



Improving Performance Effectiveness through Leadership and Management Education (Part 1)

By Dr. William S. Boddie

This article contains extracts from Dr. Boddie's recently approved Doctor of Management in Organizational Leadership Program research dissertation. This article is in two parts -- in part one, the research problem and method used to collect the research data are discussed. In part two, which will appear in the next issue, the themes and recommendations that emerged from the study will be discussed.

Abstract

It is estimated that only 30% of global IT project investments initiated in 2004 realized the expected outcomes. The purpose of this qualitative phenomenological case study was to explore the experiences and perceptions of a purposive sample of Business Information Technology Management (BITM) Certificate Program graduates regarding how the program prepared the graduates with leadership and IT management competencies. The BITM Certificate Program prepares participants with leadership and IT management competencies. The data from the in-

terviews suggested the program enabled the graduates to help improve their organization's performance effectiveness and revealed that 70% of the study participants obtained new IT leadership and management positions.

Introduction

Global leaders often depend on information technology (IT) to realize organizational performance effectiveness and efficiency. IT is defined as "computer systems hardware, software, support services, and telecommunications services" (Yamada et al., 2004, p. 3). C. K. L. Lee (2003) found that "IT is making a significant impact on almost every aspect of today's organizations" (p. 1). Many global leaders invested heavily in IT to achieve the desired performance effectiveness and efficiency outcomes for their organizations.

"Global organizational leaders collectively invested \$2.1 trillion in IT in 2002, \$2.3 trillion in 2003, and \$2.5 trillion in 2004" (Yamada et al., 2004, p. 5). Yamada et al. (2004) projected

that global organizations would invest \$2.6 trillion in IT 2005 and would invest over \$3 trillion annually by 2008. Despite making significant IT investments, many leaders failed to realize the organizational performance effectiveness and efficiency outcomes expected from their IT investments. Stang (2004) found that only 30% of global IT project investments initiated in 2004 realized the expected outcomes. Stang also found that of the global IT project teams that had a budget of "less than \$500K . . . fewer than a third were successful [in meeting the organization's expected outcome]" (p. 2). Caruso and Gentry (2005c) concluded that competent IT leaders and managers can help produce the outcomes expected from their organizations' IT investments.

The most salient IT leadership competencies are creating a shared vision, communicating the vision, and empowering others to take action to realize the vision (Caruso & Gentry, 2005c). Remenyi and Brown (2002) declared that the most salient IT management competencies were

(Continued on page 2)

Contents

IT Security Trends	4
SOA...Demystified!	6
Enterprise Instant Messaging	11



Information Resources
Management College

The IRM College is a global learning community for government's most promising information leaders.

National Defense University



Improving Performance Effectiveness

(Continued from page 1)

planning, organizing, coordinating, directing, and controlling. Mingay, Mahoney, McDonald, and Bell (2004) found that “Managers sustain established organizations and processes” (p. 3), and that managers use “execution, organization, planning, control, performance and ensuring continual improvement” (p. 2) to achieve organizational performance goals. Caruso and Gentry (2005c) emphasized that IT practitioners should receive IT leadership and management education prior to being assigned to leadership positions. Although competent IT leaders and managers can help achieve the outcomes expected from their organizations’ IT investments, little research was found that explored the effectiveness of IT leadership and management certificate continuing education programs (CEPs).

The purpose of this phenomenological case study, using a modified van Kaam method by Moustakas (1994), with audio taped and transcribed unstructured interviews, was to explore the lived perceptions of a purposive sample of 20 Business Information Technology Management (BITM) Certificate Program graduates living in the metropolitan Washington, DC, area. The BITM Certificate Program is designed to prepare participants with IT leadership and management competencies. The researcher sought to explore how the participants used the IT leadership and management competencies gained, if any, from their BITM Certificate Program experiences, to help produce the outcomes expected from their organizations’ IT investments. The study involved only BITM Certificate Program graduates who served in an IT leadership or management position and who have served in an IT leadership or management position for at least 1 year.

