CLEARING THE HURDLES OF INTERNATIONAL TECHNOLOGY IMPLEMENTATIONS

Making an action plan that addresses the infrastructure limitations and the regulatory, legal, social, and cultural boundaries and norms of the countries where an enterprise wishes to expand is critical to successfully implementing information technologies globally.

John T. Phillips, CRM, CDIA, FAI

Implementing technology-based information management (IM) systems can be a nightmare. Yet, candid vendors of IM systems will be very clear that how the technology is implemented is at least as important to its success as the product's capabilities; complete access to all of the product's features is required for the organization to fully realize its benefits.

Technical issues are to be expected; implementing a new technology may require operating systems upgrades, software integrations, accurate data migrations, and more modern hardware or networking infrastructures.

Well-known human factors to be attended to include training for the application interface, planning for the system rollout, and gaining buy-in for organizational adoption of the technology.

All of these issues must be thoroughly addressed to get maximum return on investment from any system implementation. And, extending an implementation to international business environments will compound these challenges.

... implementing a new technology may require operating systems upgrades, software integrations, accurate data migrations, and more modern hardware or networking infrastructures.

Technology Infrastructure Issues

Implementing "global technology" – any information processing and storage technology that can reach across geopolitical boundaries – throughout an international enterprise can make both the goals and the impediments to achieving those goals vastly more complex.

Determining Network Readiness

International network readiness is critical to information technology implementation and varies drastically among regions and jurisdictions.

In many geographic locations, there is an absence of networking infrastructure, supportive technology vendors, or trained personnel. Organizations must determine whether it is best to send trained individuals to sites where servers and applications will be located or to train local individuals in IT systems maintenance.

The correct decision may depend on whether there are trained and educated individuals in that location already who can receive additional training to become system administrators. How these questions are answered can have a major impact on system performance.

Unfortunately, the implementation of these technologies is very inconsistent around the globe. For instance, India is a good example of a country where records are valued, but it is swamped in managing paper records, due in part to a lack of technology infrastructure to support electronic records management.

As another example, the authors of *The Global Information Technology Report 2013 – Growth and Jobs in a Hyperconnected World* write that "Asia is home to some of the world's wealthiest, most successful economies in the world and also to some of its poorest. Unsurprisingly, a similarly profound diversity characterizes Asia's digital landscape, thus making it impossible to draw a uniform picture of the region. The most digitized and innovative nations – the Asian Tigers – on the planet are next to some of the least-connected ones. Nowhere else does the regional digital divide run as deeply as it does in Asia."

Locating Servers/Data

If an international enterprise wants to share data among employees in U.S., European, and Asia/Pacific countries, it may be a challenge to decide where it locates the servers, software, and data.

Most businesses are not comfortable with public discussion of these issues in great detail. However, in "off the record" talks, some admit they often segment data in database applications so that specific data will be stored in a distributed manner across different servers to allow compliance with the laws and regulations governing the origin of that data.

The unfortunate consequence of that approach is that some data may not be seen in the results of queries initiated from locations that do not share a mutually agreed-upon understanding of the compliance regulations of the country where the data is stored.

More common is that many enterprises separate both data and applications so there are fewer technical complexities. It is easier to generate reports that are country-specific based on the origin of the data in the reports and then subject the reports themselves to compliance scrutiny. Thus, U.S., European Union (EU), China, India, and Middle Eastern business locations may have different servers, applications, and databases.

In addition, operating systems and applications often are implemented in different languages. The very definition of a record, a document, and data can vary among cultures, as can the concepts of responsible recordkeeping. It can be easier to avoid too many interpretations of language and culture across political and regional influences by having data stored in a particular country according to its customs, linguistic nuances, and laws.

Using the Cloud

There is much discussion today about processing and storing information in "the cloud." For instance, using Gmail, Google Docs, or similar services typically means configuring an application and data storage space on a remote disk drive accessible over an Internet connection that appears as an extension of a local computer.

According to the Google website's "Google Apps for Business," "Google Apps is a cloud-based productivity suite that helps you and your team to connect and get work done from anywhere on any device." Note that it says "anywhere." Although users are expected to conform to local security policies and electronic records retention rules for their work environments, it may be difficult to implement those policies and practice those procedures in cloud environments where the organization has little control over data storage and access.

