CHAPTER

10

Global, Ethics, and Security Management

LEARNING OBJECTIVES

After reading this chapter, you should be able to:

- Learn generally about outsourcing and more specifically offshore outsourcing (offshoring) and their business and cultural implications, as well as the Software as a Service (SaaS) model.
- Know the ethical and legal issues related to ERP systems and implementations and how to protect the company assets.
- Understand the various components to system security and why security must be planned, tested, and ready by the time the ERP implementation is at Go-live.
- Understand green computing phenomenon and ERP's role in green IT.
- Examine the impact of compliance and of laws such as the Sarbanes–Oxley Act on ERP implementations.

CASE 10-1

Opening Case

Outsourcing at FERC

Source: Based on McKenna, E. (March 5, 2001). Enterprise Computing Rings in a New Era, *Washington Technology.*

The Federal Energy Regulatory Commission (FERC), an independent regulatory agency within the Energy Department, was one of the first federal agencies to use an integrated enterprise resource planning application from start to finish, including human resources, base benefits, time and labor, and payroll. In October 2000, FERC implemented PeopleSoft Financial Management for Education and Government software, including the general ledger, payables, and purchasing modules. The two systems cost about $5 million for implementation and maintenance. According to Janet Dubbert, FERC's director of management administrative and payroll support, the agency's decision to acquire the systems was prompted by a couple of issues. First, the Department of Energy would no longer support FERC's human resource, time and attendance, and payroll functions. The department made the move as part of its efforts to streamline operations under the National Performance Review. Second, the ERP systems allow the agency to add functionality at its own pace. Because the systems are integrated, they provide real-time management information to help with workforce planning efforts.

In 2001, FERC decided to outsource the ERP system to the private sector. Dubbert said, "FERC will pay less than $2 million for the hosting and day-to-day management of its human resources and financial operations, including transition and production costs, under a five-year contract." The key reasons to outsource were to relieve FERC from maintaining, upgrading, and distributing software and services to its customers, who pay a periodic fee. FERC moved to this arrangement after it began re-engineering its operations using PeopleSoft Human Resources Management for the U.S. federal government. After contracting with PeopleSoft, Inc., the organization went live with the human resources application in less than six months. With outsourcing, FERC hopes to focus on its core functions of adding new human resources and financial features, such as training and budget and accounts receivable.

- Do you agree with FERC's decision?
- What other benefits can FERC achieve with this outsourcing agreement?

PREVIEW

The rationale for outsourcing is compelling. As seen in the FERC case, outsourcing an ERP environment is not new. The key benefits of outsourcing for FERC were a predictable monthly payment and the avoidance of the headache of running the application. From the FERC perspective this was therefore a good decision. In general, outsourcing helps organizations to lower the high software ownership and maintenance costs; simplify, or eliminate, or both, the traditional difficulties in implementation; and avoid the problems of hiring and retaining IT staff to run the applications. Today, more and more organizations find outsourcing to be a better strategy for lowering the maintenance costs of ERP systems. For example, three months after the implementation

of a SAP R3 system, it was outsourced at Sebastian International, Inc., Woodland Hills, California. "Confronted by unacceptable system performance and the loss of key IT personnel, we made the decision to outsource," said Dianne King, director of IT. "We probably would have saved quite a bit if we had outsourced right at the beginning."[1] Companies thinking of outsourcing, however, need to have a strategy that is appropriate for their organizations. Management needs to evaluate whether it makes sense from both a cost and quality perspective and to make decisions on what should be outsourced and how. Outsourcing should not be used to abdicate responsibility. It requires proper oversight and a well-defined relationship with the outsourced partner.

In addition to outsourcing, this chapter will focus on the issues of ethics, legal environments, and security with ERP systems. ERP and other enterprise systems generally have a broad-based impact on organization structure, process, and people. They can also change the ethical and legal environment of the organization. Security is another major concern, both during and after the ERP implementation. ERP systems, with their power of integration and their ability to link with external systems, can create major havoc or disaster when a hacker or virus infiltrates the system's security perimeter.

OUTSOURCING

What Is Outsourcing?

Outsourcing occurs anytime a company decides to subcontract its business processes or functions to another company; therefore, instead of hiring employees to perform a task, the company (*outsourcer*) enters into an outsourcing arrangement with another firm (*outsourcee*) to provide these services under contract for a certain price and period. As mentioned earlier, outsourcing in the ERP area has been successfully used by organizations worldwide for some time. Peter Drucker,[2] the famous management guru, gave his blessing to outsourcing in 1995 when he predicted that "in 10 to 15 years organizations may be outsourcing all work that is 'support' rather than revenue producing, and all activities that do not offer career opportunities into senior management." Although he may be referring to outsourcing in general, Drucker's prediction has reached early fruition in the IT industry and ERP system.

Even as early as 2000, two respected IT research firms, Forrester Research, Inc., Cambridge, Massachusetts, and Syntacom IT-Services, Inc., Waltham, Massachusetts, had predicted ERP outsourcing to become a $6.4 billion market by 2001 with 50 percent of all ERP implementations outsourced by 2006, respectively.[3] High IT spending has been on the radar of top management in recent years, and the chief information officers (CIOs) are being asked to do more with less. Several key trends exist in ERP deployments that are helping implementation teams exploit technology in new ways to improve quality and reduce costs. Offshoring capabilities have strengthened over the years through the emergence of new global players, and they have allowed many organizations to take advantage of highly skilled labor at more cost-effective prices. Outsourcing (i.e., the delivery of IT and application software via service-oriented architecture (SOA) and Web services) is a new model that provides better value for customers than the traditional model of purchasing software licenses, installing the

[1] Teresko, J. (September 6, 1999). ERP Outsourcing: Can I Meet Market Demands? *Industry Week Magazine.*
[2] Drucker, P. (1995). Why Buy When You Can Rent? *Harvard Business Review.*
[3] Travis, L., and Stiffler, D. (2005). Offshoring Decisions for 2005 Time to Consider a New Model. www.amrresearch.com/Content/View/asp?pmillid=17890 (accessed January 14, 2005).

software, and managing application upgrades with internal resources.[4] In both cases, ERP teams face the challenge of integrating external partners with their global IT and business community.

Most IT outsourcing initially occurred in such back-office functions as technical support, software development, and maintenance areas. This was mainly triggered, in the mid- to late 1990s, by the Y2K (year 2000) software problems. The urgency in fixing these problems created a tremendous shortage for IT personnel and triggered an outsourcing boom in which U.S. and European companies hired a large number of software programmers and developers from all over the globe from such countries as India, Russia, and Ireland. The Y2K problem gave a major boost for IT outsourcing because it provided tremendous cost savings for these companies. This eventually progressed into other IT functions within the organization, where management of many companies figured that outsourcing was both cost-effective and provided tremendous flexibility. Many companies slowly started moving to front-office functions (e.g., customer support and help desk, call center functions, customer relationship management, and sales force automation). The front-office function generally includes IT solutions and support that have direct interaction with the customer. This area can be risky because many companies feel customers are too important to turn over to someone outside, particularly if the outsourcing company is from a different country (offshore) with a different cultural background. Therefore, it is very important for all parties to define their outsourcing relationship similar to one shown in Figure 10-1.

Organizations planning on ERP software are probably too wrapped up in implementation to worry about how they will maintain and update the system in the future. Most experts, however, say that in order to maximize your benefits, the sooner you start thinking of this the better. The benefits for ERP outsourcing depend on the organization. There are many other benefits beyond

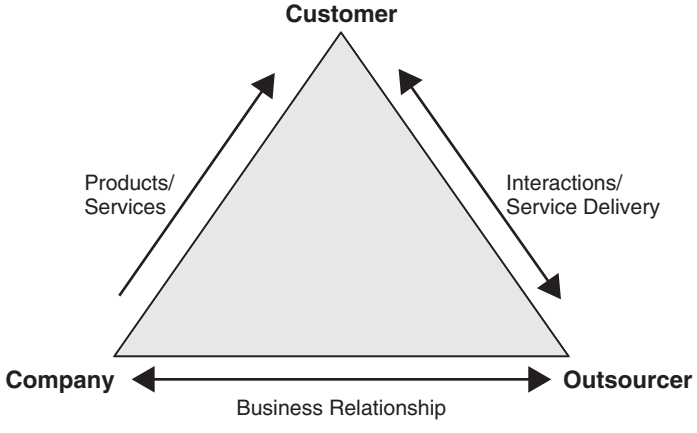

FIGURE 10-1 Outsourcing Relationship.

[4] Howarth, F. (September 16, 2005). Software as a Service-Salesforce.com's New Application Shop. *Practice Leader.* Bloor Research, Publisher: IT Analysis Communications Ltd. www.it-director.com/services/content.php?cid=8075 (accessed June 2007).

cost savings when management considers outsourcing as a business strategy. Some of the key benefits of outsourcing are as follows:

- ***Economics.*** Outsourcing provides a predictable monthly payment. A company can solve all of the problems of running an application at a lower cost. Outsourcing enterprise applications can save a company anywhere from 30 to 50 percent, depending on the task, method, location, and how the relationships are structured.[5]
- ***Market agility.*** Outsourcing the ERP function offers a faster time to solution and removes a major distraction from a company's core competence.
- ***Breadth of skills.*** Many organizations do not have in-house personnel with ERP implementation and maintenance skills. Outsourcing provides an avenue to access these advanced expertise areas quickly.
- ***Technical expertise.*** Outsourcing arrangements cost-effectively enable a company to provide access to cutting-edge IT solutions to its employees and clients. Such service providers as Accenture and IBM typically have alliances with such key ERP vendors as SAP and Oracle, which puts them in the loop of the newest and latest changes in the applications.
- ***Multiple feedback points.*** Outsourcing provides an organization with an outside or external perspective during implementation and maintenance.
- ***Best practices.*** Outsourcing can provide companies with access to best practices in ERP planning, implementation, and maintenance.
- ***Scalability.*** One secondary benefit to outsourcing is flexibility for the company to grow or shrink quickly, depending on the market demand for its products and services. Outsourcing agreements allow companies to scale their service agreements with minimal disruption as opposed to doing them in-house.
- ***Process-oriented.*** Outsourcing, by default, forces process perspective (i.e., cross-functional teams, customer focus) rather than a functional perspective, which is common inside organizations. This ensures timely delivery of quality solutions at lower costs.
- ***Solution centric.*** Outsourcing allows companies to work with both third-party components and custom-developed code to meet ERP requirements at the best-possible value.
- ***Upgrade crunch.*** ERP systems are high-maintenance software that requires constant upgrading and patching after implementation. It is hard for most businesses to keep up with these constant maintenance cycles, especially if they have customized the ERP application during installation.
- ***Fear of distraction.*** Outsourcing allows the company employees to focus on their core competencies and not get distracted by activities that lower employee productivity.