The BITM Certificate Program is a continuing education curriculum that seeks to prepare IT professionals with leadership and management competencies (Northern Virginia Community College (NVCC), 2005). Program course foci include IT leadership, systems analysis management, IT lifecycle management, enterprise architecture leadership, business process re-engineering leadership, project leadership, and IT security. Each of the seven program courses is a separate, stand-alone module within the BITM Certificate Program. The BITM Certificate Program is designed specifically for intermediate-level business professionals involved with leading and managing IT environments. The BITM Certificate Program was established in 2000 and was delivered at

selected community colleges in the metropolitan Washington, DC, area from 2000 to 2005. The program name and focus was changed to the Business Information Technology Leadership (BITL) Certificate Program in 2005. The revised program curriculum focuses extensively on IT leadership competencies, in addition to IT management competencies, to help organizations realize the outcomes expected from their IT investments. No studies were located that explored the IT leadership and management competencies participants gained from the BITM or the BITL Certificate Programs. The BITL Certificate Program is currently delivered at selected community colleges in the metropolitan Washington, DC, area.

Background of the Problem

Global organizations started using IT in the early 1960s (Field & Stoddard, 2004). Organizational leaders in the 21st century depend heavily on IT to support critical business functions in industries such as public infrastructure and utilities, financial management, and medical and health services. Dependence on IT leaders and managers to help organizations gain a competitive edge increased dramatically in the past 25 years (Koong, Liu, & Liu, 2002). Although introducing IT capabilities enabled many global organizations to gain a competitive edge in the past 25 years, effective IT leadership and management continues to challenge many global organizations. Field and Stoddard (2004) concluded that since the advent of modern IT in the early 1960s, few organizations effectively managed their IT resources.

Although IT is critical to many organizations, many global organizations struggle to realize the outcomes expected from their IT investments. According to the most recent Chaos report from industry analyst Standish Group, only one-third of all IT projects can be deemed successes. The report also shows time overruns in projects have increased significantly—from a low of 63 percent in 2000 to 82 percent in 2003. According to industry research firm Gartner, poor [IT] project manager competency accounts for the bulk—60 percent—of project failures. (p. 381)

(Continued on page 3)

(Continued from page 2)

It appeared that IT leaders and managers might benefit from IT leadership and management education. These leaders and managers could then use competencies gained in IT leadership and management education programs to help realize the outcome expected from their organizations' IT investments. Remenyi and Brown (2002) concluded that IT challenges are usually due to human factors rather than due to technological factors. Several recent challenged IT initiatives demonstrated the need for IT leaders and managers to gain and use IT leadership and management competencies.

One example of a challenged IT initiative was the United States Thrift Savings Plan (TSP) IT system conversion. The conversion of TSP was delayed by three years. The conversion delays and subsequent project cost overruns cost TSP participants and beneficiaries over \$36 million (U.S. Senate, 2004, p.1). Additionally, the delayed conversion constrained the capability for U.S. federal government TSP participants to make financial transactions. The U.S. Senate Committee on Governmental Affairs investigated the TSP conversion delay and determined that the lack of competent IT leaders and managers contributed significantly to the conversion delay.

Another example of a recent challenged IT initiative was the U.S. Internal Revenue Service (IRS) Business Systems Modernization project. The IRS project, which was launched in 1998, was designed to enable the IRS to modernize the manner in which it conducts business. It "is more than a quarter-billion dollars over budget. Its key component, renovation of the master database of taxpayer records, is more than three years behind schedule. Five other modernization-related components are late and busting their budgets" (Harris, 2004, p. 44). The TSP and IRS IT initiatives are examples of how IT investments failed to realize the organizations' expected outcomes.

The failure of IT initiatives such as the TSP and IRS examples is likely to continue to occur unless IT leaders and managers gain and use leadership and management competencies to complement their technical competence. IT leadership and management certificate programs such as the BITM Certificate Program might help prepare IT leaders and managers with IT leadership and management competencies. As a result, IT

leaders and managers could more effectively help produce the outcomes expected from their organizations' IT investments. Various researchers noted concerns about the ability of education programs to prepare IT professionals with needed competencies.

Selingo (as cited in Liu, Liu, Koong, and Lu, 2003) suggested that universities and colleges failed to adequately educate graduates to meet the needs of the IT industry in the previous decade. Selingo also noted "a disconnect between what the market needs and what the colleges are providing" (as cited in Liu et al., p. 191). Livingood (2003) cited the failure of higher level educational programs to adequately prepare IT staff as a primary contributor to the lack of skilled IT professionals. Their dependence on IT requires organizations to attract, employ, and retain IT leaders and managers with the competencies to lead and manage the organization's IT environment. However, global business leaders noted significant concerns about the lack of skilled IT professionals to support constantly changing business environments (Cortez, Dutta, & Kazlauskas, 2004).

Concerns regarding the competence of IT leaders and managers suggested a study of IT leadership and management certificate programs might add new knowledge. IT leadership and management certificate CEPs such as the BITM Certificate Program might help prepare IT leaders and managers with IT leadership and management competencies. Competent IT leaders and managers could more effectively help produce the outcomes expected from their organizations' IT investments.