Dealing with Big Data

IT systems' architectural dilemmas with storage communications or the location of servers can wreak havoc with new software technologies that support concepts like "big data." The very essence of big data technology is to cross-search databases and derive meaning from data accumulations from many sources by using advanced search algorithms to analyze information.

In fact, big data is often used to detect trends in customers or markets and, therefore, it can be particularly focused on personally identifiable data, thus running afoul of conflicting information governance statutes.

Clear understanding of the data and the metadata used to describe big data database content is critical, as is knowing precisely where each data element is stored. Unfortunately, Internet domain extensions, such as .us, .ca, or .eu, cannot be relied upon because computers do not always recognize regional boundaries even when these domain extensions are present, and the unscrupulous can devise ways to circumvent these limitations.

Protecting Intellectual Property

The growing challenge of software piracy is a good example of the starkly different perspectives among countries about technology use. Most individuals in western, economically well-developed countries understand and generally respect the system use requirements specified in software manufacturers' end user license agreements (EULAs), which users must accept for the software to be activated. Because these are contractually binding agreements, individuals in western nations generally pay attention to these "boundaries." They know they can be held financially and legally responsible for compliance.

Unfortunately, that is not the case in many other countries, where there are growing problems with software piracy and copyright violations despite occasional well-publicized prosecutions. Software piracy is an international concern, especially regarding western-created software in use in China.

Kenneth Rapoza, in his July 22, 1012, *Forbes* article "In China, Why Piracy Is Here to Stay," wrote,"Piracy goes back to the China world view that individual rights don't matter. The courts have never evolved to protect innovative individuals."

Microsoft CEO Steve Ballmer was quoted in a January 21, 2011, *Network World* article as saying that "90% of Microsoft software users in China didn't pay for it."

So, if an organization decides to expand its scope of business where there are cultural and legal system barriers to basic trust and accountability, it should not expect its own intellectual and corporate properties to be respected.

Similarly, where there is not a uniform set of legal and regulatory expectations for hardware, software, and networking systems operations and ownership, the organization may have difficulty protecting the data in its own servers and systems.

If an organization is planning to expend capital and resources where the technology assets may be at risk, it may be unable to convince investors, customers, and decision-making executives that an implementation will be successful.

… it may be difficult to implement … policies and … procedures in cloud environments where the organization has little control over data storage and access

Information Use Issues

It's one thing to worry about the consequences of investing in hardware and software infrastructure to be used internationally by employees, but it's another matter entirely to be concerned about how those employees create and share content within those systems.

Because countries have varying perspectives about information and records, they will have varying attitudes toward personal and business information that is stored in computers and transmitted across networks. In addition, what is permissible in some countries and cultures may be unsupported or a violation of others' laws.

Transmitting Info Across Borders

Of particular interest is the matter of storing and transmitting data within communications systems and large databases, especially with respect to transmitting information across international political borders. Because attitudes and regulations on the use and privacy of personally identifiable information vary dramatically among countries, some organizations maintain separate servers and networks in an attempt to identify and manage information appropriately within specific geopolitical boundaries.

In addition, communications media, such as e-mail, text messages, and social media, enable cross-border data flows and data storage at the initiation of computer users who often have little knowledge of the end use or storage location of the information they are creating and transmitting.

When people create e-mails or text messages, they usually think about their content with respect to their own information management, governance, or security policies. Rarely do they consider the receivers' information management policies or their countries' laws or regulations – or that these messages could be re-transmitted and used internationally far beyond their original intent.

Complying with End-User Agreements

Although software EULAs do not typically contain clauses that limit the content type and nature of the information that is created or stored, acceptable use policies (AUPs) for remote computing platforms, such as those offered by Google, Facebook, and other social media vendors, often impose limits.

These AUPs do not typically garner a high level of attention and compliance by end users, who often feel they can create and share "their" information any way they want. These free and freewheeling information-creation and -sharing environments often seem to encourage personal expression and communication with few restrictions, in stark contrast to the limitations described by the AUPs.

