Harvard Business Review
www.hbr.org

Top executives often feel uncomfortable making hard choices about information technology. But when they abdicate responsibility, they set their companies up for wasted investments and missed opportunities.

Six IT Decisions Your IT People Shouldn't Make

by Jeanne W. Ross and Peter Weill

Reprint R0211F

Top executives often feel uncomfortable making hard choices about information technology. But when they abdicate responsibility, they set their companies up for wasted investments and missed opportunities.

Six IT Decisions Your IT People Shouldn't Make

by Jeanne W. Ross and Peter Weill

For several years now, we have observed the frustration—sometimes even exasperation—that many business executives feel toward information technology and their IT departments. Our center runs a seminar called "IT for the Non-IT Executive," and the refrain among the more than 1,000 senior managers who have taken the course runs something like this: "What can I do? I don't understand IT well enough to manage it in detail. And my IT people—although they work hard—don't seem to understand the very real business problems I face."

Perhaps the complaint we hear most frequently from the executives—most of them CEOs, COOs, CFOs, or other high-ranking officers—is that they haven't realized much business value from the high-priced technology they have installed. Meanwhile, the list of seemingly necessary IT capabilities continues to grow, and IT spending continues to consume an increasing percentage of their budgets. Where's the payback?

Indeed, our research into IT management practices at hundreds of companies around the world has shown that most organizations are not generating the value from IT investments that they could be. The companies that manage their IT investments most successfully generate returns that are as much as 40% higher than those of their competitors.

While a number of factors distinguish these top-performing companies, the most important is that senior managers take a leadership role in a handful of key IT decisions. By contrast, when senior managers abdicate responsibility for those decisions to IT executives, disaster often ensues: Recall the high-profile instances of botched adoptions of large-scale customer-relationship-management and enterprise-resource-planning systems. It would be reasonable to assume that the CRM and ERP fiascoes were the result of technological snafus in getting the complex systems up and running. But in fact the problems generally occurred because senior executives failed to realize that adopting the systems posed a business—not just a technological—challenge. Consequently, they didn't take

responsibility for the organizational and business process changes the systems required.

Such unfortunate scenarios are likely to be replayed as companies face the next rounds of IT innovations: the increased use of Web services, the adoption of handheld devices by employees and customers, and the integration of multiple electronic sales and service channels such as Web sites, call centers, ATMs, and wireless phones.

Don't get us wrong. IT executives are the right people to make numerous decisions about IT management—the choice of technology standards, the design of the IT operations center, the technical expertise the organization will need, the standard methodology for implementing new systems. But an IT department should not be left to make, often by default, the choices that determine the impact of IT on a company's business strategy.

To help senior managers avoid IT disasters—and, more important, to help them generate real value from their IT investments—we offer a list of six decisions for which they would be wise to take leadership responsibility. The first three have to do with strategy; the second three relate to execution. Each is a decision that IT people shouldn't be making—because, in the end, that's not their job.

1

How much should we spend on IT?

Given the uncertain returns on IT spending, many executives wonder whether they are spending too much—or perhaps even too little. If we can just get the dollar amount right, the thinking goes, the other IT issues will take care of themselves. So they look to industry benchmarks as a way of determining appropriate spending levels.

But in the successful companies we have studied, senior managers approach the question very differently. First they determine the strategic role that IT will play in the organization, and only then do they establish a companywide funding level that will enable technology to fulfill that objective.

IT goals vary considerably across organizations. They may be relatively modest: for example, eliminating inaccuracies and inefficiencies in administrative processes. Or they may be central to a company's strategy: for example, supporting a seamless global supply chain, flawless customer service, or leading-edge research and development. Clearly, these different objectives require different levels of spending. And if you have determined that technology should play a central strategic role, the nature of that role will affect the required level of spending.

Take arch rivals United Parcel Service and FedEx. Both companies report spending around $1 billion on IT each year, but FedEx, which has annual revenues of about $20 billion, is just two-thirds the size of UPS. Does that mean IT plays a more important role at FedEx? No, simply a different one. UPS's IT strategy, which evolved from its industrial engineering roots, has focused on introducing efficiencies to a business that demands consistency and reliability. The company's centralized, standardized IT environment allows for dependable customer service at a relatively low cost. FedEx, on the other hand, has focused on achieving flexibility to meet the needs of its various customer segments. The higher costs of this decentralized approach to IT management are offset by the benefits of localized innovation and a heightened ability to respond to customers' needs.

