Leveraging the Information Infrastructure

A New Foundation For Business Strategy at Electric Utilities

Paradigm Shift International, January 2006, Rick Dove

EXECUTIVE SUMMARY

Information technology has come out of the closet. Not because it delivers value directly, but because it enables the information infrastructure that both current and future business performance is now dependent upon.

CEO, CFO, and CIO can find common ground and values in infrastructure leverage.

Infrastructure is a fundamental enabling and constraining platform of possibility, whether at the national, community, or corporate level. What infrastructure doesn't facilitate will not happen. What it supports defines identity and performance.

Like a nation, with its energy, banking and postal delivery segments, a corporation has multiple segments of infrastructure. But some infrastructure segments are more critical than others

The corporate *Information Infrastructure* has emerged as the strategic leverage point for business. It either provides needed information when and where needed, or it doesn't. Individual and organizational productivity and capability is held hostage by this infrastructure.

Distinguished from the Information Infrastructure is the IT Infrastructure. Attempting to deliver strategic value at the Information Infrastructure level consistently and continuously without an enabling IT Infrastructure is impossible.

Xcel Energy's strategic-IT initiatives are portrayed anew as an infrastructure focus, with manageability, predictability, and credibility as outcomes.

Alternatives for achieving infrastructure management are examined, and one that offers rapid and safe migration is discussed as a benchmark.

INTRODUCTION

Functioning systems are built on infrastructure, whether they are countries, communities, or companies. Electric, gas, and water utilities have concerns in all three arenas: as part of the national infrastructure, as providers of community infrastructure, and as users of corporate infrastructure.

All infrastructure is not created equal – some is critical. At the national level, for instance, the power grid is part of the critical infrastructure, the Postal Service is not. At the community level the electric utility serving the area is critical, garbage pickup is not. At the corporate level an electric utility's Energy Management System is critical, the Customer Billing System is not. How these lines are drawn will be seen later.

As citizens we have been sensitized recently to the importance of *critical* infrastructure at both the national and community levels with 911 and Hurricane Katrina. As corporate managers we need to be equally sensitized to the importance of critical infrastructure at the corporate level, but not simply as a disaster vulnerability. Corporate infrastructure, like community and national infrastructure, also determines and sustains identity and capability – what we are and what we can do.

At the national level the 911 wake up call precipitated the formation of the Department of Homeland Security – a custodian chartered to focus on the critical infrastructure. A new department is not needed at the corporate level, just a new awareness and focus. Moreover, the nature of the corporate focus must be broader.

The focus is security-based at the national level: vulnerability reduction and service restoration in the event of damage. Cyber security figures heavily in the national plan, with major government initiatives flowing into the electric utility world.

In addition to security, however, the corporate focus needs a proactive component, one that consolidates and amplifies the strategic leverage of infrastructure. Whether its lowering costs, introducing new revenue generating services, or growing through M&A, information access and flow has emerged as the success-gating factor. The corporate information infrastructure has become a key strategic asset.

Though this is true across most industrial sectors, regulated utilities have been later than most to wake up. Some say this is the result of regulation. Perhaps as much it is the result of a management legacy of power engineering.

The IT integration mess at most utilities is well known as a source of unnecessary business cost, a road-block to best-practice upgrade, and a cause of business inefficiency and customer dissatisfaction; yet few have made strategic effort to attack the problem. "We don't know how to deal with it," is the commonly heard candid reason. Remove the frustration, and what is being said is that safe, affordable migration paths are elusive.

What follows will first look at the necessity to change this, and then define some relevant aspects of infrastructure. The obstacles standing in the way of decision and action are then explored. Finally, discussions of successful approaches and paths to consider point the way to building an affordable and manageable information infrastructure in a legacy environment.

THREE IMPERATIVES

1. Leverage IT as business strategy.
2. Include and value IT expertise in corporate decision-making bodies.
3. Create trust in IT capability.

THREE RELATED IMPERATIVES

Xcel Energy's Chairman (mid-2005), Wayne Brunetti, stated the case: "I'm not going to get linemen to climb poles any faster or meter installers to put in meters any faster. The future of productivity improvements has to do with the systems we use to plan, buy, and schedule things for our crews and our company."[2]. Information technology is today's leverage point for business performance, innovation, best practice, and compliance frontiers. Corporate utilization of information technology (IT) as strategic leverage is the first of three related imperatives, and drives the other two.

Consider what's in the pipeline: AMR, distributed generation, BPL, demand pricing, intelligent appliances, improved reliability automation, improved outage management, wireless-connected field crews, cyber security, SCADA on the network, grid-connect responsibility, SoX compliance, and more. All of this is IT enabled and IT dependent. All of this impacts operating cost and revenue opportunity. Key point: all of this is the core of today's business performance and strategic leverage.