Statement of the Problem

The problem is that many IT leaders and managers lack leadership and management competencies. Caruso and Gentry (2005b) noted, "Leadership is critical to the success of all enterprises. Nowhere is this need more apparent than in the IT world" (p. 1). Caruso and Gentry posited, "The best technologists are often promoted and then left without guidance to learn the leadership roles [competencies] on the job, resulting in demoralized teams, overbudget projects, and a lack of project direction" (p. 1). Little research was located that

(Continued on page 4)



Improving Performance Effectiveness (cont.)

explored the effectiveness of IT leadership and management certificate programs.

information for future IT leadership and management certificate program curriculum designs.

Purpose of the Study

The purpose of this qualitative, phenomenological case study, using a modified van Kaam method by Moustakas (1994), with audio taped and transcribed unstructured interviews, was to explore the lived experiences and perceptions of a purposive sample of 20 BITM Certificate Program graduates living in the metropolitan Washington, DC, area. The researcher sought to explore how the participants used the IT leadership and management competencies gained, if any, from their BITM Certificate Program experiences, to help produce the outcomes expected from their organizations' IT investments. Many individuals serving in global IT leadership and management positions lacked IT leadership and management competencies (Caruso & Gentry, 2005b). The study involved only BITM Certificate Program graduates who served in an IT leadership or management position and who have served in an IT leadership or management position for at least 1 year. The phenomenological research design was appropriate because the researcher sought, as Moustakas concluded, "to determine what an experience means for the persons who have had the experience and are able to provide a comprehensive description of it" (p. 13).

For the purposes of the study, the central theme and its complementary foci was to attempt to (a) describe the participants' lived professional IT leadership and management experiences after completing the BITM Certificate Program, (b) explain how the program might have prepared the participants with IT leadership and management competencies, and (c) examine what might be needed in the current program curriculum to help increase the leadership and management competencies of IT leaders and managers.

Data from the participant interviews were distilled and emergent themes were identified. The data from this study can provide organizational leaders with information regarding recruitment strategies, hiring and placement decisions, and formulation of leadership and management mentoring programs for information technologists. Additionally, the data can provide continuing education program managers with

Significance of the Problem

Gomolski (2005) reported, "Across all industries, the average organization plans to devote 3.5 percent of its gross revenue to IT expenses in 2005" (p. 4) in the United States. The U.S. gross domestic product (GDP) for 2003 was \$11 trillion (Simons, 2004/2005). The *OECD Observer* reported the "Gross Domestic Product (GDP) is defined as the sum of all goods and services produced in a country over time, without double counting products used in other output" ("Is GDP," 2004/2005, p. 30). Simons reported that the global GDP in 2003 was equivalent to \$34.6 trillion dollars. This study was significant because competent IT leaders and managers could potentially help the United States and other countries realize the outcomes expected from their substantial IT investments.

This study was also significant because it sought to provide data regarding IT leadership and management competencies that could affect thousands of IT leaders and managers. The U.S. Department of Labor, Bureau of Labor Statistics (as cited in U.S. Department of Labor [DOL], 2004) reported that approximately 284,000 computer and information systems managers were employed in the United States in 2002. As reported by the U.S. Bureau of Labor Statistics, computer and information systems leaders and managers influence significant aspects of organizational activities, productivity, effectiveness, and efficiency. The U.S. Bureau of Labor Statistics projected the growth for computer and information systems managers from 2002 to 2012 to be "much faster than average growth" (DOL, 2005, ¶ 1). The "much faster than average growth" category is the Bureau's highest category of growth expectation level. The computer and information systems career field is projected to increase 36% or more by the year 2012 (DOL, ¶ 1). Little data currently exists about how IT leadership and management certificate continuing education programs (CEPs) prepare IT leaders and managers with IT leadership and management competencies. This qualitative phenomenological case study of the BITM Certificate Program graduates' post-program experiences and perceptions sought to add meaningful data to the body of leadership knowledge.

(Continued on page 5)

(Continued from page 4)

Nature of the Study

A qualitative, phenomenological case study approach was used for this research. Priest (2002) noted that phenomenology involves describing everyday experiences to understand the essential structure of those experiences. This qualitative phenomenological study will attempt to “understand people’s perceptions, perspectives, and understandings of a particular situation” (Leedy & Ormrod, 2001, p. 153). A qualitative phenomenology research method was an effective approach for this study because it enabled the researcher to (a) “gain insight about the nature of the particular phenomenon, (b) develop new concepts or theoretical perspectives about the phenomenon, and/or (c) discover the problems that exist within the phenomenon” (Leedy & Ormrod, p. 148).

