

The Metropolitan Corporate Counsel

www.metrocorp-counsel.com

Volume 16, No. 9

© 2008 The Metropolitan Corporate Counsel, Inc.

September 2008

A Simplified Approach To Dealing With The Legal Aspects Of Business Information System Integration

Scott David

K&LGATES LLP

The technology revolution has released waves of information. Huge volumes of data and information wash over businesses every day. Organizations that implement appropriate technology tools and legal rules for integrating their information system with business needs have a competitive edge over those that merely react without seeking to integrate.

This article will suggest a strategy for applying legal resources to help assemble an integrated information system that will allow company management to better “guide” change rather than merely accommodating it.

Summary

1. Business information system controls are both technological and legal, because legal rules affect the system and the behavior of individuals who interact with it.

2. Companies should seek an “integrated” system of legal arrangements associated with their information needs, just as they seek to integrate their technology resources.

3. Information system integration with company strategic goals begins by asking three questions about the legal aspects of the company information system: (i) Where are we? (ii) Where do we want to be? and (iii) How do we get there?

4. “Where are we?” can be answered with a system audit that identifies current information practices and informs decisions about needed legal controls.

5. “Where do we want to be?” requires attention to the company’s strategic goals.

6. “How do we get there?” is answered by identifying and evaluating potential legal

controls, grouped with reference to the degree they can be implemented unilaterally, i.e., internal employee policies (most discretion), contracts with suppliers and customers (intermediate discretion), and government and industry rules (no discretion).

Discussion:

I. Information Systems Are More Than Just Computers

Business information systems are not just technology. The most valuable part of a company’s information system is not the hardware, software or network. Instead, value is created by the information, data, IP and other content that flow through the system.

II. Integrated Systems Require Integrated Thinking

A. System integration relies on technological “tools” and legal “rules.”

Integrated technology infrastructures perform best. When infrastructure doesn’t interoperate, information cannot flow, efficiency slackens and communication and innovation suffer.

Information flow is also controlled by the legal “rules,” i.e., the “system” of legal arrangements relating to information. The rules include information-related provisions in: (i) internal company policies, (ii) external contracts with suppliers and customers, and (iii) governmental regulations. Better integration of both the technological “tools” and legal “rules” enables better information flow control in an organization.

B. Who is in charge of a company information system?

Most companies would identify the IT department as being in charge of their business information system, but it is not IT’s job to establish the legal rules that structure a business information system. Information is managed by the web of agreements that together define the business. This web is created and maintained through the contract and legal function. Techies configure the infrastructure, but attorneys “configure” the system of “rules” to provide the company with

information.

C. Why is an integrated approach necessary?

An integrated approach can enhance business performance, enable innovation and reduce risk. System inefficiencies, data handling errors and compromised access controls can be increasingly visible through intimate data sharing business models with customers and suppliers (e.g., joint services, extranets), and state-mandated data breach notices. These, along with increased governmental regulation (data safeguarding rules and use limitations), increase the importance (and expense) of integrated legal “rules.”

An integrated approach does not necessarily require dramatic changes. However, it is at least a matter of shifting perspective on elements of normal legal analysis and applying strategic thinking when dealing with technology and information issues. Being aware of the benefits of integration will inevitably lead to its incorporation into the legal decisions that affect business information flow.

III. Aligning Information System Integration with Company Strategic Goals

Three questions should be asked when embarking on an information system integration initiative: (i) Where are we? (ii) Where do we want to be? and (iii) How do we get there?

IV. Where Are We? – The Information System Audit

The information audit examines current information flows into, within, and out of the company. The audit should consider:

A. What information do we currently collect?

What are current information collection practices? Surveys and online tools can gather this information. The initial focus should be on information that is most critical or risky.

B. What information do we currently need?

Consider all the required information inputs for a business. Each functional unit should identify its critical information,

Scott David is a Partner in the electronic commerce, tax and intellectual property practices of K&L Gates LLP in New York City.

Please email the author at scott.david@klgates.com with questions about this article.

graded based on both benefit and risk. Compare information collection practices with needs, eliminating excesses.

C. What are the sources of needed information?

Identify the sources of each element of required information. For each source, ask whether there are legal arrangements relevant to the information.

D. How is information currently used and transferred?

Identify how information flows through the organization. Ask how the data is collected, held, used, transferred and discarded.

E. Do legal arrangements support the practices in (A) through (D)?

V. Where Do We Want to Be?

Each company has a unique position and strategy, but some generalizations can be made about incorporating company strategic goals into information system configuration. Audit results should be examined to identify how information needs relate to the performance and success of different business functions. Risk limitation is correlated with predictable systems. Information system predictability will be enhanced by establishing clearly delineated information rules.

VI. How Do We Get There?

The final step is to identify the paths in achieving the above goals. Since contracts, business lines, information needs and legal requirements are constantly changing, the integration exercise must be ongoing.