Take AMR and OMS as two examples. The potential benefits of both are compelling: better service *and* lower costs. To believe the promotion, implementation is a simple matter of decision and action. Vendors stand ready with a variety of approaches. Many utilities have already committed, and many more are weighing the alternatives.
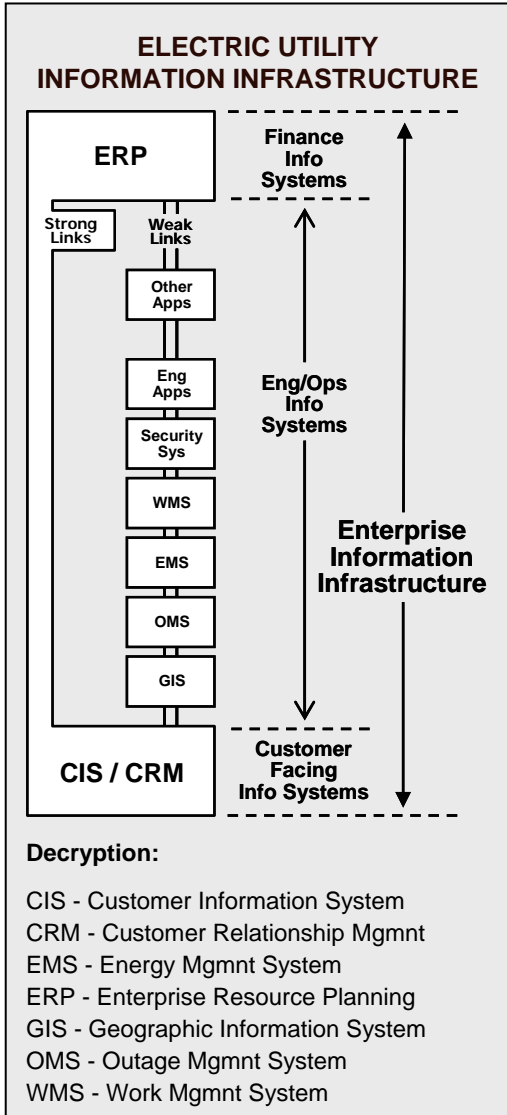
Annual planning easily includes these programs as priorities for consideration. Budget proposals address evaluation, acquisition, and installation for both the equipment and the enabling IT. Program costs, benefits, and risks are evaluated. Cost benefit ratios are compelling. Risks, however, are another matter.

In most industries the strategic spotlight has already focused on the leverage of IT. This same spotlight also illuminates a general shortfall in capability. Traditionally corporate IT has been budgeted, staffed, and managed as a tactical support function. This legacy has become a risk, evidenced by the common hew and cry in business, management, and academic publications everywhere: companies must improve IT governance, install IT expertise at the board level, and include the CIO in business strategy councils. For a good sampling of the issues, see Harvard Business Review's *Information Technology and the Board of Directors*[3]. Addressing this capability shortfall is the second of the three related imperatives.

The third imperative belongs to the CIO: new skills and new practices are needed. The game has changed. Governance (get your act together), business strategy (become an executive team player), and communication (and help us understand what you know) are the key skills wanted in the CIO today.

Governance is a pretty highfalutin word. The focus goes to governance when things look out of control. Out of control has two key components: IT projects don't deliver as expected, and IT management isn't aligned with corporate goals. Gartner's study (see side bar) shows CIO *credibility* hinging on two things: 1) how well the CIO runs IT, and 2) how well IT helps the business achieve its goals. Note that word credibility – it means trust.

The three imperatives are summarized in the sidebar. They are related because you can't accomplish the first effectively if you don't have the second, and you won't do the second if you haven't got the third. Importantly, the first and third are also related because both are enabled or inhibited by the nature of the information infrastructure. Leverage is the amplification of capability, which is only possible when the infrastructure enables it. Trust is the product of predictability, which is virtually impossible when the infrastructure impedes it.

ELECTRIC UTILITY INFORMATION INFRASTRUCTURE

ERP

Strong Links

Weak Links

Finance Info Systems

Other Apps

Eng Apps

Eng/Ops Info Systems

Security Sys

WMS

EMS

Enterprise Information Infrastructure

OMS

GIS

CIS / CRM

Customer Facing Info Systems

Decryption:

CIS - Customer Information System
CRM - Customer Relationship Mgmnt
EMS - Energy Mgmnt System
ERP - Enterprise Resource Planning
GIS - Geographic Information System
OMS - Outage Mgmnt System
WMS - Work Mgmnt System

STILL WAITING
(CFO Magazine[4] survey results, Dec 2005)

What is your approach to IT?
- 75% say it's strategic.
- 22% say it's a utility.
- 3% aren't sure.