Outsourcing Drawbacks

Many organizations do not want to trouble themselves with outsourcing. For example, Allegiance Healthcare Corp. of McGaw Park, Illinois, a 20,000-employee, $4.5 billion medical products company, decided to go in-house on its ERP implementation and maintenance. CIO Kathy White did give the outsourcing option serious consideration, but found it wanting for both reliability and cost-effectiveness. What is there not to like about outsourcing? ERP outsourcing is still a relatively new concept compared with IT outsourcing, which is simpler and involves

[5] Travis. Offshoring Decisions for 2005.

external companies operating your data centers (or IT support) either on-site or remotely. Some of the key drawbacks are as follows:

- ***Lack of expertise.*** ERP outsourcing model targets an application that may need integration with other applications and systems in the organization. An external company may not know or have the expertise to understand the in-house-developed application or how to accommodate ERP extensions like barcode data collection, warehouse management, and e-commerce. For example, a company planning an internal e-commerce implementation while seeking to outsource ERP might discover little or no cost benefit in terms of IT staffing.
- ***Misaligned expectations.*** Companies outsourcing often cannot anticipate changes in their business circumstances or in technology, resulting in surprise charges, delayed delivery, or delivery of wrong products and services. Misunderstandings can often occur between the outsourcer and the organizations.
- ***Culture clash.*** The business processes and mannerisms followed by the outsourcing organization could be very different from the organization's culture. The work habits, communication processes, and reporting habits can be very different, causing enormous tensions in the outsourcing relationships.
- ***Hidden costs.*** Surprise or unanticipated charges like travel costs, monitoring costs, lower productivity, and long-term loss of relationships with clients are hard to determine. The cost savings can often turn out to be a myth.
- ***Loss of vision.*** Outsourcing arrangements often result in a loss of institutional knowledge (e.g., feedback from clients, problem-solving capability, and new idea generation).
- ***Security and control.*** Outsourcing requires companies to share their trade secrets, which can be risky in a competitive environment. Companies have little control over employees of outsourcees, especially in global or high-turnover markets. Protection and control of intellectual property can be a critical issue when companies outsource. Companies therefore need to sign comprehensive service-level agreements to protect themselves and their partners.

Offshore Outsourcing

In recent years, outsourcing has become a global industry. When a company selects an outsourcing partner (outsourcee) from another country, it is called *offshoring,* as shown in Figure 10-2. Offshore partners are often selected from developing countries to lower the labor costs. The latest trends in IT implementations call for offshoring critical developmental tasks to improve quality, reduce costs, and speed delivery. According to AMR research, "The effective use of offshore resources means being able to do more with less. Users of offshore services for ERP implementation and support can expect savings between 15 and 20 percent the first year of the relationship, growing to 40–50 percent in ensuing years."[6]

Countries like India have a big IT industry that provides services in design, development, implementation, support, and help desk, while other developing nations are slowly emerging (e.g., Brazil, Argentina, China, Eastern Europe, Russia, and the Philippines). Three Indian IT companies (i.e., Infosys, Tata Consulting Services (TCS), and Wipro) each reported respective revenue growth of 51 percent, 44 percent, and 47 percent in Q404 more than Q304 in a $12.5 billion market in 2004 and over $16 billion in 2005. Because the worldwide spending on IT and offshoring services is estimated to be $600 billion, India accounts for only 2 percent of the total amount.[7] These global contenders are proving to be as innovative and expertly run as

[6] www.amrresearch.com/Content/View.asp?pmillid=17633 (accessed February 2001).
[7] www.amrresearch.com/Content/View.asp?pmillid=17723 (accessed February 2001).

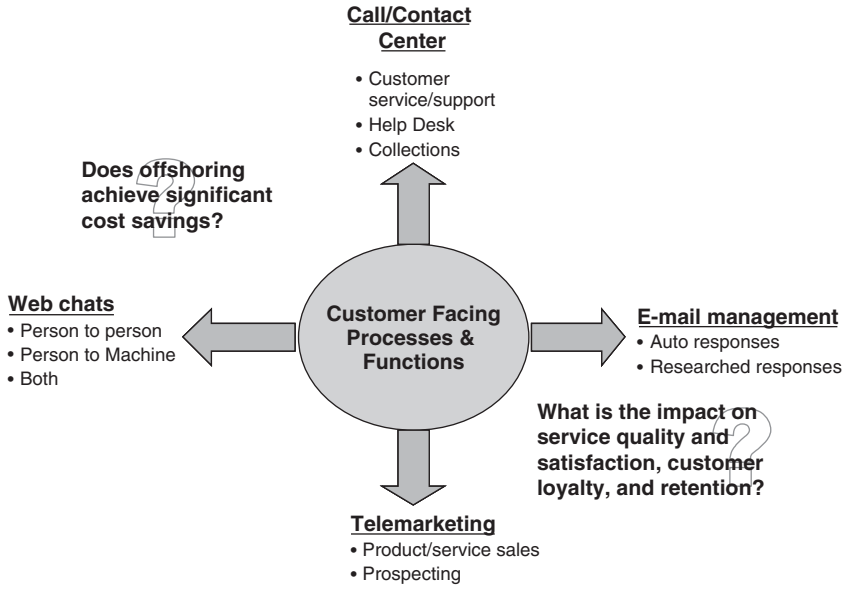

FIGURE 10-2 Offshore Outsourcing.

any in the business, intelligently absorbing consumer trends and technologies. "Their key advantages are access to some of the world's most dynamic growth markets and immense pools of low-cost resources, be they production workers, engineers, land, petroleum, or iron ore."[8]

With global ERP implementation teams, however, it is usually not cost-effective to colocate all team members. A successful ERP implementation team will recognize the potential risks associated with global offshoring due to differences in language and culture. The team will also recognize the importance of adhering to the highest of ethical standards (i.e., delivering a final product that secures and protects the organization, promotes financial growth, and provides significant return on investment to executives, board members, and public shareholders).

For a significant systems implementation like ERP, organizational change management plays a very important role. Offshore implementers can face barriers of language, culture, and values, making the ERP implementation more challenging. One example of language barrier is accent difference: Getting key messages to team members and frontline end users can be a delicate and complex issue. Savvy project managers will acknowledge the communication challenges and take the time to translate and distribute key messages through multiple channels to reach its intended audience effectively. Furthermore, not all people around the world are motivated by the same things that motivate Western society. Many Western countries value history, tradition, and work–life balance, whereas many countries in Eastern Europe and Asia value hard work, entrepreneurship, and teamwork.[9]

Offshoring requires consideration of the organization's local requirements, understanding of best practices, and an overall willingness to change. Each country is going to have its own set

[8] www.businessweek.com/magazine/content/06_31/b3995001.htm (accessed February 2001).
[9] http://blogs.ittoolbox.com/erp/roi/archives/its-not-a-small-world-after-all-managing-change-on-international-erp-projects-8437 (accessed February 2001).

of local requirements—whether they are currency related, regulatory, resource, or employee constraints (e.g., the high number of bank holidays and shorter workweeks in some European nations). Global ERP systems are equipped with handling foreign currency exchanges and value-added tax (VAT),[10] two critical areas that enable financial consolidation in complex organizations with multiple company codes. Employees in different countries also have different views on "best practices," and their belief in its effectiveness can impact the amount of justification required to support the change in business process.

Finally, different countries have varying desires to change. More-developed countries have business operations that have worked for decades, whereas many developing nations have less-mature operational models. Local culture and available resources will dictate how willing the organizational unit will be able to embrace the change required by the new ERP system. Completely localizing an ERP system increases complexity and customization, while defeating the purpose of a global solution. Corporate and local office management needs to be clear in the message for global change.

GLOBAL ERP VENDOR SELECTION In order to create a successful outsourcing or offshoring project, companies need to perform due diligence in vendor selection. When evaluating an outsourcing partner, ERP selection teams should consider financial status, technical certifications, licenses, qualifications, and related work experience (e.g., familiarity with the industry). The employees of the offshore provider are also critical: What are the working conditions like, and what kind of retention policies are in place? This is a very critical issue for security where personnel could suddenly leave the offshore service provider and go to work for your top competitor without your knowing or approval. "In the U.S. [there are] strict controls on intellectual property rights and noncompete clauses, but if you're hiring overseas much of that goes out the window. Your competitor can outsource with a firm that works down the street from your outsourcer and advise them to hire the 10-person team that works on your projects."[11] Companies also need to be prepared if the offshore experiment is a disaster: What do you do about it? Can you bring the project in-house? For this reason, a careful risk assessment needs to take place before any offshore services contract is signed.

One of the biggest challenges facing companies that offshore their ERP initiatives is culture. Making sure that your company culture meshes with that of your offshore partner ensures a successful implementation. Cultural differences include such tangible discrepancies as time zone and language or such intangible differences as nationalism or corporate pride. Dion DeLoof, CEO of Anteo Group, a project-based IT staffing and consulting firm in Atlanta, said "many of his clients have sent IT projects to India only to find out that hard-to-quantify attributes like innovation and creativity are lacking and that people there do not have the freedom to speak up or the entrepreneurial culture that rewards them if they tell their boss what they're really thinking."[12] Companies that decide to offshore their ERP projects should be prudent about the total cost of outsourcing. Securing cheaper rates for SAP or Oracle developers in India might look good on paper, but when savvy managers factor in time required for contract setup and management, time differences, travel and communication costs, and reduced productivity due to language and cultural differences, the total cost of outsourcing may not be as attractive as it was initially.

---

[10] http://en.wikipedia.org/wiki/Value_added_tax (accessed February 2001).
[11] www.projectsatwork.com/article.cfm?ID=223467 (accessed February 2001).
[12] Ibid.