Of course, UPS also uses technology to meet the needs of individual customers, and FedEx uses technology to provide consistent service across customer segments. But the thrusts of the two companies' IT and business strategies are different. Both are successful because they have matched their spending levels to those strategies—not to industry benchmarks.

In most companies, senior management has not defined IT's role so clearly, in effect abdicating that responsibility to IT people. In those organizations, the IT department can deliver on individual projects but can't build a "strategic platform," one that not only responds to immediate needs but also provides escalating benefits over the long term.

UPS's experience illustrates the benefits of a broad strategic platform. The company began investing heavily in IT in the late 1980s, at a time when FedEx was touting its package-tracking capability. But instead of simply creating a tracking system, UPS's senior management decided to build a comprehensive package database that had the potential to become a platform for numerous applications. To gather information for the database, UPS developed the Delivery Information Acquisition

Jeanne W. Ross is a principal research scientist and **Peter Weill** is a senior research scientist and the director of the Center for Information Systems Research at the Massachusetts Institute of Technology's Sloan School of Management, in Cambridge, Massachusetts.

Device, a handheld computer used by drivers to collect customers' signatures and other information electronically. The device saved drivers 30 minutes a day by reducing the manual input of delivery information. But these electronic tracking capabilities were only an initial benefit. The electronic data provided a more accurate record of deliveries, enabling UPS to collect hundreds of millions of dollars in revenues that had been lost when customers self-reported deliveries, which UPS couldn't easily verify. In subsequent years, the database allowed UPS to introduce new products, such as guaranteed delivery, and new processes, including on-line package tracking by customers. Recent enhancements will optimize the scheduling of routes and help UPS's business customers get paid faster once their goods are delivered.

Those benefits grew out of UPS's decision to make significant and consistent investments in a system that, before long, outgrew its original purpose. UPS's CEO, Mike Eskew, calls the new applications, each of which furthers the strategy of providing consistent and reliable customer service, "happy surprises." Such unforeseen benefits lead to a total return on IT investment that exceeds the sum of the ROIs of individual projects—a return far greater than many companies can imagine.

IT spending can be designed to meet immediate needs and allow for an array of future benefits only if IT and business goals are clearly defined. Some management teams offer only a vague vision—for example, "providing information to anyone, anytime, anywhere." IT units respond to such ill-defined goals by trying to build platforms capable of

What Happens When Senior Managers Ignore Their IT Responsibilities?

	IT Decision	Senior Management's Role	Consequences of Abdicating the Decision
Strategy	How much should we spend on IT?	Define the strategic role that IT will play in the company and then determine the level of funding needed to achieve that objective.	The company fails to develop an IT platform that furthers its strategy, despite high IT spending.
Strategy	Which business processes should receive our IT dollars?	Make clear decisions about which IT initiatives will and will not be funded.	A lack of focus overwhelms the IT unit, which tries to deliver many projects that may have little companywide value or can't be implemented well simultaneously.
Strategy	Which IT capabilities need to be companywide?	Decide which IT capabilities should be provided centrally and which should be developed by individual businesses.	Excessive technical and process standardization limits the flexibility of business units, or frequent exceptions to the standards increase costs and limit business synergies.
Execution	How good do our IT services really need to be?	Decide which features – for example, enhanced reliability or response time – are needed on the basis of their costs and benefits.	The company may pay for service options that, given its priorities, aren't worth the costs.
Execution	What security and privacy risks will we accept?	Lead the decision making on the trade-offs between security and privacy on one hand and convenience on the other.	An overemphasis on security and privacy may inconvenience customers, employees, and suppliers; an underemphasis may make data vulnerable.
Execution	Whom do we blame if an IT initiative fails?	Assign a business executive to be accountable for every IT project; monitor business metrics.	The business value of systems is never realized.

responding to any business need. Not surprisingly, the typical outcome of such large, undirected projects is millions of dollars spent chasing elusive benefits.