BUT...

Has IT produced the returns you expected over the past year?
- Only 40% say yes.
- 60% say no or are unsure.

Has Sarbanes-Oxley fostered a closer relationship between finance and IT?
- Only 34% say yes, down from 48% a year earlier.

INFORMATION INFRASTRUCTURE

Webster defines infrastructure as: "An underlying base or foundation, especially for an organization." In electric utilities infrastructure typically means the equipment, systems, and wires used to generate, transmit, and distribute electricity. Apart from this service infrastructure, a utility's business activity also has an infrastructure. One that enables and constrains value creation.

Value creation relies mainly on two intangible assets: information and human capital. The right information in the right place at the right time determines how productive and effective people and processes can be. Productivity is tied to the availability and timeliness of information. Effectivity is tied to the quality of the information. Similar to the service infrastructure, information storage (data bases), transformation (applications), and delivery (networks) employs equipment, systems, and wires. The physical part is the IT infrastructure, the value-creation part is the information infrastructure.

All companies have an information infrastructure. How it is constructed determines whether it does more enabling or more constraining. The side bar depicts a typical arrangement that has evolved in today's electric utility, more or less.

A loose review of history will put this picture in perspective, as evolution continues.

Management Information Systems (MIS) spawned the information infrastructure in the '50s by automating financial management activities. In the '70s Material Requirements Planning (MRP) expanded the scope into operations, but principally to support financial management needs. In the '80s Enterprise Resource Planning (ERP) began extending the infrastructure across a broader-base of business processes, eventually encompassing Supply Chain Management (SCM) in the '90s – but again, principally to aid financial planning and management.

Independently the needs in marketing and sales management in the '90s created demands for CRM (customer relationship management) and CIS (customer information systems). Customers are the source of revenue and the consumers of service, concepts tied closely to the financial interests of ERP. Strong links naturally formed between these two areas as the information infrastructure emerged as *business* process support.

Ignored in this expanding integration were the many stand-alone systems that supported various engineering and operations activities. Forging infrastructure integration ties from the business side into engineering and into operations was traditionally viewed as mixing cats and dogs to no benefit – by all sides.

In the '90s, however, the leverage for business performance began shifting. The need for astute management of financial resources didn't decrease – an inadequate job there can still destroy any company. Nor did the need for innovative engineering and competitive operations lessen. But all of these areas had refined their internally-focused improvements to diminishing returns. Continued performance improvement required better utilization of information. Technology made it possible, and early adopters set new performance benchmarks. Then the relentless evolution of market expectations, demands, and opportunities jumped on the bandwagon.

Engineering had their infrastructure. Operations had theirs. Neither saw the need for much internal integration, let alone the need to integrate across departments to the extent that the business side had done. Infrastructure did not have to be integrated to be effective...once upon a time.

The values of an integrated information infrastructure came to the front in the new millennium. Unfortunately the legacy of patch work has become a major barrier for most, and the rush to add new IT-enabled services amplifies the mess.

CRITICAL INFORMATION INFRASTRUCTURE MANAGEMENT

Key Attributes

- Accessible to all relevant decision makers
- Access to all relevant information
- Consistency and accuracy of data
- Real time currency of data

DEFINING CRITICAL INFORMATION SYSTEMS [6]

1. Systems whose rapid failure would lead to a catastrophic loss of life.

2. Systems whose failure or significant degradation would lead to unacceptable economic consequences.

3. Systems whose rapid failure would significantly impact rescue/response efforts.

4. Systems whose significant degradation would significantly impact recovery efforts.

CRITICAL INFORMATION INFRASTRUCTURE

Infrastructures are platforms of fundamental resources that allow organizations to function. If any element of an infrastructure becomes dysfunctional, performance degrades immediately. Yet all elements of the infrastructure are not equal. Some *are* more critical than others.

At the national level, the USA Patriot Act defines *critical infrastructure* as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5]

What made the cut? "...an interdependent network of critical physical and *information infrastructures*, including telecommunications, energy, financial services, water, and transportation sectors."

A joint USA/Russian workshop[6] in 2004 refined the definition of critical systems:

1. Systems whose rapid failure would lead to a catastrophic loss of life.
2. Systems whose failure or significant degradation would lead to unacceptable economic consequences.
3. Systems whose rapid failure would significantly impact rescue/response efforts.
4. Systems whose significant degradation would significantly impact recovery efforts.

Though items 2 and 4 speak just as clearly to any corporate infrastructure, all four have a defining role for an electric utility's *Critical Information Infrastructure*.