Software as a Service (SaaS)

Software as a Service (SaaS) is a model of software that can be rented or leased from a software vendor that provides maintenance, daily technical operation, and support for the software. SaaS is a model of software delivery rather than a market segment; it assumes the software is delivered over a secure Internet connection. Software can be accessed from a browser by any market segment, including home consumers and small, medium, and large businesses. The SaaS model brings lower risk in the implementation cycle and better knowledge transfer from integrators to users of systems. "When the implementation partner leaves, the implementing hosting vendor is still there managing the solution. So the knowledge transfer happens seamlessly, automatically, for no additional cost, no impact on schedule, and, of course, lowering risk. With conventional implementations the opportunity exists for disconnects that could hamper the knowledge-transfer process to the customer's support staff."[13]

BENEFITS OF THE SAAS MODEL The traditional rationale for outsourcing of IT systems is that by applying economies of scale to the operation of applications, a service provider can offer better, cheaper, more reliable applications than companies can themselves. The use of SaaS-based applications has grown dramatically, as reported by many of the analyst firms that cover the sector. But, it's only in recent years that SaaS has truly flourished. The advent of PCs and high-speed Internet has provided an opportunity to the way we work and made this rapid acceptance possible. Some benefits of the SaaS model are as follows:

- ***Universal access.*** Most information workers have access to a computer and are familiar with conventions from mouse usage to Web interfaces. As a result, the learning curve for new Web applications is lower, requiring less hand-holding by internal IT staff.
- ***Ubiquitous computing.*** In the past, corporate mainframes were jealously guarded as strategic advantages. The applications were later viewed as strategic. Today, people know it's the business processes and the data themselves (i.e., customer records, workflows, and pricing information) that matter. Computing and application licenses are cost centers. As such, they're suitable for cost reduction and outsourcing. The adoption of SaaS could also drive applications to become a commodity.[14]
- ***Standardized applications.*** With some notable, industry-specific exceptions, most people spend most of their time using standardized applications. An expense reporting page, an applicant screening tool, a spreadsheet, or an e-mail system are all sufficiently ubiquitous and well understood that most users can switch from one system to another easily. This is evident from the number of Web-based calendar, spreadsheet, and e-mail systems that have emerged in recent years.
- ***Parameterized applications.*** In older applications, the only way to change a workflow was to modify the code. In more recent applications, however, and particularly Web-based applications, significantly new applications can be created from parameters and macros. These allow organizations to create many different kinds of business logic atop a common application platform. Many SaaS providers allow a wide range of customization within a basic set of functions.

---

[13] Traudt, E., and Konary, A. (June 2005). *2005 Software as a Service Taxonomy and Research Guide* 7. IDC.
[14] www.saasblogs.com/2006/09/26/scale-as-a-commodity-2/ SaaSBlogs: Scale as a Commodity (accessed February 2001).

- ***Global market.*** A company that made software for human resource management at boutique hotels might once have had a hard time finding enough of a market to sell its applications. A hosted application, however, can instantly reach the entire market, making specialization within a vertical both possible and preferable. This in turn means that SaaS providers can often deliver products that meet their markets' needs more closely than traditional "shrink-wrap" vendors.
- ***Reliability of Web.*** Despite sporadic outages and slowdowns, most people are willing to use the public Internet, the hypertext transfer protocol, and the TCP/IP stack to deliver business functions to end users.
- ***Transparent security and trust.*** With the broad adoption of SSL and HTTPS protocols, organizations have a way of reaching their applications without the complexity and burden of end-user configurations or VPNs.

LIMITATIONS WITH THE SAAS MODEL SaaS is conceptually similar to the original mainframe computing model that had a centralized control, minimal user privacy, and limited flexibility allowed to the individual user. Much of the explosive success of the PC after its introduction in the late 1970s and early 1980s was due to the power it gave to individual users. This empowerment will erode once users feel that with SaaS they lose their privacy and control. Another mitigating factor is the need for disconnected use. Many users (e.g., traveling salespeople) with expensive wireless connections need access to data in offline mode. Although some vendors provide offline modes that synchronize data, solutions are not optimal and not all vendors provide such functionality.

Although there is no large investment for software license at the onset of the project, the ongoing costs of SaaS are categorized as monthly expenses and do not depreciate over time as would a capital investment of perpetual software licenses. Such vendors can easily mislead customers into thinking that with SaaS there is no cost to configure the software or customize integrations because it's all delivered "out of the box." Smart ERP teams will see through this myth and realize that in order for any ERP solution to be successful, there needs to be significant investment in resources (and possibly third-party technology) to configure and support the solution, perform change management, and facilitate business process redesign so that ERP efficiencies can be realized. This cannot take place without thorough understanding of the requirements of the business, the SaaS configuration capabilities, and the difference between the two. It is quite possible that over a three-or five-year period, traditional ERP architecture might even be cheaper than a SaaS solution.

TYPES OF SAAS PROVIDERS There are two types of SaaS providers. The first has often been referred to as an application service provider (ASP) where a customer purchases and brings to a hosting company a copy of software, or the hosting company offers widely available software for use by customers (e.g., hosting Microsoft Office and making that available across the Web to customers who pay a fee per month for access to the software). The second type of SaaS provider offers what is often called software on demand (SOD), where a company offers to customers' software specifically built for one-to-many hosting. This means that one copy of the software is installed for use by many companies who access the software from the Internet.

In the first type of provider, a licensing fee and a monthly fee are separate and are paid to the maker of the software and to the software host like an ISP. With the second type of hosting there is no division between licensing and hosting fees, and there is traditionally little or no customization of software for customers. With mature SaaS providers (e.g., Salesforce.com) on-demand solutions can be highly customized.

Outsourcing Best Practices

Balancing outsourcing and in-sourcing approaches can be a complex process, but the relationship can yield very successful results when done correctly. To maintain a higher success rate with outsourcing and offshoring ERP implementations, two best practices have emerged. First, a better way to manage the offshore relationship through a practice called "in-sourcing," where good ERP managers invite a representative or entire team to work on-site.[15] This allows the project manager to supervise the work personally to ensure that agreed-upon metrics are met, as well as to facilitate the collaboration that is only possible when the entire team is colocated in the same office. The second emerging best practice is for the creation of a formal governance process to manage the offshore relationship. A report by Meta Group in Stamford, Connecticut, said, "Vendor governance is becoming a critical success factor and must include global relationships and business-process outsourcing with formal methodologies followed to refine quality and improve consistency."[16]

Companies considering outsourcing must first understand what they want to accomplish, benchmark their current costs and level of quality, and then build an infrastructure to ensure the expected value is realized. A good example of this relationship is shown in the McCormick and Patni Systems vignette.

McCormick and Patni Systems Offshoring Partnership

McCormick and Patni Systems partnered together on McCormick's global SAP implementation. McCormick, a Fortune 500 company, is a global leader in the manufacture, marketing, and distribution of spices, seasonings, and flavors to the food industry worldwide. Patni, based in Mumbai, India, is one of the leading global IT and business solutions providers with more than 12,000 clients supported from 23 offices across the Americas, Europe, Asia, and eight offshore development centers in India. In order to enhance its competitiveness, McCormick wanted to improve the time to availability for its products and enhance the overall efficiency of its business channels.[17] They searched and found a global partner that provided a cost-effective solution by scaling resources up and down as they rolled out SAP to more than six worldwide manufacturing locations. Patni provided the collaborative approach they were looking for—leveraging local engagement teams to ensure a strong customer focus. Patni's cross-functional team aligned with McCormick's business model to conduct on-site activities, such as functional/technical specifications and integration testing, while delivering offshore tasks, such as effort estimation, technical analysis, and development. The in-house ("in-sourcing") team focused on the quick resolution of project issues so that the offshore team could continue to provide quality deliverables—on time and on budget. This relationship was successful because of the flexibility of Patni's technical resources and the creativity of McCormick's management team. Jeff Malat, director of process solutions and ERP implementations at McCormick, describes the engagement as follows: "Patni has demonstrated a high degree of flexibility, scalability, and service orientation to enable us to meet the strategic goals for some of our largest IT initiatives. Their sheer commitment, execution excellence, and ability to work with us to envision our overall program had made a tremendous difference."[18]

---

[15] www.projectsatwork.com/article.cfm?ID=223467 (accessed February 2001).
[16] Ibid.
[17] www.patni.com/resource-center/collateral/manufacturing/McCormick_SAP_ERP.html# (accessed February 2001).
[18] Ibid.

ERP experts say it's never too soon to plan for installing upgrades, maintaining modules, troubleshooting problems, and policing platforms once the software enters the longest phase of its life cycle—ongoing operations. When and for whom does an outsourcing ERP operation make sense? Furthermore, once that decision has been made, what are the major contract-negotiation and management issues IT executives should consider as ERP implementation begins to wind down? In 1999, *CIO Magazine* put those questions before a number of companies that were exercising their outsourcing options on ERP operations—and one that considered that path but rejected it in favor of taking care of the work itself. Small and midsize IT organizations will be most inclined to outsource ERP operations because they lack the resources to handle them internally, but larger companies can also derive advantages. The reasons for ERP outsourcing are ultimately as varied as the participants.

ERP implementation teams should not consider outsourcing and offshoring when they want someone else to take accountability or to deflect blame in the event something unfortunate transpires. Another reason for bringing on an offshore partner is for expediency. In the event resources are not available due to competing priorities or the resources lack a general set of knowledge or maturity, send the work to a qualified partner and reap the benefits of watching and learning for the first time. This approach may, in fact, reduce risk and give the staff a chance to improve their skills for the next project.

No matter whose logo is on the paychecks, the challenge of managing the folks in the ERP trenches doesn't go away. "It takes more work on our side of this than I originally thought," says Coup. "You can't just turn (any part of SAP) over to someone and then sit back while they go and do the job. We've found that we have to have very active involvement from good technical people working with the vendor."

ETHICS

Ethics is a general term for what is often described as the *science of morality.* In philosophy, ethical behavior is that which is good or right in a certain value system. Ethics is different from law. Whereas laws are enacted by the government or developed through a process of jurisprudence and enforced by the legal system, ethics are developed through culture, value, and belief system of an individual with influence from family or society. Ethical violations cannot be curbed unless they are made part of the law. For example, some of the disclosure rules enforced by the Sarbanes–Oxley (SOX) Act were enacted into law for enforcement across all U.S. corporations; however, they were considered unethical and implemented in many companies even before SOX.