Kleiman (2004) suggested that phenomenology studies focus on the lived experiences of participants in a specific phenomenon. He noted lived experiences reveal one's immediate and pre-reflective consciousness about an event one experienced. Kleiman further suggested that such lived experiences become the basis for reflecting on an event and transforming the event into an object of consciousness. Bernard (2000) provided additional insight about phenomenology. The phenomenological research method is appropriate for this study in that, as Bernard noted, phenomenology “emphasizes direct observation of phenomena” (p. 20). He noted phenomenologists seek to describe their experiences rather than attempt to explain what they experienced.

The qualitative, phenomenological case study was appropriate for this research because the BITM Certificate Program graduates’ perspectives regarding their program experiences were described in the study. The participants selected for this research study were graduates of the BITM Certificate Program. Bernard (2000) noted, “If you want to know about the lived experience of individuals, you need a nonrandom sample of respondents. You choose those respondents because they offer insight into something that they are best able to talk about—their own lives” (p. 192).

The research procedure included unstructured interviews with open-ended questions. Bernard (2000) argued that unstructured interviews involved having a clear plan and exercising minimum control over the respondent. Bernard also noted that unstructured interviews enable respondents to freely express themselves at the respondents' pace. He stated, “A lot of what is called ethnographic interviewing is unstructured” (p. 191). Bernard emphasized the value and benefit of unstructured interviewing and maintained the following:

When you want to know about the lived experience of fellow human beings—what it’s like to survive hand-to-hand combat, how you get through each day when you have a child dying of leukemia, how it feels to make it across the border into Texas from Mexico only to be deported 24 hours later—you just can’t beat unstructured interviewing. (p. 193)

Unstructured interviews were conducted to provide the participants the greatest latitude and flexibility in responding to the interview questions and to facilitate asking follow-up questions based on the participants’ responses. Each interview lasted approximately 30 to 60 minutes and was audio taped to assure each participant that the information was accurately documented. After collecting all the interview data, the data were analyzed to identify emergent themes relating to post-BITM Certificate Program IT leadership and management competencies the participants might have gained and used to help produce the outcomes expected from their organizations’ IT investments.

Research Question

This study was guided by the following research question: How has including leadership and management competencies in an information technology education program prepared graduates to help produce the outcomes expected from their organizations’ IT investments?

Dr. Boddie’s article will continue in the next issue of Info Trends for Information Leaders.



IT Security Trends:

Highlights of the 2006 Gartner IT Security Summit

By Paul Flanagan, Les Pang and Kathleen Schulin

Held in Washington, DC in early June, the Gartner conference covered a broad array of topics related to the management and implementation of security within organizations. The following are some of the key observations made by IRMC attendees:

Keynote Thought

The challenge of the 21st Century is more information and less wisdom. This was an observation of Mary Matalin, one of the Keynote Speakers, while addressing Info Security, The Patriot Act, Civil Liberties, and Privacy.

Managerial Trends

Information security managers are facing new and expanding challenges as the IT security discipline is maturing.

- ◇ Executives and budget approving authorities are expecting a return on investment from security expenditures. Some are even expecting more security at a lower cost.
- ◇ Managers need to apply structure and proven approaches to security management such as quality assurance, strategic planning, and policy and program management.
- ◇ Managers need to be able to have the conversation with the senior-most organizational leader about baking-in security—physical and information security go hand in glove.
- ◇ The first 90-days are the most vital in identifying security vulnerabilities and establishing a remediation plan—people and organizational culture are often the keys, not technology.
- ◇ Information privacy is a corporate responsibility that must be addressed cooperatively at the most senior levels of an organization.

The Federal government may have a security breach disclosure law similar to those found in about 33 states.

For the private sector the true cost for security and privacy breaches cannot be measured by the cost of fines or penalties from regulators. The real cost is the loss of trust from current and future customers.

Approaches for Reducing Security Expenditures

- ◇ Instead of a collection of best-of-breed point solutions, look into single-vendor security suites.
- ◇ Acquire sound and properly tested security tools in the first place which are absent of vulnerabilities and other security weaknesses.
- ◇ Examine open source products for reducing total cost of ownership.
- ◇ Re-engineer in-house software development processes to emphasize security and thereby reduce producing code with security flaws.
- ◇ Move the management of "mature IT threats" from the IT security department to the operations department where costs of labor and hardware are lower.
- ◇ Use automated approaches to reduce labor costs such as self-service password reset technology.
- ◇ Investigate and challenge the security of purchased software at the application level. As network security becomes stronger, the applications become logic targets for security breaches.