Establishing the *critical* perimeter is a job for King Solomon. At first thought few people will agree on what is and is not critical. Every bit of it (no pun intended) is necessary to continue normal functions. That is the very nature of infrastructure. Losing access to an ERP system for a week, however, does not have the same lasting consequences as losing control of an Energy Management System for a week. Nor do the consequences of an incapacitated CRM system compare to an inoperable Outage Management System. You have to think in the extreme and imagine the worst possibilities. The four criteria in the side bar provide a good definitional gauge.

The national critical infrastructure focus through the Department of Homeland Security (DHS) works from the assumption that the infrastructure only needs protected from attack. This is clearly not the case, as evidenced, just for one example, by the cascading power outage that hit 40 million people in August 2003. Fortunately there are initiatives separate from DHS that are addressing infrastructure inadequacy, at least for the grid. These initiatives are addressing needs for better visibility, better management, and better response and recovery capability.

Carry that thought into the corporate infrastructure. Waiting for the corporate version of the August 2003 infrastructure failure before addressing inadequacy is executive suicide, if not corporate suicide as well. Protecting the information infrastructure from attack is of course important as well.

Infrastructure management doesn't exist in the infrastructure architectural picture painted on the previous page. Valuable information assets are isolated or weakly linked at best, and important information is inaccessible to those who need it.

A generic Information Infrastructure *Manager* is depicted on this page with its key attributes. The critical *reactive* objective is optimal restoration of service and operational functionality. Think in terms of the coordination and visibility needed for the recent hurricane aftermaths, and the response and recovery management needed in the face of a concerted professional cyber-attack, as well as more localized events. The critical *proactive* objective is the enablement of safe and predictable IT migration.

<div style="border:1px solid">

CHIEF INFORMATION OFFICER
(Excerpts from Wikipedia[7] –
The On-Line Encyclopedia, Nov 2005)

The prominence of this position has risen greatly as information technology has become a more important part of business.

No specific qualification is typical of CIO's in general; every CIO position has its own specific job description. Many have degrees in computer science, software engineering, or information systems, but this is by no means universal. Many were programmers in the past. Further management training and experience is also required.

The CIO, unfortunately, also carried the backronym* of "Career Is Over". This is due to the fact many CIOs have been fired due to the inability to fix some technical problem, or to direct the technology program of the organization to align it with the organization's goals.

* Backronym – a phrase later back-fitted to an in-use acronym.

</div>

<div style="border:1px solid">

A PRESCRIPTIVE PERSPECTIVE FOR THE CIO

1. Credibility is the issue.

2. Building trust is the antidote.

3. Project predictability is the trick.

4. Infrastructure is the leverage point.

Infrastructure is the business's leverage point for performance and also the CIO's leverage point for building and maintaining respect for IT.

</div>

THE OBSTACLE COURSE

CIO means "career is over", goes the old saw, born of repeated observation. The buck stops there when a major project fails (see side bar). IT projects can be quite expensive, and when they fail to deliver some other part of the business can't perform as planned. High visibility.

A consultancy called IT Cortext has gathered some sobering statistics from a variety of sources. In this compendium[8] one reference is the landmark study done by the Standish group on IT project failure. "The Standish Group research shows a staggering 31.1% of projects will be canceled before they ever get completed. Further results indicate 52.7% of projects will cost over 189% of their original estimates. On the success side, the average is only 16.2% for software projects that are completed on-time and on-budget. In the larger companies, the news is even worse: only 9% of their projects come in on-time and on-budget...[and] have only approximately 42% of the originally-proposed features and functions." That original study was done in 1995. Standish statistics today continue to paint a similar picture.

High visibility failures pinned on IT are not just project based. "It took no more than a simple engineering error, a software malfunction and a communication failure to cause the largest blackout the world has ever seen – the massive power outage that hit 40 million people ... on August 14, 2003." This statement[9] is attributed to Dick Lord, CEO of the Steadfast Group [and] a member of the US Department of Energy Office of Electric Transmission and Distribution Blackout Forum, in his keynote speech to the Australian 2004 GITA conference.

The report of that speech goes on to detail the IT role in that event: "The blackout started in the area surrounding Cleveland, Ohio. The electric utility serving that area suffered an EMS failure several hours before New York lost its power. The EMS failure was software-related so the IT network administration folks came in to fix it. They dutifully failed-over the errant workstation to its backup, observed proper performance for a few minutes and retreated to their stations. Eleven minutes later that workstation also failed, with no backup. According to the records, the IT folks assigned to fixing the EMS never informed the operations folks about the problem. For more than 90 minutes, energy management system operators watched their multiple monitors and wall screens and seeing no new alarms, assumed everything was well with the network, even as 345,000 volt lines were dropping off line and generators shutting down. Cleveland lost power, then Detroit. Lord says the EMS operators' first real clue to the impending disaster was when the lights blinked in their control centre." [5] The gist of the rest of that article indicates that Lord blames the CIO. Some may rightfully take issue with that assessment, but the CIO is convenient. No matter where you go, there you are.