ERP implementations can have a wide variety of impacts on the ethical principles of the organization. Consider the following scenario:

> The ERP system integrates information from various departments of the organization. What if the one department finds out the expenses of another department and reports to everyone in the company? Should this sort of information sharing be allowed? Should the company have developed a policy on accessing information from the system?

Abuses like the preceding one are eventually observed, converted into authorization policy, and enforced by the security system of the company. Two forces endanger privacy in the information age: one is the growth of information technology and other is increased value of information in decision making. Misinformation has a way of "fouling up" people's lives, particularly when the party with the inaccurate information has an advantage in power and authority. There are substantial economic and ethical concerns surrounding property rights, which revolve

around the special attributes of information itself and the means by which it is transmitted. There are also very few institutions that can protect intellectual property rights globally. Thus, ethics play a crucial role in governing the use of information. ERP system facilitates easier access to vast amounts of corporate data from a single source, thereby making them vulnerable. Very little corporate governance exists on how to use or share this information. As such, the principles of ethics should influence the development and operations of ERP systems.

Ethical Principles

As shown in Figure 10-3, information technology can impact ethics in four ways, which can be summarized by means of an acronym, PAPA, which stands for privacy, accuracy, property, and accessibility.[19] Privacy is concerned with how personal information is safeguarded in the system. Accuracy requires systems to validate the correctness of the data in the system and who is responsible for this accuracy. Property governs who has ownership rights to the information. Accessibility is concerned with who has access to what information. The PAPA principles of ethics have been tested in a variety of systems in the last 20-plus years and are an important influence on the development of information systems.[20]

What does PAPA have to do with ERP? "If an ERP team leader says 'I've never faced an ethical issue,' they're not living in the real world," said Larry Ponemon, chairman and founder of the Ponemon Institute, a security and privacy research think-tank based in Tucson, Arizona.[21] ERPs have the capability to access and provide detailed information on various aspects of business and customers from the databases. PAPA can provide some guidelines for implementation and operation of ERP in organizations. The TJX example that follows highlights how a small security breach can create havoc with the privacy of millions of users in today's digital economy. Unless ERP users are knowledgeable with privacy regulations and take active measures to protect their privacy, frauds like identity theft will keep rising.

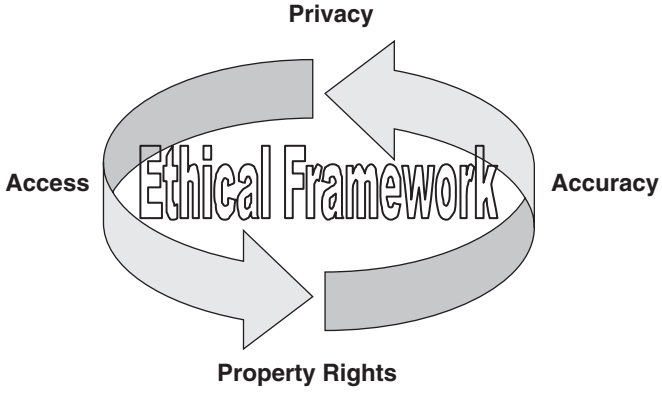

FIGURE 10-3 Ethical Framework.

[19] Mason, R. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly,* 10 (1), 5–12.
[20] Peslak, A. R. (Spring 2006). PAPA Revisited: A Current Empirical Study Of The Mason Framework. *The Journal of Computer Information Systems,* 46 (3), 117.
[21] Levinson, M. (March 1, 2005). Ask the Ethicist, *CIO Magazine.* www.cio.com/archive/030105/ethics.html (accessed January 15, 2007).

TJX Cos., parent of T.J. Maxx, Marshalls, and HomeGoods retail stores had a major security breach in 2006 when hackers entered their network and stole the data on millions of consumers from the United States, Ireland, the United Kingdom, and Canada. The hackers were able to access a wide range of financial information, including credit cards, debit cards linked to checking accounts, and transactions for returned merchandise, and make fraudulent purchases with the stolen customer data. For example, one TJX customer reported that $6,700 in unauthorized transactions—including purchases from Wal-Mart Stores Inc., Flowers.com, and iTunes.com—were made with his card account number.[22] This breach could impact more than 40 million credit card users. Although U.S. retailers are required to follow stringent card industry rules (e.g., the establishment of firewalls to protect databases and prohibited from storing unprotected cardholder information), many merchants don't comply with them. Of its 330 largest merchants, 31 percent comply with the requirements, according to Visa.

PRIVACY Privacy means providing individuals with the right to be left alone. In most societies, adult human beings have the right to control what information about themselves needs to be safeguarded and what can be made available to the public. This right, however, must be balanced with the public's right to know or societal needs (e.g., Patriot Act of 2001). Any organization that collects personal information must follow a process on how this information is collected, used, and shared. This process is influenced by laws of the land and ethics. Information systems in general provide easy mechanisms to collect, use, and share these data without any knowledge of the information owner. Temptations exist in a competitive market for organizations to use such information systems as ERP to violate individual privacy rights for marketing or accidentally releasing this information to third parties that do not have the right to it. Other problems are hacking, snooping, and virus attacks on the system, which also violate the privacy rights of individuals.

Until recently there have been very few privacy legislations around the world. Examples of privacy laws passed in the United States are the Privacy Act of 1974, which mostly applied to governmental agencies, the Children's Online Privacy Protection Act of 1998, and the e-Privacy Act of 2002. The latter two laws take into account for system-related or online violations. The European Union, ASEAN, and other countries have similarly passed regulations to protect individual privacy. The key tenets of these regulations are getting prior consent of the individuals before collecting the data, getting approval for sharing, informing individuals when their information is requested or shared with a third party, and setting regulations on collecting information on individuals from Internet browsing, junk-mail, fraud prevention, and others.

The biggest threat to privacy from ERP systems is from data mining activities. ERP systems simplify the process of collecting, sorting, filing, and sharing information on customers with external organizations. It was very complex, cumbersome, and expensive before to collect and look for consumer patterns on buying or predicting purchasing behaviors. With easy access to large amounts of data, new data mining software can reveal hidden consumer spending habits for business or identify patients with high risk for health care and insurance companies or reveal terrorists for security agencies or reveal fraudulent transactions for financial and credit card companies. Although these are beneficial to companies and society, they can be dangerous if they end up in the wrong hands. Identity theft (i.e., crooks using another individual's profile for fraudulent transactions) is now the number one crime in many parts of the world. ERP systems

[22] Pereira, P. (January 25, 2007). Wide Credit-Card Fraud Surfaces in TJX Hacking. *Wall Street Journal,* D3.

must therefore be proactive in embedding the best practices on privacy principles to increase the confidence of management and users in organizations.

ACCURACY The accuracy principle of ethics requires organizations that collect and store data on consumers to have a responsibility in ensuring the accuracy of this data. Its major concern is to protect an individual or consumer from negligent errors and to prevent intentional manipulation of data by organizations for their advantage. With the amount of data that is being collected today and integration of data from multiple sources there is a great possibility of these data being corrupted. There needs to be policy and mechanisms to prevent and correct these errors. ERP systems must embed these best practices on data accuracy and make them available to organizations. Through an ERP system companies can enforce traceability and manage data quality across the supply chain. Data tracing enables you to comply with such regulations as the EU General Food Law Regulation, the U.S. Public Health Security and Bioterrorism Preparedness and Response Act of 2002, and other import–export regulations. In addition, ERP systems can help in synchronizing data with the trading partners.

For example, most consumers who use credit cards have their profiles maintained by companies like Visa and MasterCard, but they are also reported to credit reporting agencies (CRA) that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes. They hold the databases that are the origins of a consumer's credit report. Examples of CRA in the United States are companies like Experian (which purchased the files and other assets of TRW), Equifax, and TransUnion. These organizations are for-profit entities and possess no governmental affiliation. During this reporting what if errors occur by these credit card companies or during the storage process by credit reporting agencies? This can create problems for the individuals because it affects their credit rating, and they may not be able to get loans or approval for new credit cards. The accuracy principle was developed to prevent this problem. Such laws passed by the federal government as the Fair Credit Reporting Act (FCRA)[23] have focused on this issue of accuracy by regulating the collection, dissemination, and use of consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA),[24] it forms the base of consumer data rights with credit reporting agencies in the United States. These laws require information providers to report under the following guidelines:

- They must provide complete and accurate information to the credit rating agencies.
- The duty to investigate disputed information from consumers falls on them.
- They must inform consumers about negative information that has been or is about to be placed on a consumer's credit report within 30 days.

When organizations are caught violating these guidelines, a consumer may collect $1,000 for each willful or negligent act that results in the violation of the FCRA. Any person may file suit in local court to enforce the FCRA, which entitles individuals to repair their credit report. You have a legal right to dispute any information you find on your credit report. The FCRA, which was enacted in 1971, stipulates that the credit bureaus investigate all consumer disputes if they challenge credit information on their credit reports. As per this act, the credit bureaus must complete the investigations within a 30-day period. Any information that cannot be verified or is found to be inaccurate must be deleted immediately.

[23] www.ftc.gov/opa/2004/06/factaidt.htm (accessed February 10, 2007).
[24] FTC Statutes. www.ftc.gov/os/statutes/fdcpa/fdcpact.htm (accessed February 10, 2007).

PROPERTY The property principle of ethics makes organizations realize that they are not the ultimate owners of the information collected on individuals. Consumers give organizations their information on a condition that they will be guardians of this property and will use it according to the permission granted to them. Organizations do not have a right to share information collected without getting explicit permission from the user. Sharing information in the digital economy is very easy with the advent of data warehouses, networks, and Internet. In addition to information sharing, property rights extend to issues of piracy that can involve copyrights, trademarks, and other intellectual rights issues.

Although a comprehensive look at property rights is beyond the scope of this book, ERP systems can be a *double-edged sword* when it comes to information property rights. On the bad side, ERP systems facilitate the process of sharing information easily by integrating information within the organization and across organizations. If implemented without proper controls, ERP can make it hard to safeguard information. On the good side, ERP systems can enforce corporate policy on data sharing consistently and embed best practices that can highlight the property rights issue in an organization.