New and Growing Threats

- ◇ Spam relays – Spam can be distributed via innocent third parties similarly to denial-of-service attacks.

(Continued on page 7)

(Continued from page 6)

- ◇ Lost or stolen laptops and other small information devices – The VA stolen-laptop incident underlines this security breach. (Expect more organizations requiring full-disk encryption of laptops.) Small handheld devices need to be password protected and an organization must incorporate the ability to disable or “kill” devices once they are lost or stolen.
- ◇ New technologies – RFID, Voice over IP, Bluetooth, Web Services and other emerging or maturing technologies have potential security issues which need to be addressed.
- ◇ Instant Messaging is coming a part of the enterprise communications infrastructure and must be managed at the enterprise level.

Technology Trends

- ◇ Organizations are moving from a single security perimeter around the enterprise to multiple perimeters within the enterprise – this is due to insider threats which create most of the security problems for an enterprise.
- ◇ Microsoft is offering a collection of free or low-cost security tools as part of its upcoming Vista operating system and its future security products.
- ◇ Security safeguards are being pushed upstream into the “cloud” such as switches in the Internet.
- ◇ Security software is becoming embedded in silicon.

New Security Approaches and Tools

- ◇ Security Incident Event Management (SIEM) – provides for situational awareness of the security environment through the use of distributed data collectors linked to a centralized monitoring system.
- ◇ Virtualization – having a physically distributed security application within a virtual server.

- ◇ Code scanners – automated systems are used to review code for possible security breaches such as buffer overflows.
- ◇ Alternate sites in the event of a disaster – use hotels and motels as temporary work sites for employees – this came from the Hurricane Katrina experience.
- ◇ Password recovery tools – these are getting much more powerful as processors improve (faster clock speeds and the use of multi-core microprocessors).

Other Insights

- ◇ Complying with security regulations does not mean that you are more secure.
- ◇ Although better than WEP, wireless laptops using WPA2 are still vulnerable to hackers.
- ◇ Security managers need to show results and success after project implementation in order to convince managers to continue funding on subsequent projects. Migrate from security point solutions to a continuous security improvement program.
- ◇ The use of current investigative technologies to search for terrorists often results in an excessive number of false positives.
- ◇ Poor architecture equals poor security.

A Lesson Learned...

**“Poor architecture
equals
Poor security”**

SOA...Demystified!

By Drs. Ai-Mei Chang, Les Pang
and Donald Chi (Food and Drug Administration)



SOA is an acronym for "service oriented architecture." The Office of Management and Budget (OMB) calls it an architecture composed of a set of interdependent services which can be defined at various levels, from federal-wide, to a specific system solution within an agency. The agency defines a service as a discrete unit of functionality that can be requested, performs one or more operations, and returns a set of results. Many consider SOA as an evolution in architecture, not a revolution, and it captures many of best aspects of the architectures that came before it.

SOA is more than technology. It is an architectural strategy which is referenced in the current Data Reference Model (DRM 2.0) as part of the Federal Enterprise Architecture (FEA) as a means to provide data sharing and system interoperability. It looks at SOA from this perspective -- "nodes on a network making resources available to other participants in the network as independent services that the participants access in a standardized way."

Some say that an organization's Chief Architect (or equivalent) should take the lead in this SOA evolution. It should also involve the Chief Technology Officer, the Information Systems Security Officer, and whoever is in charge of application architecture.

The technology piece of SOA is typically based on a concept called "Web Services" -- simple, self contained applications which perform functions ranging from simple requests to complicated business processes. (Note: Web Services is not SOA. Web Services plus a number other things together yield SOA. Enterprise Service Bus (ESB) and middleware provides the other "things" to create the SOA environment.) This concept uses:

- Extensible Markup Language (XML) - all components are written in this language
- Web Services Description Language (WSDL) - description of web services that allows the systems of one organization to use the services of the other directly
- Universal Description, Discovery and Integration (UDDI) - directory services to discover Internet-based services, and
- SOAP – a protocol that permit services to be invoked over the Internet.

When two organizations are aware of each other's services through WSDL, they can link or bind to each other – provided that security concerns are properly managed. SOAP acts like an envelope for the WSDL delivered by HTTP.