Business and academic factions expect governance, alignment, and communication to harness IT in service to strategy. Soft terms in a hard world. These *are* necessary and timely concepts, but they don't strike to the heart of the problem nor provide the core of a solution. Enterprise IT long ago crossed into the realm of complex systems, where engineering science is still groping for rules of order. To the rest of the company IT projects are a mystery, a too frequent disappointment, risky, and expensive.

The CIO is where the buck stops. Credibility is the issue. Building trust is the antidote. Project predictability is the trick. Infrastructure is the leverage point.

The CIO must take the initiative. If the CEO and Board do not yet recognize the strategic role of IT, taking the initiative may be more difficult, but it is all the more necessary. A late wake up call in top management can only bet on demonstrated competency.

THE UTILITY POSTER-CHILD OF IT LEVERAGE

Xcel Energy was recognized as the top IT organization in the energy and utility market by *InformationWeek* in 2004, and as number 7 of the top 500 IT organizations in America in 2005. Ray Gogel, Vice President and CIO then, had responsibility for *Business Systems*, which manages portfolio performance for Information Technology, Utility Innovations, Corporate Business Planning, and Business Processes. Gogel is still Vice President and CIO now, but with a broader responsibility for *Customer and Enterprise Solutions*, which adds responsibility for Customer Care and Human Resources.

In January 2005 *Computerworld* recognized Gogel as one of the business world's Premier 100 IT Leaders. Dick Kelly, now Chairman and CEO of Xcel, made a telling comment as COO then: "With the help of a strong leadership team and the talented and dedicated members of Xcel Energy's Business Systems group, Ray has turned the IT function at Xcel Energy into a truly visionary model. This honor, following on the heels of the September announcement that InformationWeek ranked Xcel Energy No. 20 in its list of the 500 most innovative users of information technology, is clear evidence that our company is redefining the role of IT in creating business value." [11]

Gogel, probed for infrastructure insight in November 2005 by this author, introduced Mike Carlson as the *Infrastructure Manager*. Mike is actually Vice President of Business Transformation and Customer Value. Gogel's responsibilities, Carlson's title, and Kelly's comment speak clearly of Xcel's strategic view of IT.

Mike described their Information Infrastructure. "We recognize eleven core mission-critical application areas: Finance, HR, CIS, OMS, GIS, EMS/SCADA, Asset Management, Trading Systems, Plant Systems, Technical Infrastructure, and Work Management (logistics, supply chain, time and motion, etc). The most intertwined are OMS, CIS, and Work Management." [see sidebar page 3 for acronym map]

They've just completed a five year plan that transformed a typically chaotic interaction of IT applications into a rational infrastructure, aligning the technology architecture and business processes. "Now we are working on what we've trademarked as the Physics of Process™, so we can anticipate the effects of change and identify which areas of the technology footprint to address in advance. The objective is to avoid those old surprises in broken legacy capabilities caused by forward migration."

"Technical change management is what this is. We crossed the threshold this year from firefighting to something that resembles a managed activity. In the planning phase we ask if we can migrate within the architecture, and can we maintain the integrity of the environment as we migrate."

"We work to KPIs [key performance indices]. We measure standardization, time to solution, performance on delivery, customer satisfaction, among others. One key metric tracks how many problems are identified by the technical staff as opposed to end users. We have automated processes in place that monitor performance. We want to know when performance is dropping or when something stops working immediately so corrective action can be taken before things get out of hand."

As to the critical elements of the Information Infrastructure, Mike says you can see those priorities in the disaster recovery requirements plan. "OMS is a priority over financial management, certainly. CIS is critical for company survival, but if we're not controlling the grid it doesn't much matter."

Xcel Energy saw the handwriting on the wall five years ago and did something about it. They have built an environment of predictable, reliable, aligned IT performance. In so doing, they have created a trusted foundation for the future. Credibility is not an issue here.