With the vast ability to store data in corporate databases, and with the growth of online transactions, organizations are tested on data property rights by various stakeholders. For example, in 2006, the U.S. Department of Justice wanted to compel Internet search giant Google to share records that detail millions of Internet searches.[25] Google denied requests for the data under the Child Online Protection Act (COPA), which protects children from online pornography. Given revelations about illegal wiretaps and state spying on American citizens, Google refused to share this data because the government was planning to use the data to conduct an experiment to show that Internet porn filters were ineffective. Access to data held by Google and the other main search engines was not going to target named individuals, but a data mining operation to detect pornographic activity against children. With the passage of the Patriot Act the U.S. government has gained access to vast databases of telephone records and e-mails provided to it by airlines and telecommunications companies, and the government was not doing the same with Internet search engine companies. The user data collected by Google is among its greatest assets due to the revenue it raises from targeted advertising and other services.

ACCESSIBILITY The accessibility principle of ethics forces organization to have proper controls for authorization and authentication. ERP implementation teams must ensure that information stored in the databases about employees, customers, and other partners is accessible only to those who have the right to see and use this information. Adequate security and controls must be in place within the ERP system to prevent unauthorized access. More details on authorization controls will be covered later in the security section, but an organization needs to develop a wide policy on accessibility before implementing ERP.

In the information society, organizations need to balance the needs of the workers who need access to vast amounts of data to make good decisions with the needs of society, which is increasingly hostile when data privacy rules are violated. In addition, hacking, snooping, and other fraudulent access to data are a big concern to organizations. There has been a recent surge in identity theft crimes to $55.7 billion in the United States,[26] where hackers steal individual profile data to open bank accounts and credit cards, apply for loans and driving licenses, and conduct

[25] Hafner, K., and Richtel, M. (January 20, 2006). *San Jose Mercury News.*
[26] Identity Theft Resource Center. www.idtheftcenter.org/ (accessed February 10, 2007).

fraudulent activity using a victim's name. All of these have made it difficult for organizations to balance the needs of various stakeholders. The good news is that identity theft in the United States is declining. According to the third annual survey by Javelin Strategy & Research, a research firm in Pleasanton, California, the estimated number of victims dropped for the fourth consecutive year in 2006, by about 500,000, to 8.4 million persons. Researchers attributed the decline to better consumer education and awareness as well as to the increased use of online banking and financial sites that allow individuals to monitor their accounts more frequently.[27]

Code of Ethics for ERP

With advances in new technology becoming a routine, organizations constantly face ethical challenges in dealing with information. ERP systems have become key tools for improving operational efficiency and building strategic alliances and partnerships. In the urge to gain competitive advantage, these systems also become tools for violating the code of ethics. Due to the newness of this technology, this area lacks the norms of ethical behavior one would find in established disciplines. Nonetheless, managers implementing ERP systems in organizations must assess the implementation in light of such ethical principles as PAPA, discussed earlier. There is a distinct possibility of an ERP development team in which most members or team leaders with training in computer sciences and engineering fields may not possess the background in ethics and social norms to incorporate the code of ethics in ERP system.

There are three normative theories of ethical behavior[28] that can be used by organizations to influence the ERP implementation. They are as follows:

- ***Stockholder theory.*** Protects the interest of the investors or owners of the company at all costs. This is the ultimate implementation of the free market concept, where the responsibility of management is to maximize profits with legal and nonfraudulent methods.
- ***Stakeholder theory.*** Protects the interests of everyone having a stake in the company success, namely, owners and stockholders, employees, customers, vendors, and other partners. Management using this theory has to balance the interest of these various groups while making organizational decisions.
- ***Social contract theory.*** Includes the right of society and social well-being before the interest of the stakeholders or company owners. Management using this theory must think of the well-being of society first (e.g., protecting the environment or helping the socially challenged individuals before thinking about profits of the organization).

In context of ERP implementation, the stockholder theory would implement very few restrictions on using the information from this system to monitor employee performance or to collect and share consumer information from the system. On the other hand, the stakeholder theory would put restrictions on using the preceding information because the organization is committed to protecting employee and consumer rights. Both these theories, however, would implement the ERP only if the savings are greater than the costs, and they must improve the organization's efficiency and effectiveness. In context of the social contract theory, the ERP system would not be allowed to share or collect consumer information unless the consumers were notified of this plan and only if this activity would result in a net benefit to the society. These theories, even though not perfect, provide management with guidelines on developing the code of ethics for their ERP implementation based on their organization's culture and moral principles.

---

[27] Mincer, J. (February 7, 2007). Identity-Theft Incidents Declined 12% Last Year. *Wall Street Journal.*
[28] Hasnas, J. (1998). The Normative Theories of Business Ethics for the Perplexed. *Business Ethics Quarterly*, 8 (1),19–42.

Thus, it is practical for all organizations to develop a code of ethics for ERP systems implementation. In order to formalize the implementation of ethics consistently, the code of ethics policy of the organization must be explicitly communicated to all the stakeholders, including external partners and community. Without this, it will be very difficult to enforce the desired ethical behavior and deal with violators. This code should generally address the four principles of privacy, accuracy, property, and access in context of the organization's position on the normative theory, discussed earlier. It should provide guidelines on such issues as dealing with offensive content, copyright information, employee education on who has right of access to certain information before sharing, and how to protect consumer data (e.g., not downloading consumer data files in nonprotected areas of their computers or destroying such data after usage).

The following is an example of code of ethics for ERP implementation policy:

- Protect the interest of its customers.
- Privacy decisions are made free of owner's influence.
- We insist on fair, unbiased access of all information.
- No advertising that simulates editorial content will be published.
- Monitoring fellow employees is grounds for dismissal.
- Company makes prompt, complete corrections of errors.
- Implementation team members do not own or trade stocks of ERP vendors.
- No secondary employment in the ERP industry is permitted.
- Our commitment to fairness is our defense against consumer rights.
- All comments inserted by the employees will be clearly labeled as such.
- CIO will monitor legal and liabilities issues with the ERP system.
- Company attorneys regularly review our ERP system policy to make sure that there is nothing unethical or illegal in the implementation process.

GLOBALIZATION AND ETHICS The legal and technical costs of complying with an expanding patchwork of state, federal, and foreign privacy laws are mounting for global companies. Jay Cline,[29] an expert on privacy, has outlined seven global privacy principles that can improve the global privacy climate. These principles include (1) giving notice to consumers before collecting data, (2) collecting only relevant consumer data and retaining these data only until needed, (3) providing access for consumers to correct data for accuracy, (4) protecting data with firewalls to prevent unauthorized access, (5) giving consumers choice of sharing their data with third parties, (6) giving consumers a choice on whether marketers could contact them, and, finally, (7) ensuring every organization has an officer enforcing the compliance of privacy principles.

Globalization and offshoring have raised the level of ethical concerns. For instance, the International Association of Outsourcing Professionals (IAOP) has released a code of ethics and a set of business practice standards that are designed to help companies improve their processes for awarding and managing outsourcing contracts. The standards apply to IT deals as well as other forms of outsourcing, and they provide guidelines to the parties in an outsourcing agreement based on a common business framework. The standards are general, but they weigh heavily in favor of disclosure, candor, and the use of objective metrics that are agreed on by both sides. The benefits are that everyone is up front with the governance, so there is therefore less confusion and fewer misunderstandings in dealing with third parties.

[29]Cline, J. (January 29, 2007). *Computer World Magazine.* http://www.computerworld.com/s/article/280320/It_s_Time_to_Forge_Global_Privacy_Rules (accessed February 2001).

GREEN COMPUTING

Green computing or green IT is extremely popular with organizations. With business always growing and more and more cars and people on this planet, we are beginning to come to the harsh realization that our natural resources are not infinite. Countries around the world are trying to take the initiative and reduce the amount of wasted resources and pollution of our planet. This is especially true for businesses that are faced with increasing energy costs and an expanding need for power consumption. Governments and companies are working hard to portray themselves as being "green."

Green is not only good for the environment but also for business. Today, a green company is viewed as a responsible and caring company. Poland Spring, for example, has reduced the amount of plastic it uses in its water bottles. Automakers are making their vehicles much more fuel efficient. People, especially in America, are seeing how their waste and overuse of utilities like electricity or using plastic bags every time they go grocery shopping is affecting our environment. A company going green can also cut costs by eliminating waste and being more efficient. Anheuser-Busch has saved lots of money by trimming an eighth of an inch off of the diameter of their beer cans and saving 21 million pounds of metal every year.

These are some common examples of companies being green. Companies can go green simply by successfully implementing an enterprise resource program. ERPs are systems that facilitate all of the real-time data flow inside of an organization and manage connections to outside stakeholders. ERPs focus on efficiency within organizations to allow data to only be processed once. They have eliminated much waste by incorporating best practices into their software.

Companies are able to have some tangible and intangible results in regard to the greenness of their ERP. Primarily the tangible results are immediate and measurable. They can cut back on resources like paper by being able to do much more reporting electronically without the need for a hard copy on paper. Customers are also able to view order statuses and obtain much product information online, eliminating the need for printed product catalogs or printed receipts. This can save much on paper and ink costs.

Computer hardware has also come a long way toward being more energy efficient in today's business world. The Energy Star Program created in 1992 by the U.S. Environmental Protection Agency has helped to ensure the energy efficiency of the hardware components that go into an ERP. These include, but are not limited to, the desktop computers, laptops, and servers with one to four processor sockets. Computers marked with the Energy Star logo may only consume 15 percent of their maximum power use while inactive. This has set a benchmark for hardware manufacturers to strive for and continually improve. Consumers are also aware of this rating, allowing them to make a smarter decision in purchasing a machine that will reduce electricity costs for the home or business.

The NetApp's data center at Research Triangle Park in North Carolina was the first data center ever to receive an Energy Star for superior energy efficiency. NetApp scored 99 out of 100 and has reduced CO_2 emissions by 95,000 tons annually. This is a big step in maximizing the efficiency of a data center. By using overhead air distribution and a pressure-controlled room, NetApp's data center has really set a precedent for the industry that will become a model for data storage in the future. ERP relies on data storage 24/7. This requires running servers at all hours of the day that use up electricity. Data can be efficiently stored on servers in a room like NetApp's data center and be more effective in reducing a company's carbon footprint.