For instance, the first three of eight restrictions in Google Cloud Platform's AUP are:

"Customer agrees not to, and not to allow third parties (including End Users) to use the Services:

- to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act);
- to engage in, promote or encourage illegal activity;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose (for example, this may include phishing, creating a pyramid scheme or mirroring a website);…"

Users in various countries will have different interpretations about what "illegal activity," and "violate, or encourage the violation of, the legal rights of others" mean. It may not be clear to them whether these terms are defined according to U.S. law (where Google's corporate headquarters is located) or according to the laws of the country where the employees and customers reside or use these technologies.

These matters make it clear that it's crucial to retain expert counsel who speak the language, understand the business environments and cultural norms, and can assist directly in disputes within the legal and regulatory frameworks of the countries that would be a part of the expanded enterprise.

Rolling out information technologies requires a consensus from the parties involved that these risks will be addressed during implementation so misunderstandings about the appropriate use of technology are few. Having individuals to represent an organization overseas who have "boots on the ground" can be invaluable.

Making a Global Technologies Action Plan

When enterprises are moving business processes overseas or planning to take advantage of foreign operation sites and employees, a specific plan to address international IM technology implementation issues will be critical to the success of those initiatives. Technologies, IM policies, applicable laws, regulations, and cultural norms must be evaluated by a cross-enterprise team of information users, compliance experts, and IT professionals. Consider taking these actions:

1. Identify and technically characterize the extent and specific infrastructure of each technology to be used, such as e-mail and social media.
2. Identify the locations where data may be stored or shared among users and characterize the content.
3. Identify the applicable laws, regulations, IM standards, and cultural norms that may have an impact on records management or technology use in the countries of interest.
4. Identify records management consultants and service vendors with experience and existing services in the countries of interest.
5. Identify law firms with international legal system expertise that are familiar with relevant laws, regulatory guidelines, and cultural expectations.
6. Create a matrix of these factors.
7. Form a technology implementation team wherein individuals take responsibility for creating portions of a global technology implementation compliance plan that will address all issues.

Protecting Information Privacy

Posing particular dangers during international implementation of technologies are the varying cultural and geopolitical infrastructures that bear on information creation, storage, and use.

A good example is the extreme difference between European and U.S. laws on the privacy and control of personal data. U.S. citizens have little control and voice in enterprises' use and reuse of their personal data for business purposes, whereas there are strict rules in Europe on the use of personal information for commercial purposes.

The EU is subject to Data Protection Directive 95/46/EC that protects individuals with respect to the collection, processing, and storage of data. It strives to achieve a comprehensive balance between protecting personal data and allowing the free flow of information within the EU. Europeans are often concerned with how data created in the EU could eventually be transmitted to the United States and misused according to EU regulations.

That is because U.S. laws tend to regulate the use of personal information only in specific circumstances. For instance, the Privacy Act of 1974 protects information gathered on individuals working within the federal government framework, but it does not apply to the private sector. The Health Insurance Portability and Accountability Act (HIPAA) governs restrictions on health information, but it is focused primarily on medical records. And, the Gramm-Leach-Bliley Act governs how financial institutions create policies to share data about customers between those businesses.

Obviously, it can be difficult to determine how to integrate and navigate all of these overlapping or conflicting legal and regulatory mandates. So a U.S.-EU Safe Harbor Directive was developed by the U.S. Department of Commerce and the European Commission to bridge "differences and provide a streamlined and cost effective means for U.S. organizations to satisfy the (EU) Directive's 'adequacy' requirement."

If an organization is going to do business in Europe, either by creating data there or creating it in the United States and exchanging it across national boundaries, it must be able to comply with the requirements of the business environment.

Planning for Success

All of these factors have a direct impact on the manner, means, and feasible extent of implementing technologies across international enterprises. Organizations must address the types of risks described above to negotiate the implementation hurdles that can arise. Planning thoroughly to address the expanded enterprise challenges of international projects is critical to achieving success in implementing information technologies globally. **END**

John T. Phillips, CRM, CDIA, FAI, can be contacted at john@infotechdecisions.com. *See his bio on page 47.*