2
Which business processes should receive our IT dollars?

As most executives know, IT initiatives can multiply quickly. We have seen companies of a few hundred people that have a few hundred IT projects under way. Clearly, not all of them are equally important. But we find that senior managers are often reluctant to step in and choose between the projects that will have a significant impact on the company's success and those that provide some benefits but aren't essential.

Leaving such decisions in the hands of the IT department means that IT executives set the priorities for what are in fact important business issues—or, just as troubling, they try to deliver on every project a business manager claims is important. Presented with a list of approved and funded projects, most IT units will do their best to carry them out. But this typically leads to a backlog of delayed initiatives and an overwhelmed and demoralized IT department.

The failure of senior managers to choose a manageable set of IT priorities can also lead to disaster. One need only remember Hershey Foods' infamous decision in 1999 to implement several major systems simultaneously, including CRM, ERP, and supply chain management, which ultimately resulted in the company's inability to deliver candy to important customers during the Halloween season.

Contrast this with Delta Air Lines' disciplined approach to IT investment in recent years. In 1997, the company was facing a technology crisis. Several years before, the airline had outsourced its corporate IT function, which prompted individual business units, unhappy with the service they were receiving, to create their own IT capabilities. (For a discussion of outsourcing, see the sidebar "Why Not Just Outsource IT?") Running disparate systems across the units made it difficult for employees to provide timely, accurate customer service. One question—for example, "At what gate will my plane arrive?"—could conceivably generate 17 different answers, depending on which system an employee checked. In addition, many of the systems were based on older technologies that might not perform properly with the arrival of the year 2000.

In a move as farsighted as UPS's decision to create a package database, Delta's senior man-

Why Not Just Outsource IT?

Given the potential headaches of managing IT, it is tempting to hand the job over to someone else. Indeed, outsourcing once appeared to be a simple solution to management frustrations, and senior management teams at many companies negotiated contracts with large service providers to run their entire IT functions. At a minimum, these providers were often able to provide IT capabilities for a lower cost and with fewer hassles than the companies had been able to themselves.

But many of these outsourcing arrangements resulted in dissatisfaction, particularly as a company's business needs changed. Service providers, with their standard offerings and detailed contracts, provided IT capabilities that weren't flexible enough to meet changing requirements, and they often seemed slow to respond to problems. Furthermore, a relationship with a supplier often required substantial investments of money and time, which entrenched that supplier in the company's strategic planning and business processes. The company then became particularly vulnerable if the supplier failed to meet its contractual obligations.

Not surprisingly, other problems arose because senior managers, in choosing to outsource the IT function, were also outsourcing responsibility for one or more of the crucial decisions they should have been making themselves. Indeed, companies often hired outside providers because they were dissatisfied with the performance of their own IT departments—but that dissatisfaction was primarily the result of their own lack of involvement.

In light of this track record, most bigger companies, at least, are deciding to keep their main IT capabilities in-house. But many engage in selective outsourcing. Good candidates for this are commodity services—such as telecommunications, in which there are several competing suppliers and specifications are easy to set—and services involving technologies with which the company lacks expertise.

Unlike decisions to outsource the entire IT function, selective outsourcing decisions are usually best left to the IT unit—assuming that senior management has taken responsibility for the six key decisions. For example, once the acceptable level of security and privacy risk is determined, IT executives can research competitive offerings and conduct the cost-benefit analysis for completing these projects internally versus externally.

agers opted to use the Y2K threat to build a powerful technology platform, dubbed the Delta Nervous System (DNS), to provide real-time information for flight operations and customer service. The three-year, $1 billion project would provide every employee with constant updates on the status of any flight or customer. As the managers defined the vision for this system, they made another critical decision: They would not invest simultaneously in a new revenue-planning system. Such systems help airlines make complex decisions concerning scheduling, pricing, equipment configuration, and routing that directly affect profitability. But Delta knew it couldn't address all of its technology needs at once. Given the limitations of the company's IT and business resources, additional projects would have threatened the success of the DNS. So the company put a new revenue-planning system, also key to Delta's strategy, on hold until 2002, when the DNS was in place.