Another important hardware development has been made by General Dynamics Itronix in Cupertino, California. They have developed the Tadpole ultra thin client, which replaces and

consumes 50 percent less power than a laptop. They have labeled it a "green computing alternative." This is possible because of the following reasons. It is free of hard drives, memory, and operating system or application software. The Tadpole's core computing is done at a secure centralized server. As this will replace many laptops that have spinning hard drives and where computing uses up precious resources, this will cut costs for the company. These Tadpoles are already being used in enterprise systems by Derby College in the United Kingdom and Cascade's IT departments.

Not only is ERP's hardware green, but the software is where ERPs really have green potential. The newer ERP software allows organizations to track their carbon emissions. Virtualization allows multiple applications to run on a single server. It can significantly reduce the amount of hardware necessary for an ERP implementation. Less hardware means less energy needed to run that hardware. This is one of the leading green practices for IT. People in F5 Networks and Pace Harmon say that virtualization allows an organization to eliminate about 5–10 pieces of hardware equipment and improves the utilization of a server by up to 85 percent.

A nonvirtualized data center can have all of those servers running at about 5–15 percent of their capacity. This means about 10 servers are being used to do the job that virtualization allows 1 server to do. Undoubtedly this allows an organization to drastically reduce power consumption and its carbon footprint, not to mention the equipment needed for cooling all of those servers. Virtualization allows for maximum power management, permitting an organization to only use what it needs. If a company can regularly and effectively monitor the metrics on applications and servers, they can get the most out of new virtualization tools, including moving virtual machines to lower energy costs.

Virtual data centers can be moved to different areas depending on electricity costs. If costs are cheaper, let's say in Montana than in New England, a company could move its virtual data to Montana to decrease its costs further. This would not do much for its carbon footprint, however.

Virtualized computer resources will also allow workers to work from home. This will allow an organization to save on heating a facility. This is useful especially in climates like that of New England, where the winters are very cold and will require much heat to get through a day. An employee would be taking that heat cost from the organization to heat his or her home while he or she works in comfort, reducing the need for a facility to be heated.

Another big step for green ERP is that ERP vendors are now including carbon-monitoring applications in their software suites. These allow organizations to track the amount of carbon they are producing by powering and heating their businesses as well as using fuel to deliver goods and move equipment. These factors are becoming increasingly important to companies, especially package delivery companies like UPS and FedEx. They have been able to alter delivery routes to minimize greenhouse gas emissions by using ERP software.

The government has taken a great initiative in setting an example for green business. In addition to the Energy Star Program, the government will offer tax cuts to organizations that can reduce their carbon emissions, which is a very positive incentive. It is not always easy or cheap for a company to implement green ERP. However, over time, an organization can save a lot of money by becoming green and this will also contribute to the health of the planet. There is a common saying by hardware vendors that "green desktop and server hardware is good for the planet, and what's good for the planet is good for business." This is the view that needs to be shared by all businesses in today's global economy.

The future of ERP is definitely green. Companies benefit greatly by becoming green, whether it be by reducing heating and electricity costs and materials costs, being more efficient in their data processing, or using their greenness in their marketing. Monitoring CO_2 will become a more and more common module for ERP in the coming years. Companies will be

able to receive tax benefits by having greener practices and measureable results. This will not only benefit the organization but also the planet. Throughout the growth of business, history shows that we have done much damage by polluting the planet. Ideally ERP will help organizations to become wholly green and be able to recycle all of their energy and hardware. The green market is growing and is expected to go from $47 billion in 2009 to 223.7 billion in 2013. This will prove to be a very profitable venture for ERP vendors and organizations that use ERP.

COMPLIANCE ISSUES

The pressure in today's competitive environment requires the use of enterprise systems such as ERP to be effective and efficient in the management of the business operations. No commercial enterprise, government, or institution is an exception to this requirement. The validation of these systems to attest that they are fit for the specified purpose and meet user and compliance requirements is critical. Although no organization is subject to pressure to validate the system, other forces have pushed them toward embracing the concept. Thus, complying with specific regulations such as FDA, HIPAA, and SOX is becoming critical for the system to be valuable. It has been proven that only performing system validation or software validation does not mean that the system has been designed to meet these requirements. The validation concept and the compliance requirements of computerized systems are often misunderstood and thus need clarification. Business managers, who have the primary responsibility for ensuring that the ERP objectives in terms of compliance requirements are met, must know the principles surrounding ERP system validation and regulatory compliance. Ultimately, the validation would ensure that the system meets its requirements. According to Tim Flanigan and Robert Mackey, the fear of validation can be replaced with its embracement once it's understood that validation could be and should be beneficial to the overall ERP investment project.

SOX Compliance and EU Regulations

SARBANES–OXLEY ACT The Sarbanes–Oxley Act of 2002, sponsored by U.S. Senator Paul Sarbanes and U.S. Representative Michael Oxley, represents the biggest change to federal securities laws in a long time. It came as a result of the large corporate financial scandals involving Enron, WorldCom, Global Crossing, and Arthur Andersen. Sections 404 and 409 relate to IT controls. Section 404 illustrates rules set up on internal controls. It discusses the necessity for clear responsibility in IT systems, as well as for maintaining an adequate internal control structure and procedures for financial reporting. Section 409 illustrates real-time information concerning material changes in the operational or financial condition of a company.[30] In order to comply with these sections, companies must have adequate controls on the business processes and information systems that feed their financial reports.

In an article, Rob Smith describes seven different control considerations for information technology (see Appendix D). It is clear after reading these that SOX must be kept in mind when implementing an ERP system. You want to make sure that internal controls such as separation of duties, safeguarding of information, and the like are in place. With internal controls in an ERP system you will be able manage risks and monitor the reliability and integrity of financial reporting. Because most ERP systems contain data that feed the financial reports, compliance of SOX is definitely a topic to cover when choosing and implementing an ERP system.

[30] Smith, R. Seven Things You Need to Know About IT Controls. Sarbanes-Oxley 404/409. http://www.techrepublic.com/whitepapers/sarbanes-oxley-404409-seven-things-you-need-to-know-about-it-controls/113303 (accessed October 2004).

BOX 10-1 SAP and SOX

Systems Applications and Products (SAP) provides software for businesses in every type of industry. SAP is a major ERP provider, so when Sarbanes–Oxley sections 404 and 409 were introduced, they had to think about their market force and their own company. SAP is a worldwide company that was started in Germany. In a recent article, it was noted that as of July 15, 2006, overseas companies listed in the United States had to be SOX 404 compliant.[31] SAP is a "software giant" that has a lot of activity in the United States. Dirk Matzger, head of risk management at SAP Asia-Pacific, said in an interview that SAP has been actively researching and working on becoming SOX 404 complaint since the regulations first came about in 2002. They have involved process owners and have also chosen current employees to champion the project and are in charge of SOX 404–related tasks. They are working on their company's internal controls and incorporating them with SAP's risk management function. SAP currently has biannual audits by their auditor, KPMG, on SOX 404 compliance. They expect these audits to benchmark their progress in becoming compliant and hope to obtain first certification of compliance.

SAP is currently marketing their mySAP ERP Financials. They claim that "mySAP ERP Financials software provides extensive capabilities to ensure continuous compliance with regulatory mandates—enabling high governance standards and reducing IT and audit costs. Using mySAP ERP Financials, you can manage the complex documenting, testing, mitigation, and sign-off procedures associated with Sarbanes–Oxley sections 302, 404, and 409, as well as fast close and section 301 whistleblower requirements."[32] Their software enables companies to manage their systems and financial information while supporting the regulations of the SOX Act.

SOX IMPACT ON PRIVACY AND SECURITY Two key concerns for SOX are privacy and security violations. Audits are done to a company's ERP systems to test the privacy and security levels of the system (e.g., who has access to what information and what internal controls are involved in the ERP system?). The major areas of privacy include access to the system, user ID and verification, evaluating configurations relating to business processes, change management, and interfaces.[33] As discussed earlier, ERP systems integrate almost all business functions into one system. It uses one database, one operating system, and so on. People who have access to this system should have user IDs, passwords, and access controls. All users should not be able to change financial information, personnel information, vendor information, and the like. Most auditors get a list of users and what permission they have in the system. They also check to see what process is used for user IDs and passwords: How often are passwords changed? How complex are the user IDs? They also check on how easily changes or modifications can be made to the system. Change management is something that should be controlled by a limited number of experienced people in ERP software. Privacy and security are extremely important with ERP systems.

Along with SOX requirements related to privacy and security violations, other government entities also require companies to maintain certain standards of data integrity. The FDA requires that computerized data be as "accurate, authentic, attributable, current, and legible" as paper

[31] http://news.zdnet.com/2102-1009_22-6098931.html (accessed February 2001).
[32] www.sap.com/solutions/business-suite/erp/financials/sox.epx (accessed February 2001).
[33] www.isaca.org/Content/NavigationMenu/Students_and_Educators/IT_Audit_Basics/IT_Audit_Basics_Auditing_Security_and_Privacy_in_ERP_Applications.htm (accessed February 2001).

BOX 10-2 UC Berkeley—Privacy and Security Violations

Over the past few years, colleges and universities have been implementing ERP systems to integrate all student information into one main database. Students enroll in classes, drop classes, pay bills, receive grades, and update personal information all in one central location. This is a great idea because in the past, if a student moved, they would have to change their address at the registrar's office, financial aid office, and admissions office; it was just a very redundant and frustrating process. With the implementation of these systems, however, came violations of security. Most of the systems that are integrated are secure, but individuals with certain accesses are able to download information on their laptops or PCs, and that is when the information becomes very insecure and out of control of the CIO that oversees the centrally located systems. There was a major incident at Berkley in 2005: "As chancellor of the Berkeley campus, I was stunned to learn of the theft of a laptop computer in the graduate division, which contained personal information for approximately 98,000 current and former graduate students as well as persons who applied to our graduate programs. Our students, staff, and alumni expect us to protect the information they have given us confidentially, and we have not maintained that trust. This incident revealed serious gaps in our management of this kind of data. The campus has been instituting new policies to address these issues for several months, and we will do much more. Accountability for this effort ultimately lies with me."[34]

records (Colorado Analytical Research & Development).[35] Exhibits 1-1 and 1-2 present a more comprehensive list of requirements, but the main ones are that all data must be accurate and a record is available of when the data were entered or changed and by whom. SOX has more requirements regarding auditing data and access to the data. Digital data are now more common than data recorded on paper. Signatures on paper are being replaced with digital signatures backed by some sort of biometrics or as is more common an ID and password. But the most telling issue is that managers must now understand how their computer systems process data.

