups, IM is often seen as bureaucratic overhead and extra cost, which is why education and communication about IM are essential. "You have to allow time for these groups to get on board with this concept and come around to the necessity of taking the time to do IM right," said a

participant. He noted that this effort has to be repeated at each level of the organization. "Senior management may be supportive, but members of the working groups may not really understand what we're trying to accomplish."

- ***Get the incentives right.*** Even with IM "socialization" (i.e., education and communication), politics is likely to become a major hurdle to the success of any IM efforts. Both giving up control and taking accountability for key pieces of information can be hard for many business managers. Therefore, it is important to ensure incentives are in place that will motivate collaboration. Metrics are an important way to make progress (or the lack of it) highly visible in the organization. One firm developed a team scorecard for its customer information working group that reported two key measures to executives: the percentage of remaining duplicate records and the percentage of "perfect" customer records. Each of these was broken down into a number of leading indicators that helped focus the group's behavior on the overall effort rather than on individual territories. Another firm linked its process and information simplification efforts to budgets. The savings generated from eliminating duplicate or redundant information (and its associated storage and processing) were returned to the business units involved to be reinvested as they saw fit. This proved to be a huge motivator of enterprise-oriented behavior.
- ***Establish and model sound information values.*** Because frontline workers, who make many decisions about information and procedures, ultimately cannot cover all eventualities, all staff need to understand the fundamental reasons for key company information policies and directives. Corporate values around information guide how staff should behave even when their managers aren't around. And they provide a basis for sound decision making about information (IBM 2012; Stewart 2004). Others have noted that senior IT leadership should primarily be about forming and modeling values, not managing tasks, and this is especially true for IM, said the focus group. Values are particularly important, they noted, now that staff are more mobile and virtual and, thus, more empowered. If such values are effectively articulated and modeled by leaders, they will drive the development of the appropriate culture and behaviors around information.

Conclusion

Information management is gaining increasing attention in both IT and the business. Driven by compliance and privacy legislation, the increasing vulnerability of corporate information, and the desire for greater integration of systems, IM is beginning to look like an emerging discipline in its own right. However, the challenges facing organizations in implementing effective IM practices are many and daunting. Not least is the need to try to conceptualize the scope and complexity of work to be done. Tackling IM is likely to be a long-term task. IT managers have a huge communications job ahead in trying to educate business leaders about their responsibilities in information stewardship, developing sound IM practices, and inculcating the culture and behaviors needed to achieve the desired results. Developing a plan for tackling the

large and ever-increasing amount of information involved is only the first step. The more difficult effort will be involving every member of the organization—from the board to frontline workers—in seeing that it is carried out effectively. Although IT can lead this effort initially and provide substantial support for IM, ultimately its success or failure will be due to how well the business does its part.

References

Beath, C., I. Bercerra-Fernandez, J. Ross, and J. Short. "Finding Value in the Information Explosion." *MIT Sloan Management Review* 53, no. 4 (Summer 2012).

Ginzberg, M. "Achieving Business Value Through Information Technology: The Nature of High Business Value IT Organizations." Report commissioned by the Society for Information Management Advanced Practices Council, November 2001.

IBM. *CEO Survey 2011: Leading through Connections Executive Summary*. Somers, NY: IBM Global Business Services, May 2012, GBE03486-USEN-00.

Kettinger, W., and D. Marchand. "Driving Value from IT: Investigating Senior Executives' Perspectives." Report commissioned by the Society for Information Management, Advanced Practices Council, May 2005.

Marchand, D., W. Kettinger, and J. Rollins. "Information Orientation: People, Technology and the Bottom Line." *MIT Sloan Management Review* 4, no. 41 (Summer 2000): 69–80.

Perez-Lopez, S., and J. Alegre. "Information Technology Competency, Knowledge Processes and Firm Performance." *Industrial Management and Data Systems* 112, no. 4 (2012): 644–62.

Pfeffer, J., and R. Sutton. *The Knowing-Doing Gap.* Boston: Harvard Business School Press, 2000.

Smith, H. A., and J. D. McKeen. "Marketing KM to the Business." *Communications of the Association for Information Systems* 14, article 23 (November 2004): 513–25.

Smith, H. A., and J. D. McKeen. "Information Delivery: IT's Evolving Role." *Communications of the Association for Information Systems* 15, no. 11 (February 2005a): 197–210.

Smith, H. A., and J. D. McKeen. "A Framework for KM Evaluation." *Communications of the Association for Information Systems* 16, no. 9 (May 2005b): 233–46.

Smith, H. A., and J. D. McKeen. "Customer Knowledge Management: Adding Value for Our Customers." *Communications of the Association for Information Systems* 16, no. 36 (November 2005c): 744–55.

Smith, H. A., and J. D. McKeen. "IT in the New World of Corporate Governance Reforms." *Communications of the Association for Information Systems* 17, no. 32 (May 2006): 714–27.

Smith, H. A., J. D. McKeen, and S. Singh. "Making Knowledge Work: Five Principles for Action-Oriented Knowledge Management." *Knowledge Management Research and Practice* 4, no. 2 (2006): 116–24.

Stewart, T. *Intellectual Capital: The New Wealth of Organizations.* New York: Doubleday, 1999.

Stewart, T. "Leading Change When Business Is Good: An Interview with Samuel J. Palmisano." *Harvard Business Review* 82, no. 12 (December 2004).