3
Which IT capabilities need to be companywide?

Increasingly, executives are recognizing the significant cost savings and strategic benefits that come from centralizing IT capabilities and standardizing IT infrastructure across an organization. This approach leverages technology expertise across the company, permits large and cost-effective contracts with software suppliers, and facilitates global business processes. At the same time, though, standards can restrict the flexibility of individual business units, limit the company's responsiveness to differentiated customer segments, and generate strong resistance from business unit managers.

When IT executives are left to make decisions about what will and will not be centralized and standardized, they typically take one of two approaches. Depending on the company's culture, either they insist on standardizing everything to keep costs low or, recognizing the importance of business unit autonomy, they grant exceptions to corporate standards to any business unit manager who raises a stink. The former approach restricts the flexibility of business units; the latter is expensive and limits business synergies. In some instances, systems using different standards can actually work against one another, resulting in a corporate IT infrastructure whose total value may be *less* than the sum of its parts. Consequently, senior managers should play the lead role in weighing these crucial trade-offs.

The experience of Johnson & Johnson, the global consumer and health care company, illustrates the challenges of achieving the right balance when trying to impose companywide standards. For almost 100 years, J&J enjoyed success as a decentralized organization. By the early 1990s, though, it had encountered a powerful new breed of customer with no patience for the multiple salespersons, invoices, and shipments that resulted from doing business with more than one of the company's roughly 200 operating units. J&J's management had to decide how to reconcile the growing need to act as a unified company with its historical preference for business unit autonomy. IT would be central to the resolution.

A key IT decision involved data standards. Senior managers quickly realized that global data definitions, which would facilitate information sharing among business units, would be difficult to implement. Over the years, data items such as product codes, product costs, and customer accounts had been defined locally to meet the needs of operating units in different countries. Accordingly, the company's senior managers formed a team to define the limited set of standard data definitions needed to provide a single view of the customer. The remainder could be determined at the regional or business unit level. Achieving a single view of the customer also required a single technology base, one that allowed electronic communication across units. So J&J broke with tradition and instituted corporate, rather than business unit, funding for the implementation of a standardized workstation with a standardized interface to J&J corporate systems and data. Over time, J&J has continued to shift IT capabilities from the business units to centralized systems. It has moved cautiously, though, recognizing that a sudden shift to a more standardized environment could be disruptive.

Management teams in every company, whether centralized or decentralized, must constantly assess the balance between companywide and business-unit IT capabilities. Traditionally centralized organizations like UPS find that their shared infrastructures sometimes do not meet the needs of new,

smaller businesses. Thus, they have gradually introduced some localized capabilities in the same way that the traditionally diversified J&J has introduced centralized ones.

4
How good do our IT services really need to be?

An IT system that doesn't work is useless. But that doesn't mean every system must be wrapped in gold-plated functionality. Characteristics such as reliability, responsiveness, and data accessibility come at a cost. It is up to senior managers to decide how much they are willing to spend for various features and services.

For some companies, top-of-the-line service is not negotiable. Investment banks do not debate how much data they can afford to lose if a trading system crashes; 100% recovery is a requirement. Similarly, Gtech Corporation, the company that runs the majority of the world's government-sponsored lotteries, cannot compromise on response time. Most of its contracts in the United States specify that customers will receive their lottery tickets within five seconds—and it takes three seconds just to print the ticket. Nor can Gtech afford any downtime: State governments specify penalties as high as $10,000 per minute if the system is unavailable. This is a fairly compelling justification for ensuring that computers will continue to run despite floods, tornadoes, power outages, and telecommunications breakdowns, regardless of the cost.

But not every company is a Gtech or a Merrill Lynch. Most can tolerate limited downtime or occasionally slow response times, and they must weigh the problems these create against the cost of preventing them. Consider Dow Corning. The nature of the company's operations means that a brief downtime of its ERP system would be an inconvenience but would not stop production or result in lost customer orders. Although senior managers wanted to prevent all downtime, the cost was prohibitive. So in 1999, when they decided to build a backup, or "hot," site, they opted for one that would be used only if the system went down for several hours. The company periodically reviews its backup capability and in the past few years has been able to reduce its risk even more as technologies become more affordable.