REFERENCES

1. "The Door Is Unlocked for CIOs", Special Report: CEO Guide To Technology, *Business Week*, 7/26/05.
2. "The Inside Story", Warren Causey, *EnergyBiz Magazine*, Energy Central, Jul/Aug 2005, pg 64.
3. "Information Technology and the Board of Directors", Richard Nolan and F. Warren McFarlan, *Harvard Business Review*, Oct 2005, pps 96-106.
4. "Still Waiting", Scott Leibs, CFO Magazine, Dec 2005, pg 28.
5. Critical Infrastructures Protection Act of 2001, (section 1016 of) Public Law 107-56 [H.R. 3162] (USA Patriot Act of 2001).
6. Critical Infrastructure definition, see pg 61, *Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings (2004)*, Rossi Iska, National Academic Press, Jan 2005.
7. "Chief Information Office", Wikipedia, www.wikipedia.org.
8. "Statistics Over IT Projects Failure Rate", IT Cortext, www.it-cortex.com.
9. "Critical Threats", Sue Bushell, *CIO - Australia's Magazine for Information Executives*, IDG Communications, 4/4/05.
10. "Interview With Raymond E. Gogel", Ethan Cohen, Daily Issue Alert, UtiliPoint International, 12/3/04.
11. "Xcel Energy's Chief Information Officer Honored... ", Xcel Energy News Release, www.xcelenergy.com, 1/4/05.
12. "Integration's New Strategy", Christopher Koch, Sep 15, 2005, *CIO Magazine*, pps 42-48.
13. 4DataLink.
14. "Investment Decision Quality at Utilities - An Examination of Downward Trends and Upward Leverage", Rick Dove, Public Utilities Fortnightly, Feb 2006.
15. "Managing the Business Risks of Information Technology Dependencies", NERC Critical Infrastructure Protection Forum, National Electric Reliability Council.

LEVERAGING INFRASTRUCTURE

To review: Credibility is the issue, building trust is the antidote, project predictability is the trick, and infrastructure is the leverage point. Xcel walked that path. Their approach was tailored to fit their situation, however, and is unlikely to work elsewhere as task-by-task steps. The takeaway is that they earned credibility with a focus on infrastructure, in two senses: the Information Infrastructure *and* the IT Infrastructure.

The Information Infrastructure is what users and decision makers relate to. It is the visible value of IT effort. It either provides needed information when and where needed, or it doesn't. Individual and organizational productivity and capability is held hostage by this infrastructure. Provide users with new and valuable information that increases personal productivity and capability, and you get their attention. Display that information consistent with existing mental models, and you get a customer.

The IT Infrastructure is what the IT staff relates to. It is the underlying technology and architecture that defines what is possible and what is not. This is where the reality of integration occurs and where the legacy of bad integration lurks. Not until the past is untangled and the architecture rationalized will predictable projects be possible. Attempting to deliver strategic value at the Information Infrastructure level consistently and continuously without an enabling IT Infrastructure is impossible.

CEO and CIO agree. "The urgency and intractability of this problem is underlined in CIO's [the magazine] 'State of the CIO' survey: Integration has been the number-one technology concern of CIOs since we began doing the survey in 2002. CEOs also put it at the top of their list when we began surveying them in 2004. CEOs' three primary complaints about IT, according to survey after survey—that it is too expensive, too slow and too inflexible—all lead back to integration. In short, the business is tired of waiting for IT to catch up with its demands." [12]

Enterprise IT lives in the realm of what is technically called complex systems – where too many interacting components with too many inter-component interactions defy predictable behavior. Complex systems are insufficiently understood by science as yet, but some engineering approaches are proving useful for IT infrastructure.

Three general techniques are in play:
- EAI – Enterprise Application Integration – Typically employs a common message bus accessible to all applications, and a bi-directional translation-module between the bus and each application typically referred to as an ETL (extract-translate-load). Pro: Custom built to fit requirements, can provide a manageable and predictable environment. Con: Integrator-team dependent, often a grand-plan total-replacement strategy. Can be fairly risky for completion costs and schedules.
- EII – Enterprise Information Integration – Typically employs a special *meta* data base that catalogs and links to the data in all of the other data-bases, and a user interface for seamless navigation through all of the data. Can also be an application integration hub if it provides bi-directional data transfers. Pro: Safely integrates data without unintended operational consequences, new application data bases can be added incrementally and inexpensively. Lowest risk of the three. Con: Capabilities are vendor specific, may not be based on standards.
- SOA – Service Oriented Architecture – Typically a loose collection of independent application components that provide specific services. A user interface translates a user's need into calls on appropriate service components, or negotiates through special broker-modules to assemble a just-in-time collection of components. Pro: Un-coupled components can be changed, augmented, and upgraded transparently. Con: Pioneering exploratory effort as yet. Highest risk of the three.

A manageable infrastructure is one that can readily absorb and support new strategic initiatives affordably, predictably, and quickly.

4DataLink's INFORMATION INFRASTRUCTURE MANAGER

IIM: Information Infrastructure Manager

- Integrates information across corporate and departmental data bases.
- Provides seamless access across *critical* information infrastructure.
- Resolves conflicting data from multiple data bases for accuracy.
- Matches access with authorization, and logs administrative actions for compliance.
- Enables graceful incremental migration.
- Provides platform for IAM.