It should be pointed out that SOA can be implemented using any service-based technology with loose coupling among interacting software agents. Imagine a system involving two entities in which one is providing a service to another. Loosely coupled means a change in one entity will not require a change in the second entity. One classic example is our phone system which changes in the hardware in one phone will not impact that of the other phone. Loose coupling also means that either system has no knowledge of the state of the other system.

However, the important part of SOA is not its technology but how it can be used to improve the business processes in an enterprise or in a business-to-business (B2B) environment when it is coupled with Business Process Management (BPM), and more importantly, in the integration of applications built and run on different platforms. For instance, a J2EE application can be integrated with CICS applications, and rendered a service through the use of adapters.

Some argue that SOA is a "style" of design, deployment, and management of applications and software infrastructure and therefore it should be called "service-oriented style." However, the problem with that term is that the corresponding acronym "SOS" has some negative connotations.

Benefits for Government

Generic benefits include internal and external integration, multi-channel application integration and strategic business transformations. From a government perspective, OMB sees the following benefits:

Transformation:

- Cost-savings
- Improved mission-performance

Adoption:

- Identification and establishment of shared service centers for HR & FM Lines of Business

(Continued on page 9)

(Continued from page 8)

- Standardization and streamlining of business processes
- Migration to common solutions

Foundation:

- Identify opportunities for common solutions
- Architect common solutions
- Establish governance models
- It supports information sharing among different systems and reusability (shared services).

Enterprise architects believe that SOA will help businesses respond more quickly and cost-effectively to the changing market conditions they may face by promoting reuse and interconnection of existing IT assets rather than more time consuming and costly reinvention. In short, SOA can render an IT organization agile, and hence make the business organization agile.

How SOA will be used in Government

OMB is looking at these areas for SOA applications:

- Lines of Business
 - Operational Phase
 - Human Resources (HR) Management, Financial Management (FM), Grants Management (GM), Case Management (CM), and Federal Health Architecture (FHA)
 - Planning Phase
 - Information Systems Security (ISS) and IT Infrastructure
- E-Gov Initiatives
 - Driving toward usage and adoption by agencies
 - Self-sustaining fee-for-service model
- SmartBUY Agreements

Another key application is the need for integrating systems in different agencies such as FBI and CIA.

Examples of SOA Applications in Government

Typical examples include sharing of data between States and the Federal Government, the exchange of data among Federal entities and the numerous supply chains consisting of vendors, brokers and government agencies. Non-traditional applications include use for emergency first responders, medical data distribution by researchers and GIS information providers. The potential use in Federal government is limitless.

The DoD is trying to transition from data silos located in disparate networks and within legacy systems to an enterprise environment where users can access any information and can post their contributions for discovery purposes. To achieve that goal, the department is advocating publishing and subscribing data and services supporting authorized users. Key to this concept is a shared space consisting of metadata registries and information catalogs -- all of which leverages SOA. The net-centric initiative is based on the SOA concept.

Under DoD Directive 8320.2, the goal is to make data visible, accessible and understandable. The Department wants to facilitate data sharing through Communities of Interest (COIs) -- any collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared vocabulary for the information they exchange.

Challenges Associated with SOA

Technical challenges include:

- Decomposing the business into discrete services
- Continuous nature of development (not discrete projects but continually evolving applications)
- Managing metadata, which helps ensure the common semantic understanding of terms across different domains
- Security – firewall issues (Note: Without security we should not use SOA because all data are expressed in XML, which are text-based. A number of standards have been implemented in SOA. This is another topic that requires a one semester course. For instance, in the SOA environment, Federated Identity and trust management become critical.)

(Continued on page 10)

SOA (Cont.)

(Continued from page 9)

Managerial challenges include:

- Fostering an environment of sharing
- Finding a champion who can talk business and communicate with technical personnel
- Convincing the budget people of the economic value (ROI) of SOA
- Fear of losing power and jobs due to this new technology
- Resistance to change by developers and stakeholders

Also, Gartner identified four major challenges: questions such as which agency owns the service components and interfaces, who pays for the SOA infrastructure, implementation and use, what are the priorities in implementation, and who uses what services.

Best Practices in Implementing an SOA Strategy

- Have an architectural platform in place first. It should support a single governance structure (centralized control), metadata standards (common vocabulary), and a repository (allows for sharing SOA components). A cross-functional architectural steering committee would be useful for guiding the SOA evolution.
- Do pilot implementations starting with small successes and learning from these experiences.
- Identify services by focusing on processes that provide the highest value for the government agency.
- “The bottleneck is always at the top of the bottle.” Get buy-in from the top executives and managers to ensure the free flow of resources and other support and increase the chances for success.