Decisions concerning the appropriate levels of IT service need to be made by senior business managers. Left to their own devices, IT units are likely to opt for the highest levels—providing Cadillac service when a Buick will do—because the IT unit will be judged on such things as how often the system goes down. Typically, the cost of higher levels of service is built into the price of IT systems and is neither broken out nor discussed separately. IT people should provide a menu of service options and prices to help managers understand what they are paying for. Business managers should then, in consultation with IT managers, determine the appropriate level of service at a price they can afford.

This kind of analysis can have an impact not only on onetime IT investments but also on annual operating costs, a contentious issue at many companies. In many cases, fixed costs can be significantly reduced if managers establish, during system development, lower expectations for requirements such as reliability and response time. Conversely, the analysis might reveal that the company is underestimating its risk of downtime and has not sufficiently protected itself against it.

5
What security and privacy risks will we accept?

Security, like reliability and responsiveness, is a feature of IT systems that requires companies to weigh the level of protection they want against the amount they are willing to spend. In this case, though, there is another trade-off: Increasing security involves not only higher costs but also greater inconvenience.

Take our own organization, MIT. Because the institute is a particularly attractive target for hackers keen to show off their skills, MIT has developed a state-of-the-art security system that successfully repels a continuous stream of attacks. It features a firewall different from the type most organizations use to limit external access to their internal systems. But although it provides greater protection, MIT's nonstandard approach means that the institute cannot install most commercial software packages for applications such as course registration and student accounting. MIT sees these limitations as a cost of doing business, but many private companies would likely find such extraordi-

nary security efforts to be too costly and onerous.

As global privacy protections increasingly become mandated by government, security takes on new importance: Well-designed privacy protections can be compromised by inadequate system security. Yale University's decision to allow applicants access to their admissions decision by providing their dates of birth and Social Security numbers, while convenient for users, allowed an official at Princeton University, which was competing for the same students, to access the site with ease. Financial services firms face similar threats when they design systems that give customers quick and easy electronic access to their accounts. Telephone companies that allow on-line payment of bills render vulnerable the records of customers' telephone calls. In every case, these organizations are—consciously or not—making the trade-offs between customers' convenience and privacy.

It is up to senior managers to assess those trade-offs. Many IT units will adopt a philosophy that absolute security is its responsibility and will simply deny access anytime it cannot be provided safely. But try running that idea by a bank's marketing executives, who are counting on simplified on-line transactions to attract new customers.

6

Whom do we blame if an IT initiative fails?

The recurring concern we hear from executives in our courses—that IT efforts fail to generate the intended business benefits—is often accompanied by some finger-pointing: There must be something wrong with the IT function in our company. We have found, however, that the problem more often reveals that something is wrong with the way non-IT executives are managing IT-enabled change in the organization.

Look at those well-publicized examples of ERP and CRM initiatives that never generated measurable value. Invariably, the failures resulted from assumptions that IT units or consultants could implement the systems while business managers went about their daily tasks. In fact, new systems alone have no value; value derives from new or redesigned business processes. We recall the experience of a midsize manufacturing company that had installed an expensive ERP system with no apparent impact. A new CEO came on board and, impressed by the system's potential and the fact that no one was using it, reorganized the company's business processes to take advantage of its capabilities. He attributed the company's ability to turn a profit for the first time in five years to this reorganization. Think of the benefits that might have been realized if the system had been designed to serve specific processes in the first place.

To avoid disasters, senior managers need to assign business executives to take responsibility for realizing the business benefits of an IT initiative. These "sponsors" need authority to assign resources to projects and time to oversee the creation and implementation of those projects. They should meet regularly with IT personnel, arrange training for users, and work with the IT department to establish clear metrics for determining the initiative's success. Such sponsors can ensure that new IT systems deliver real business value; blaming the IT department reflects a misunderstanding about what that group can deliver.

IT success may also require a sustained commitment on the part of the managers who will use and benefit from the technology. Take the case of the Longitudinal Medical Record system, introduced in 1998 at Partners HealthCare, a Boston-based umbrella organization of major hospitals and local clinics. From the beginning, the managers—in this case, a cadre of practicing physicians in management roles—took full responsibility for extracting value from the LMR's new technology. For every patient they see, the physicians are supposed to enter electronically, in a standard format, all diagnosis and treatment information so that the system can highlight key facts for physicians examining the patient in the future. Deploying the LMR posed significant technological challenges, but the greater challenges were organizational: The system required physicians to spend precious time on data entry using a tool that was far from perfect in its early versions.