IAM – Intelligent Active Model

- Translates data into information meaningful to user interests.
- Monitors critical infrastructure for preset conditions.
- Mirrors real-time condition of operations and field-asset status.
- Traces asset-network operational connectivity on demand.
- Simulates what-if futures to facilitate repair and engineering strategy.
- Replays past events for compliance reporting and event diagnosis.

A BENCHMARK INFORMATION INFRASTRUCTURE MANAGER

Of the three general techniques for building a manageable infrastructure, SOA is not a rational contender for a utility as yet. Xcel's Carlson, for instance, says he is excited about the SOA concept, but "We have not made a play there because we don't think we can afford to do it ourselves. Our business-software partners need to drive a collaboration on this. It's a good concept but culturally challenged so far. Business models have to be remade."

Xcel choose the EAI route three years ago in 2002, and just recently, according to Carlson, crossed the threshold of manageability. Vendors and integrators selling EAI solutions will tell you it doesn't have to take that long. And they're right...if you're willing to do a scorched earth implementation. Xcel chose an incremental implementation that minimized risk and disruption, and built trust as it progressed.

If you didn't start three years ago, and you're not comfortable with a scorched earth policy, you might consider some version of an EII approach. EII can deliver an integrated information infrastructure in less than six months with virtually no risk, and it is fully compatible with both EAI and SOA. Compatibility means it will continue to be value added even if one of these other approaches is a longer range strategy.

Though a number of vendors offer general purpose EII, one company employs this technique specifically as an information infrastructure manager for utilities. 4DataLink (4DL)[13], headquartered in the Boston area for the last few years, spent over 10 years evolving this approach in South American deregulated markets first.

The depiction of 4DL's approach on this page encompasses the general purpose IIM integration and transparency concepts shown earlier. Notably differing from general purpose EII, 4DL's approach includes an indigenous focus on the critical information infrastructure along with an intelligent active model (IAM) of operational status. This IAM is an object-based model that provides live mirroring of operational and field-asset status at all levels, all the way down to automated meters. Almost like a GIS that walks and talks. In fact, 4DL's preferred implementation subsumes GIS functionality internally to the IAM. The reader is referred to another benchmarking example[14] for a deeper discussion of IAM as an asset management and investment decision tool. Here the focus is on management of the information infrastructure.

4DL calls their information infrastructure manager NIM (network information manager), in reference to its IAM field-asset-network orientation. NIM is nevertheless not limited in content to network asset information, and can be used to provide integrated views of virtually anything available in standards-based data bases.

Of the key points itemized in the side bar, graceful incremental migration is a prime objective of infrastructure management. Ideally incremental migration transforms an IT legacy environment into an agile yet fully integrated infrastructure one small risk-free step at a time. Or at least in annually-affordable increments. The transformation neither disrupts ongoing business-as-usual, nor introduces unintended consequences along the way. The transformation proceeds in a highest-returns-first sequence, rather than needing lengthy investment in new IT infrastructure before anything materializes at the information infrastructure level. Finally, once initial transformation is completed, the result facilitates continuous transformation, for that is the reality of the need.

Ideally, at best, generally means not quite attainable. Not so in this case. The very nature of an EII approach, done right, is non disruptive, because nothing is disturbed or changed. Read-only links from the IIM are extended into the data bases of interest. Nothing that currently happens is stopped. Data bases can be added one at a time whenever the next increment of integration is desired. Every added database provides added information access, immediately and seamlessly to the user.
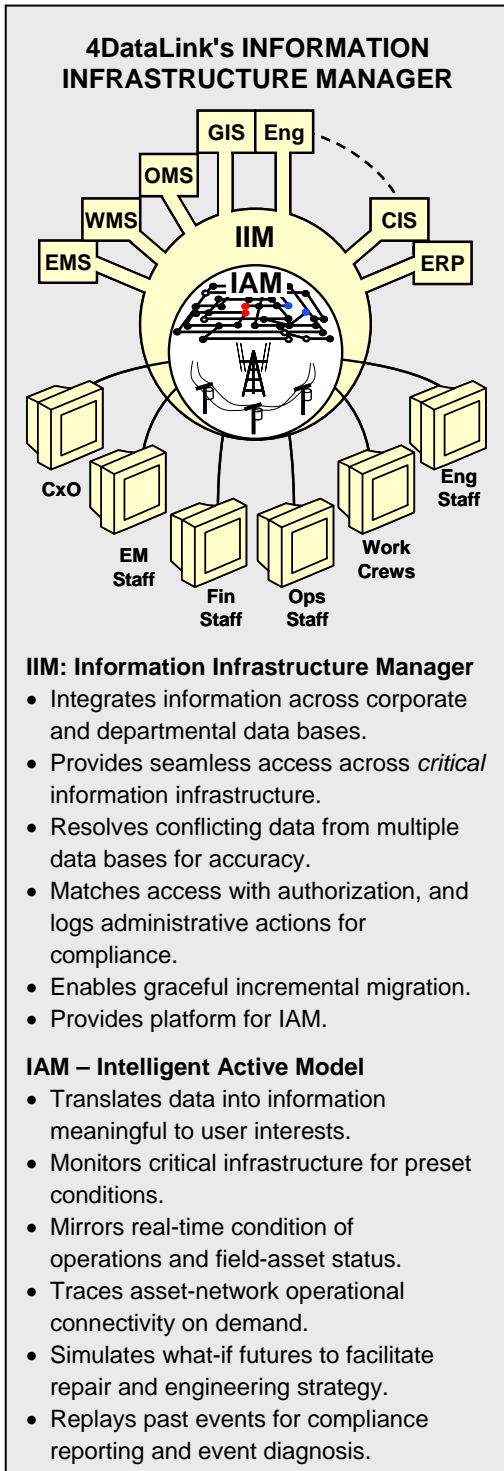
HOW'D WE GET HERE?