What's Next for SOA

OMB has the following vision:

- Citizen Service: One view of government

- Performance: Common performance measurement framework for OMB and all agencies; robust budget-performance integration
- IT & Services: Minimal redundancy in IT spending; component-based architecture promotes reuse
- Budget Allocation: Budget analyses take business lines into consideration; funds allocated to support cross-agency collaboration

For a technical standpoint, “BPEL” has become a buzzword associated with SOA. According to IBM, Business Process Execution Language is an XML-based language for the formal specification of business processes and business interaction protocols. It enables web services to support business transactions. It is the result of a cross-company initiative between IBM, BEA and Microsoft to develop a universally supported process-related language. BPEL links SOA with BPM, narrowing the chasm between business and IT organizations.

In conclusion, building the basic technology foundation was relatively easy, but the managerial and cultural changes that lie ahead to support SOA may be a rough road. However, many say that it will be worth it.

References

Burk, Richard, Director, Federal Enterprise Architecture Program, OMB, The Government's SOA Roadmap

Data Reference Model 2.0, Federal Enterprise Architecture Program, Office of Management and Budget and Federal Chief Information Officer Council, November 17, 2005

DoD Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense", ASD(NII)/DoD CIO, 12/02/2004

Gartner, GCON: The Gartner Government Conference 2006, 14-16 June 2006 Washington DC

IBM, Retrieved from:
<http://publib.boulder.ibm.com/infocenter/adiehelp/index.jsp?topic=/com.ibm.wsinted.glossary.doc/topics/glossary.html>

Leganza, Gene, Vice President, Government Research, Forrester Research, SOA - The Key to Transforming Government Services.

Service-Oriented Architectures for E-Government Conference, various presentations.

Wikipedia. "SOA" definition.

Enterprise Instant Messaging

By Wade Doenges, Maureen Pearson, Joel Rothschild, Stephanie Spengler and Mickie Wiser

“Changing World of the CIO” Students

Instant messaging (IM) is the act of instantly communicating between two or more people over a network such as the Internet. The term Enterprise Instant Messaging (EIM) is the next generation of instant messaging where the technology is used within an organizational construct to deliver similar services and capabilities, thereby improving organizational communications. Instant messaging requires the use of a client program that hooks up an instant messaging service and differs from e-mail in that conversations are then able to happen in real-time. Most services offer a "presence awareness" feature, indicating whether people on one's list of contacts are currently online and available to chat. Most instant messaging applications also include the ability to set a status message, roughly analogous to the message on a telephone answering machine. EIM is the result of the acceptance, by businesses and government organizations, of technology that is in wide use in the public sector. It has the potential to revolutionize corporate communications.

Benefits

The primary benefits of implementing EIM revolve around the increased efficiencies of the worker sitting at his desk, using his computer to communicate. He will be able to collaborate on the fly when information is needed, coordinating tasks and getting answers to questions much faster than with normal email. He won't need to schedule a meeting ahead of time, or schedule a meeting room, or worry about the availability of a phone or video bridge. He will be able to look at his screen and know if the people he needs are available, reducing both phone tag and email tag. He will be able to communicate with one person or a group of people at his site or anywhere on the network, depending on how EIM is implemented. He will be able to have multiple conversations at once -- for example, he can hold an IM session at the same time he is on the phone.

With the advent of collaborative software incorporating both IM and document sharing, the benefits for the organization could include a reduction in unnecessary travel, saving on travel expenses. Workers can “meet” together as often as necessary, whether they are in an office, on a client site, or at home in their pajamas. This can lead to increased quality of work due to increased availability of skilled personnel. One of the authors is actually doing this today using the Groove application to coordinate service delivery and share key stakeholder requirements across a collaborative Booz Allen,

Dell Professional Services and InSource Partners teaming. From locations in Japan, Hawaii, San Diego, Chicago, Bahrain and Naples, people are able to work with a shared voice, and without track/edit changes being necessary on the documentation.

Challenges

These potential benefits will not be realized without first addressing significant issues and challenges. IM is a vulnerable technology that needs significant security management. Security measures need to include protection against viruses, worms, , malicious code, spam (called “spim” for IM), and other security vulnerabilities. The organization needs to ensure the infrastructure is protected using firewalls and similar safeguards and likely include encryption of the EIM traffic.