"If you can't explain how things going into the sausage machine come out the other end, then you will be in trouble," said a compliance officer with a London investment bank. For example, upcoming international capital adequacy rules, known as Basel II, will require firms to consider operational risk, such as the risk of a trade not being settled, when calculating capital levels. Without a clear view of how a firm's systems process trades, it will be very difficult to calculate operation risk, he noted. SOX, meanwhile, requires that firms audit and understand their own software. "Before it was like getting a drivers license, as long as you could drive the software you were fine," said Kusionowicz. "But now they are saying you have to show you know what IT systems are doing, so to get your driver's license you have to be able to strip down and rebuild an engine" (Compliance Reporter).

ERP systems are time-savers and money savers, but the very complexity of the system that makes them so advantageous also means that they have many potential areas of weaknesses. Security of the data is of utmost importance if a company wishes to satisfy an auditor that it is in compliance with all the regulations mentioned in SOX. In 2005, a study showed that a large company can expect to spend 70,000 man-hours and $7.8 million reporting and correcting material weaknesses in its financial controls (Dave McClure).

---

[34] www.educause.edu/apps/er/erm05/erm05613.asp?bhcp=1 (accessed February 2001).

[35] Keatley, K. L. (April–June 1999). A review of US EPA and FDA requirements for electronic records, electronic signatures, and electronic submissions. *Quality Assurance,* 7 (2), 77–89. Colorado Analytical Research & Development, an Operating Unit of Pyxant Labs, Inc., Colorado Springs 80907, USA.

However, there can be a significant point of material weakness in a company's financial controls. ERP systems have access to all data, thus incorrect data being used in a variety of a company's financial reports could render the entire financial report fraudulent under the law. Many companies have stepped up to market software that can be used to flag suspicious activity that would be in violation of the SOX. Some examples are DC2, OpenPages, Certus, MetricStream, and MKInsight. All these software packages are searching for multiple levels of access for a single user. For instance, setting up a new vendor in the company's account system, creating a purchase order against the approved vendor list, approving an invoice from that same vendor, and finally paying the invoice all four of these tasks should be handled by different people. If the same person has access to all four functions, then that person could single-handedly commit fraud (Jon Brodkin). Software packages would be examining the millions of transactions made by a company and searching for anywhere the same person was involved in all four steps.

SECURITY

Today's ERP systems are largely Web browser based, meaning they can be accessed anytime and anywhere. In addition, supply chain or e-commerce environments within the ERP are exposed to the intricacies of the Internet world. As ERP systems are implemented, they become exposed to the good and bad of the Internet. Hackers are becoming more and more sophisticated at gaining access to systems. Worms, viruses, and Trojan horses are common, and hackers are now using a variety of other methods to capture information to gain access to systems. An ERP system's security, as shown in Figure 10-4, is only as good as company employees are aware of the importance of

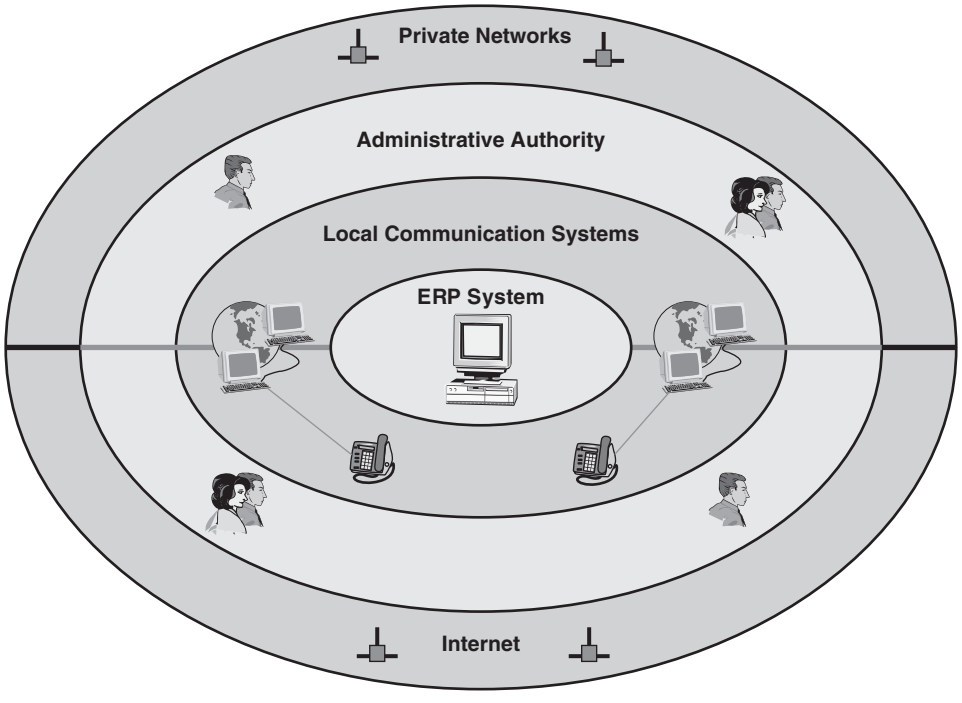

FIGURE 10-4 Security.

maintaining a secure environment. It is still the case that systems that are inappropriately accessed come from the stealing of user IDs and passwords because they are written down and posted on an employees' monitor or in an employee's desk. Securing an ERP system is complex and requires both good technical skills and communication and awareness. It is often said that a system's security is only as good as its weakest link. In the case of systems connected to the Internet, the weakest link may not even be the company's employee—it could be someone else that has been given access to the system for e-commerce purposes.

System security cannot be underestimated or overlooked in an ERP implementation. Like any system, a security plan must be developed to address all the issues related to access with an implementation methodology employed to ensure proper installation and testing. Organizations many times hire security consultants to attempt to access the ERP to see how secure the system really is, and even to continue to try to break in once the system is in production. This will include not only breaking in through electronic means but also accessing computers, stealing user IDs and passwords from employees, and even taking laptops or PDA devices that may contain sensitive information. It certainly seems to be the case, as in the nonelectronic world, that it is difficult if not impossible to keep up with the creative ways thieves or hackers can gain access to systems. ERPs are prime targets because they have so much information that can be harvested and used. A currently published statistic estimates that there are 100 million published data leaks.

Security needs to be in place, tested, and enforced from Day one. The Internet makes access from anywhere anytime possible, but it also opens up a company ERP to many more people than just the company employees.

A good security plan will consist of the software products needed to ensure proper and secure access but will also consider physical access and user security awareness.

USER ID AND PASSWORDS There is a balance to user IDs and passwords. The current trend is to provide access to systems through an ID Management system. This will afford the users a single user ID and password. This is highly desirable for the end users. It helps them to manage a single ID and will most likely stop the writing down or storing of user IDs and passwords. On the other hand, users must be made to understand the importance of a good password that is not crackable. (A number of systems now require a password with as least one number and one special character.) A policy of changing passwords periodically is also needed. The current best practice is somewhere between 30 and 60 days.

In addition, there need to be policies for how a password is reset if it is forgotten and for the suspension or deletion of user IDs if an employee leaves the company or changes roles in the organization. It is vital for HR to work with IT security to ensure that only active employees have appropriate access to the system. A yearly audit of who has access should be conducted to ensure nothing has been missed.

PHYSICAL HARDWARE SECURITY It used to be that physical access to the computer center was a big exposure or risk to the system security. Even though the security to computer centers has gotten better with the advent of networks and PCs connected to them, physical access includes network closets or switch rooms and access to PCs. All must be secure. Thefts of laptop computers with sensitive information on them have become a bigger issue for companies. One may think that the data on a laptop hard drive are secure if the PC can only be accessed through a user ID and password. This is not the case. Thieves often take out the hard drive and connect it to another PC, and the data are readily available. The encryption of hard drives, especially from laptops, is one solution that is becoming more and more available. PCs have been a weak link in

TABLE 10-1 List of Some Company Data Leaks

Institution	Type of Leak	Year	Records
UCLA	Hacked into database	2006	800,000
Aetna	Stolen backup tapes	2006	130,000
Boeing	Stolen laptop	2006	382,000
Bank of America	Lost data tapes	2005	1,200,000
Stanford University	Network breach	2005	10,000
University of Connecticut	Hacking program on server since 2003	2005	72,000
University of Southern California	Flaw in online application database	2005	270,000
Wilcox Memorial Hospital	Theft of hard drive	2005	130,000

overall system security. There are many published stories of hackers gaining access to a PC to gather information and to launch an attack on the rest of the company's systems of which the ERP is the prime target.

NETWORK SECURITY The Internet has its share of less-than-ethical individuals accessing it. In fact, there are likely many people doing a wide variety of illegal activities on the Internet. The Internet and illicit activities seem to be in the news every day. This illustrates how big the Internet has become, and that network security is in its infancy. There are devices that will address significant amounts of network security, but it is complex and requires constant updating. Most companies implement some form of firewall(s), virus controls, and network or server, or both, intrusion detection to safeguard the networked environment. Operating systems need the latest patches, and virus software needs to be updated regularly with antispyware installed to prevent further access. All need to work together to ensure the network environment remains secure and stable. Network security is one of the more complex IT jobs around today. The staff needs to address its throughput and response time, and they must try to ensure the network is free from viruses, intrusions, and, in general terms, attacks to the environment.

INTRUSION DETECTION Network and server intrusion detection comes in many forms of hardware and software. The notion is to catch and track intrusions in the best case as they are happening and worst after they have happened and been discovered.

BOX 10-3

An **intrusion detection system (IDS)** generally detects unwanted manipulations to computer systems, mainly through the Internet. The manipulations may take the form of attacks by skilled malicious hackers or script kiddies using automated tools.

An intrusion detection system is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data-driven attacks on applications, host-based attacks such as privilege escalation, unauthorized log-ins and access to sensitive files, and malware (viruses, Trojan horses, and worms).