(*Integration's New Strategy* - excerpts[12])

"Technical limitations and time pressures often made integration a haphazard affair. Rushing to meet deadlines, developers cobbled together direct links (point-to-point integration) to share data and business logic among applications. While that kind of integration is quick and relatively simple, over time it has crippled the health and flexibility of most IT architectures by creating a cobweb of hundreds, even thousands, of brittle linkages that have to be torn apart and reassembled every time one of the applications changes.

"All those links, built up over decades, have created a crisis that goes far beyond IT. The rise of the Internet has made businesses completely dependent on IT to add new capabilities. The foundations of those new capabilities often lie buried inside old systems that were never designed to communicate with one another. Adapting those systems to communicate can take so long that entire generations of business opportunities (new products, alliances, mergers and acquisitions) can grow old while IT fiddles with the wiring. Unable to explain the complexity of their problem, CIOs inevitably wind up on the defensive, with only the most patient, tech-savvy CEOs able to commiserate.

AUTHOR Rick Dove is the Agility Practice Leader for UtiliPoint International and Chairman of Paradigm Shift International. His monthly column on Utility Agility reaches over 250,000 subscribers through five Energy and Utility sector newsletters. He co-led the seminal effort at Lehigh University that defined agility in the early nineties as the survival need of the new millennium. His recent books include *Response Ability: The Language, Structure, and Culture of The Agile Enterprise* and *Value Propositioning – Perception and Misperception in Decision Making*. Email dove@parshift.com.

CONCLUSION

NERC (North American Reliability Council) says it well: "In addition to helping electric utilities collect field data and issue the control commands needed to reliably generate, transmit, and distribute electricity, computer systems increasingly are being used to enter new markets, achieve business operating efficiencies, and communicate with customers and business partners. Therefore, the reliability and security of these information systems are more important to electric utilities' competitive positions than ever before. Chief information officers (CIO) are the management officials responsible for procuring and managing mission critical information systems." [15]

The typical CIO grew up on the technical side and developed a great sense of confidence in technical understandings and capabilities applied in service to the company. Before that technical hat gets knocked off or taken off, everybody should realize that governance and goal alignment are really just aspects of sound Systems Engineering principles, but now with the enterprise being the system. All the same engineering analysis and design disciplines apply. The principle difference being that technical requirements and specifications are driven by broader business requirements and specifications, as opposed to departmental or user requirements.

In review, three related imperatives were cited:
1. Leverage IT for business strategy.
2. Install IT expertise in corporate decision-making bodies.
3. Instill trust in IT ability to deliver strategic capability

These three imperatives are related in that the first will not happen without the second, and the second will not happen without the third. There are no short cuts. For most, the path must start at the third imperative. For some, the third and even the second may have already occurred, and only the decision to leverage IT strategically remains. For a few, an almost simultaneous attack on all three is possible, with Xcel as the poster case.

Too many *intelligent* solutions to the integration problem are major, throw-it-all-out, start-over-again projects. These can make a lot of sense on paper, but too often stumble badly and publicly during implementation. Though project cost overruns in the tens of millions are not uncommon, bigger costs are hidden in business disruption, completion delay, unrealized expectations, and postponed opportunity.

Big projects are not the only ones that exhibit these risks. Another common approach is what could be called islands of integration. Here the strategy is to replace some number of independent legacy applications with an integrated suite. They promise smaller cost and less total business risk – but still face the unpredictable results of changing entrenched and familiar ways of conducting business.

It doesn't have to be that way. Xcel Energy made the EAI approach work, and 4DataLink stands as a benchmark for the EII approach.

What will it be: Career is Over...or...Critical Infrastructure Officer?