As with many new technologies, there is a lack of recognized standards. In addition to addressing security and infrastructure issues, the organization needs to address the IM conversations themselves. Regulations such as HIPAA require businesses to save and store digital information. IM conversations are business records, which must be saved and archived like email, raising potential electronic records management issues. Storing the IM conversations leads to privacy issues. When the IM session is initiated, do participants need to be notified the conversation will be saved? Can the conversation later be divulged without the participants' consent? Can these issues be addressed in the same manner as electronic mail accounts? Is the only way you can use EIM applications is to consent to their monitoring?

The organization needs to have guidance and policy in place for the use of EIM in the workplace. It has the potential to reduce productivity; workers can spend working hours carrying on personal conversations. EIM sessions are by nature more informal than email, workers need to be careful not to divulge sensitive information in the course of the session. Training and policy are essential to address the control of sensitive information and inappropriate conversations. In addition, EIM can be a psychological challenge for some workers who are not comfortable with technology, and may resist using it. It can also be a nuisance with multiple chat sessions appearing on the business computer at inappropriate times.

(Continued on page 12)

Enterprise IM (cont.)

(Continued from page 11)

EIM Use in Government and Military Environments

In the current era of widely dispersed government agencies and worldwide military deployments, it was only a matter of time for an EIM solution to take hold. Government agencies have a critical need to share timely information and interact with other agencies around the world in near real-time. At Headquarters United States European Command (EUCOM), the commander, EUCOM staff and component planners conduct online planning sessions using InfoWorkSpace which is an enterprise suite of collaborative tools containing an integrated instant messaging client. Face to face meetings are kept to a minimum, which has helped to reduce the travel budget of the Command. In this time of shrinking resources this has been of great benefit.

The most visible use of an EIM solution is on the Army and Air Force portals. The Army portal, also known as Army Knowledge Online (AKO), is reported to be the largest online community in the world. An IM solution was incorporated into AKO to enable soldiers and their families a means of communicating during deployments and separations. The Air Force is using their IM solution to collaborate on issues and is looking to use it as a means of conducting “town hall” meetings in the future. Both the Army and the Air Force use the Bantu EIM Platform as their IM solution. Bantu is also being used by the Navy, Homeland Security and the State Department, with discussions of using Bantu to allow EIM across the services (Kenyon, 2004).

EIM -- The Future

If the collaborative effort of the US Army and Air Force, in conjunction with Northrop Grumman and Bantu (Kenyon, 2004), is any indication of the future of EIM, it shows that not only will EIM continue to thrive within business walls; it will be used across boundaries. Deploying secure, “interdomain” messaging capabilities will allow the Department of Defense to set up forums, user groups and chat rooms for specific missions and tasks. It also can restrict users from having inappropriate access to “User Lists” if there is no distinct need to know.

“The views expressed in this publication are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government.”

Corporate America is also riding the wave of EIM. Research done by IDC reports that sales of EIM applications have risen 37 percent this year alone (Boulton, 2005). IDC also reports that the EIM market will at least double between 2005 and 2009, with sales of EIM servers and services rising to \$736 million (Boulton, 2005). America Online, Yahoo, and Microsoft are all selling EIM tailored versions of their messaging services, and businesses are buying (Hu, 2002). What began as large companies employing a hybrid of free instant messaging products and their own administrative tools (Instant Messaging Gains Corporate Success, 2002) has evolved into an industry that maximizes global knowledge sharing.

Conclusion

Enterprise instant messaging, although initially resisted by businesses and government alike, is a system that has grown and enveloped our “must have this now” society, and is being deployed as a method to continue streamlining the efficiencies of our e-government. Collaboration, formerly done with expensive trips and summits, can now be done with something as simple as a computer and a phone line.

There are issues that need to be addressed, largely in the realm of security, but vendors are working to address them. The organizations deploying these systems across their enterprises are also working on developing the policies and procedures for use and monitoring. With mitigations in place, it would seem that EIM is here to stay.

Note: No endorsement of any products mentioned in this article is expressed or implied.

INFORMATION RESOURCES MANAGEMENT COLLEGE

The World Leader in Information Resources Management Education

300 5th Avenue Marshall Hall (Building 62)

Fort Lesley J. McNair, DC 20319
(202) 685-2096

<http://www.ndu.edu/irmc/>

ISSUES ONLINE: http://www.ndu.edu/irmc/out_infott.htm

Director: Dr. Robert Childs

Dean of Faculty & Academic Programs:

Dr. Elizabeth McDaniel

Editor-in-Chief: Dr. Les Pang

Associate Editor: Dr. James Kasprzak