An IDS is composed of several components: **sensors** that generate security events, a **console** to monitor events and alerts and control the sensors, and a central **engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize IDS, depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations, all three components are combined in a single device or appliance.

From Wikipedia, the free encyclopedia.

All intrusions must be taken seriously and investigated. Hackers are very sophisticated and can sometimes access systems without it being noticed. Real-time monitoring and after-the-fact reporting of anomalies and misuse of network and server activities will assist in spotting intrusions and safeguarding systems from inappropriate access to information stored in the ERP. Infrastructure implementation planning should address intrusion detection during an ERP implementation. It may be that the IT organization has this capability and is trained adequately, but validation of their capabilities is needed along with a thorough test plan.

Sample List of Intrusion Detection Systems
VCC/TripwireTM
Computer Misuse and Detection System (CMDS) by SAIC
Kane Security Analyst by Intrusion Detection, Inc
NetRanger by Cisco Systems
Symantec Intruder Alert by Symantec
Real Secure by ISS now IBM
G-Server by Gilian Technologies

PORTABLE DEVICES It may not be easy to steal desktop PCs, and thieves are finding that stealing laptops and PDAs is much easier. Society is demanding more and more portability. PDAs and even mobile phones can store large amounts of data. The theft of laptops and PDAs that have stored identity information is common. Safeguarding against stealing of portable devices is difficult. Society wants the convenience of portability, but it comes at a cost of less security. Laptops can be stolen from offices, cars, trains, airplanes, and homes. Once stolen, the storage media can be mined for information that can be used to gain access to confidential data. Use of passwords and data encryption is important in securing a portable device, but the key is for the users to be very aware of what is being stored and to ensure its safety from hackers and thieves.

AWARENESS Users often do not understand the vulnerabilities of Web-based ERP systems to unauthorized access. Even though it may be difficult to convey these vulnerabilities to end users, making them aware of the possible issues is key to a successful security plan and program. There should be two facets to awareness. First, ensure that users are aware of security risks (e.g., writing down or choosing simple passwords). Second, enforce policies and procedures related to access. Security violations must be enforced or all system security plans will be compromised. It is often said that system security is only as good as the weakest link. Those seeking to gain access illegally will find it and expose that weakness.

SECURITY MONITORING AND ASSESSMENT A good security plan will also detail how to provide for constant assessments of security. A periodic review of who has access, what they have access to, and how often they are accessing the system should be part of the review. Setting up and reviewing audit logs must be addressed with an ERP implementation. Logging transactions and reviewing them on a daily or, at worst, a weekly basis is a must for any financial transaction. Audit logs will reveal any unusual transactional activity and help to minimize revenue loss due to fraud or hacking. Intrusion detection must be in real time, and any anomalies or unusual happenings on the network or ERP servers uncovered through daily reporting should be investigated. Virus scanning and general malware must be addressed, along with an evaluation of physical security. Physical security includes those who have physical access to the servers and why. Some companies have hired consultants to provide this type of security assessment on a periodic basis. However it is accomplished, whether in-house or by outsourcing, this type of monitoring must be available to the production ERP system.

ENCRYPTION The process of taking data and making it unreadable to those who should not see the data has been around for a long time. The complexity has been to encode the data in such a way that the data is reliable to those who should be able to read it. Encryption involves using a key, usually a very long prime number that is difficult to guess or program, to scramble at one end and unscramble at the other end. One way hackers gain access to systems is through monitoring data passing through a network. If the key is unscrambled, the process with the right tools and knowledge is relatively simple. In today's Web-based Internet applications, data encryption is highly desirable. Customers and users are sending and storing confidential data (e.g., credit card numbers and social security numbers) over the network. Encrypting that sensitive information will help to prevent theft of information. In today's ERP implementations, network data encryption and even storing encrypted data need to be addressed. Even the sensitive data on laptop hard drives or PDA storage should be encrypted for security purposes. If the laptop or PDA is then stolen, accessing the hard drive to retrieve data will be next to impossible without the proper key.

Disaster Recovery and Business Continuity Planning

Mission-critical systems must have a plan in place that will provide for the recovery of a number of disasters that can occur to a business. ERP systems play a key role in company business and profits. When a system is unavailable, significant revenues are often lost. It must be said that disaster recovery and business continuity planning are not just an IT responsibility. All departments that use an ERP system must play a part in providing business continuity while a system is unavailable. In planning for a disaster a company must address the level of risk versus the amount of money to ensure that systems are available as quickly as possible. Some of these costs include alternate sites or mirrored sites to ensure ongoing business availability, software and data backups stored off-site, alternative computer centers with the network connectivity, and workstations needed to run the business and the support to ensure that the sites remain in synchronization as the software and hardware configurations are changed. In any planning process (e.g., disaster recovery), evaluating risk or loss of revenues should compare the amount of funds necessary to recover any possible risks in a timely fashion. This planning process is very complex and time consuming and is well beyond the scope of this book. The key concept is to understand that planning for a disaster is part of ongoing business and must include all departments involved in a mission-critical system.

IMPLICATIONS FOR MANAGEMENT

Outsourcing

Outsourcing is certainly not a new idea; however, the face of facility service outsourcing is changing. You now have a wide range of companies with very assorted business models. There are companies that self-perform services, who subcontract services, and who contract manage services. Your next avenue of support lies somewhere in the middle of the crowd of service companies. When companies outsource, it raises ethical questions, especially in this post-Enron era. Casseres[36] said, "My favorite post-Enron cartoon, by Dan Wasserman, has two captains of industry discussing what to do about the fallout from corporate scandals. 'We are seen as ethical disasters,' says one of them. 'How are we going to rebuild public trust?' In a flash of brilliance, the other answers: 'We could outsource it!' " He further continues his article saying that when companies begin to outsource, you can't help but ask if they are shedding ethical responsibility for their company. The key to realizing the benefits of outsourcing or offshoring ERP implementation activities is to know when to use these services properly.

The first consideration is to determine the amount that companies should rely on outsourcing and the extent to which they do.[37] Even though IT budgets have been flat through much of this decade, government regulations (e.g., SOX) have required companies to innovate to remain competitive. Offshoring and outsourcing services include data center operations, help desk and application maintenance, and specialized project work (e.g., global ERP implementations). IT and business management need to determine where offshoring fits with their business goals and how much makes sense for the organization, both fiscally and culturally.

The second consideration is to reevaluate the level of support required for the ERP implementation. Companies need to decide if and when to replace traditional business and implementation services with comparable services from one of the major Indian offshore services providers mentioned earlier. ERP projects are one of the largest budget items of most IT organizations, enforcing the need for more affordable services in this area. ERP support is quickly becoming a buyer's market, and savvy IT organizations are exploiting this fact to their advantage, proving to be a more cost-effective option and improving the company's bottom line.

The third consideration is to evaluate business process outsourcing (BPO) and hosted applications for key business processes. BPO is the contracting of a specific business task (e.g., payroll) to a third-party service provider. Software as a Service (SaaS) is renting externally hosted enterprise applications on a fixed monthly, per seat cost from application service providers like Salesforce.com or NetSuite. The BPO and SaaS providers have matured to the point that they warrant consideration for key ERP-related business functions. IT and business leaders can be assured quality solutions through BPO providers or subscription-based hosted providers, and they can be cost-effective alternatives to traditional software purchase and installation. In fact, according to Dana Stiffler, a research director for AMR Research, "BPO can offer operational savings of up to 50 percent over purchased applications."[38]

Last, when considering outsourcing solutions (whether they be offshore development or SaaS providers), ERP management teams need to look beyond cost. Given the emotional

---

[36] Gomes-Casseres, B. (October 1, 2005). Outsource, Don't Abdicate. *CIO Magazine.* www.cio.com/archive/100105/keynote.html?page=1 (accessed January 15, 2007).
[37] www.amrresearch.com/Content/View.asp?pmillid=17890 (accessed February 2001).
[38] Ibid.

nature of the decision, managers need to focus on resource availability, staff experience, and motivation. In fact, there are six key assessment factors to consider when making the in-house versus outsource or offshoring decision: (1) ERP team's skills and experience; (2) resource availability; (3) project priority; (4) availability of funding; (5) severity of problem; and (6) development motivation.[39] Implementation teams should consider keeping the project internally if there is a high need for control (e.g., keeping company activities secret for competitive advantage). Furthermore, if the organization can afford the time and cost to educate the internal staff, then they may be better off in the long run to perform the implementation internally. The decision might be about national pride and ego (i.e., teams may not want to see these jobs go overseas).

ETHICS Ethics should be a major concern of the ERP implementation team. An ethics guru should be appointed to the team to guide the team on privacy, accuracy, property rights, and access principles. The best ethical practices should be embedded into the ERP system with other business processes. The integration of ethics both in the system and in the change management strategy and training program would help create higher ethical standards with systems in the organization and improve the compliance with such government regulations as SOX and HIPPA. Another major concern for management should be with data mining activities with ERP systems. Setting high ethical standards during and after ERP implementation will prevent data mining from identifying individual consumer identities.

LEGAL Management cannot assume all will go well with ERP implementations. Software products sometimes do not perform as advertised, software companies go bankrupt or are bought out by other companies, and consultants overextend themselves or do not have the skills necessary to be successful. It is important for management to address as many possible legal issues up front to protect the company's investing in the ERP and the successful implementation. Contracts must be scrutinized by both the legal department and the project director, project manager (PMO), or both.

AUDIT The key issue for management with ERPs in general is the law around Sarbanes–Oxley. It has had a big impact on systems as it is related to the integrity and completeness of controls and processes that are oftentimes coded into the ERP. As the SOX law continues to be clarified in the courts and therefore in compliance, it will continue to have impacts on existing and new systems. Changes are often required to ensure that compliance is reached.

SECURITY Securing an ERP system is complex and requires good technical skills as well as communication and awareness. As mentioned before, it is often said that a systems security is only as good as its weakest link. In the case of systems connected to the Internet, the weakest link may not even be the company's employee, but rather someone else that has been given access to the system for e-commerce purposes. System security cannot be underestimated or overlooked in an ERP implementation. Like any system a security plan must be developed to address all the issues related to access with an implementation methodology employed to ensure proper installation and testing.

[39] www.projectsatwork.com/article.cfm?ID=224597 (accessed February 2001).