Ultimately the purpose of legal rules is to affect human behavior, and the main focus should be on how to most effectively coordinate and influence the behavior of the people who interact with your system. Thus, the rules should be established (in the case of internal policies and external contracts) or identified (regulations) and then publicized and enforced as desired or required.

The mechanisms for causing rules to affect behavior vary based on many factors. Rules can be enforced by technology (password and encryption policies) and efforts to influence behavior through a mix of approaches such as training, enforcement and economic compulsion to the extent allowed by law.

One way of approaching the task is to group the rules based on the level of control exerted by the company. There are two groups of interactions to consider: internal and external. Internal interactions are those among employees, where a company can theoretically at least, exert unilateral control and can expect the greatest conformity with the "rules."

The "external" group includes (i) supplier and customer contracts and (ii) regulatory authorities. In the case of contracts, the company has influence and (depending on leverage) can have some effect on how integrated and consistent those arrangements are with its needs. In the case of regulatory authori-

ties, the company can do little (other than lobbying) to influence these external guidelines for system configuration.

The reason for establishing these groupings is to identify the most effective legal tools and strategies for dealing with each group.

A. Internal policies

In addition to technological controls, companies can influence employee information system behaviors through (i) training, (ii) sometimes appropriate policies and standards, and (iii) economic compulsion. Of course, a determined employee can ignore or abuse any policy, but we are talking conceptually here.

Full discussion of the factors to consider in dealing with internal rules is not possible here, but a sampling is illustrative:

1. Recognize that employees are important information system components

Employees perform critical information storage functions (i.e., think of how important human memory is to every company). Employees also continuously exercise judgment about the use of company information, unlike system infrastructure where decisions are programmed. System integration is enhanced if employee judgment is informed in a way that is consistent with the information system goals of the organization.

2. Implement training and establish "simple" rules

Mandatory information system training programs increase uniform application of internal rules. Even the best training will not, however, prepare employees to deal with every situation. Implementation of basic rules will foster a consistent approach across the organization at a basic level. Reality is different: the number, variance, and complexity of laws regarding some types of information (e.g. privacy laws) can preclude "simple" rules and complex roles might be ignored. Within that reality, some steps can be taken.

3. Manage change, don't fight it

Technology is changing all information systems, both business and personal. Some applications find use in both areas, and business use is often driven by initial personal adoption. Employees use information technologies (such as IM and blogging) in their personal lives, and will try to use them at work if it makes their jobs easier. Companies should understand how people are actually working in the organization and guide or attempt to preclude that work as needed. Engagement with technologies in the form of appropriate rules is generally preferred to an outright ban on popular technologies but in many circumstances legal rules may require that attempt, even if futile in fact.

4. Identify the new and unique information issues arising from digital technologies

Digital information technologies enable ubiquitous interaction recording, information

persistence and infinite duplication. Each of these characteristics requires a rethinking of how information is managed. Ubiquitous interaction recording raises privacy concerns, information persistence requires increased attention to document retention policies, and infinite duplication creates legal risks (e.g., infringement) and makes it difficult to identify the location of data. Notwithstanding these dramatic changes, many businesses operations have not changed. Change is necessary to turn these features of digital information from sources of risk into tools for managing information.

5. Embrace new technologies and challenges

Other new technologies are changing the way people work and are challenging businesses to re-examine internal policies. Examples include: instant messaging, use of camera phones, mp-3, flash memory, blogging, wikis, social networking and virtual reality interfaces. Internal company rules may need to deal with these technologies as employee adoption spreads (or should be prevented from spreading, as appropriate). Companies that establish informed and thoughtful policies will enable the use of effective technologies and will enjoy a competitive advantage assuming legal coordination.

B. External contracts

Outside of the company walls, contracts document relationships. A variety of contracts affect information flows. This is an intermediate control situation, because in the contract setting, negotiation and market forces limit unilateral action. Contracts mediate a company's information interactions with third parties.

A number of contract "tools" can be used to help configure information flows, including: (i) IP provisions (look for scope of use and license, ability to sublicense and create derivative works); (ii) data provisions (who owns data and how can it be used, who is responsible for security); (iii) confidentiality (are limits consistent with anticipated uses?); (iv) treatment of information on termination, and (v) warranties, indemnities, liability and limitations relating to information.

C. Laws

While the law struggles to keep pace with technology and information trends, the lag has not prevented the passage of many laws relating to information. A summary of laws will not be attempted here. Suffice it to say that the relevant laws and industry standards form an external set of rules that must be complied with by the affected companies. These external rules will affect how the "rules" of a business information system are configured.

Taking an integrated approach to information system rules can reduce risk, enhance company performance and enable innovation, yielding not only benefits to a company but also to its employees.