The physicians participating in the initiative have continued to play a role in the development of this IT system, a role that goes far beyond helping to define requirements. They must use the system (even though the technology sometimes breaks down), provide constant

feedback on its features (so the IT unit can make continual improvements), and encourage colleagues to sign on to the project (because its value is limited until its use becomes widespread).

Unless managers take responsibility for the success—and failure—of IT systems, they will end up with systems that, while perhaps technically elegant, will have no impact on the business. The IT department should be held responsible for delivering systems that are on time and on budget and that have the potential to be both useful and used. But only business executives can be held responsible for making the organizational changes needed to generate business value from a new system. Until they accept this responsibility, companies cannot hope to eliminate complaints about having spent too much money for too little value.

• • •

While we firmly believe that senior business executives err when they abdicate responsibility for these six IT decisions, we aren't advocating that any of the decisions be made unilaterally in the executive suite. Clearly, such complex issues can't be dealt with in a single senior management meeting at which executives lay down mandates for IT spending, management, and use. Although senior managers need to ensure that IT spending and initiatives are aligned with and further the company's strategy and goals, such decisions are best made with input from both business unit and IT executives.

Instead of approaching IT decision making in an ad hoc manner, companies increasingly are establishing formal IT governance structures that specify how IT decisions are made, carried out, reinforced, and even challenged. Such structures apply principles similar to those of financial governance—for example, who is authorized to commit the company to a contract or how cash flow is managed across the enterprise.

A company can choose from a variety of fundamentally different governance approaches depending on its culture, strategy, and structure. But good IT governance identifies who should be responsible and accountable for critical IT decisions. For example, decisions about IT investment are often made as part of the companywide budgeting process approved by senior management. Decisions about IT architectures and the associated standards are often made by committees with both technical and business membership. In all cases, though, effective governance ensures that IT-related decisions embody uniform principles about the role IT plays in the organization.

IT has long been a key to the success of State Street Corporation, a leading global financial-services firm. But although nearly one-quarter of its operating expense budget typically has been devoted to technology, until recently there was no companywide IT budget, and almost all spending decisions were made by the individual business units. To ensure that IT decisions supported the company's new strategy of presenting a single face to customers across business units, State Street recently established an Information Technology Executive Committee. The committee, whose members include the COO, the CIO, and the heads of the business units, meets every two months. It is responsible for setting IT direction within the context of State Street's strategy and then balancing companywide and business unit needs to create a single IT budget for the company.

Under State Street's IT governance structure, the CIO plays an active role in setting the company's IT strategy and facilitating the effective use of IT. At the same time, however, note the level of commitment shown by the company's business leaders, including the COO. In that sense, State Street is an illustration of the proposition that there are key IT decisions your IT people shouldn't make—on their own.

Reprint R0211F; *Harvard Business Review* OnPoint 2160
To order, see the next page
or call 800-988-0886 or 617-783-7500
or go to www.hbr.org

Harvard Business Review OnPoint

Harvard Business Review OnPoint articles enhance the full-text article with a summary of its key points and a selection of its company examples to help you quickly absorb and apply the concepts. *Harvard Business Review* OnPoint collections include three OnPoint articles and an overview comparing the various perspectives on a specific topic.

Further Reading

Six IT Decisions Your IT People Shouldn't Make is also part of the *Harvard Business Review* OnPoint collection **Making IT Matter,** Product no. 5895, which includes these additional articles:

Getting IT Right
Charlie S. Feld and Donna B. Stoddard
Harvard Business Review
February 2004
Product no. 5905

Putting the Enterprise into the Enterprise System
Thomas H. Davenport
Harvard Business Review
May 2003
Product no. 3574

Harvard Business Review

To Order

For reprints, *Harvard Business Review* OnPoint orders, and subscriptions to *Harvard Business Review:*
Call 800-988-0886 or 617-783-7500.
Go to www.hbr.org

For customized and quantity orders of reprints and *Harvard Business Review* OnPoint products:
Call Frank Tamoshunas at 617-783-7626,
or e-mail him at ftamoshunas@hbsp.harvard.edu