

November 19, 2004

## Enterprise Agility—Is Risk Management

By Rick Dove

Consultant, UtiliPoint International, [www.utilipoint.com](http://www.utilipoint.com), [dove@utilipoint.com](mailto:dove@utilipoint.com)  
Chairman, Paradigm Shift International, [www.parshift.com](http://www.parshift.com), [dove@parshift.com](mailto:dove@parshift.com)

Plain and simple, the value proposition for enterprise agility is rooted firmly in risk management. The purpose of agility is to maintain both reactive and proactive response options in the face of uncertainty.

We explore the value proposition in terms of *enterprise risk management* (ERM)—with an important twist. Current ERM extends standard risk management strategies to a larger set of business risks, notably those of operations and project decisions—but generally focused on risk analysis as it affects available choices. Half the story. The other half of risk *management* is to proactively increase the choice options with lower risk alternatives. Precisely the purpose of agility.

*CFO Magazine*<sup>1</sup>, cited Seminole Electric Cooperative as an early adopter of ERM. "We needed to create a broad list of risks facing the company, not just the risks that executive staff had cited, but risks perceived by executives across all corporate lines," says John Geeraerts, Seminole's financial services VP. They boiled an initial 60 defined risks down to a forced top five. "Number one was electrical-generation capacity—the loss of a generating plant due to an unplanned or forced outage. The company evaluated factors such as tornadoes and terrorist incidents that would disrupt power supply or cause a unit to go down. The second-highest risk was loss of market, a concern given Seminole's status as a cooperative. [The next three were] the need to have an optimum mix of power resources to serve customers, fuel price volatility, and regulatory risks, such as the impact of potentially stricter environmental standards." Mitigation was then considered. "For fuel price volatility, the option is a fuel hedging program; for the loss of power lines, the option is insurance; for the risk of terrorism, the option is elevating our security officer to senior staff level," notes Geeraerts." Given the focus on security today, I expect this was more than a simple title change.

Economist Frank J. Bernhard, interviewed by *CSO* (Chief Security Officer) *Magazine* describes the difference between economic risk and business risk: "Economic risk can involve things like supply-and-demand conditions or geopolitical events. Business risk extends to the outcome of not getting investors. Or losing customers. Or the failure of a product or service<sup>2</sup>."

*CIO Magazine*<sup>3</sup> ran an excellent article on ERM—as a business process, not as a buzzword software package. Many, but not all, of the values and examples they cite are related to making better corporate and departmental IT project decisions. But then, decisions about IT infrastructure and business process support affect the entire organization, with major operational impact—especially if they fail to perform as and when expected.

Scott Berinato, writing in *CIO* on ERM and its relationship to IT, says: "The reason these risks are suddenly being accounted for is because the systems are becoming ever more critical. Today, one bad IT decision can severely hamper—or even take down—a company. "

### The ERM-Agility Connection Is Made

Rockwell-Collins, an aerospace company, is cited by *CIO Magazine* as an early adopter of ERM decision-making procedures. According to the magazine, even though they lost 20% of their revenue generation capabilities as a result of 9/11, yet ... "The company has turned a profit every single quarter after 9/11. And in January 2004, *Forbes* called Rockwell Collins the best-managed aerospace firm in America... 'We're able to react [to that complex environment] because of our risk mind-set,' says [CIO John-Paul] Besong. 'With what happened to us, our *agility* was called to task. And we had the risk methodology in place to handle it.'" When I worked with them during the nineties we didn't associate our agility work with enterprise risk management. They have clearly made the connection since.

Energy sourcing, disaster planning, customer credit, cash flow protection, and security are commonly practiced forms of risk management. Less common are the potential impacts of new business processes, IT infrastructure and applications, outsourcing, and growing electronic automation and networking, to name some.

Agility expands the options for response when unpredictable events occur; by reducing the cost of response, the time of response, the predictability of response, and the range of response. It does this principally through infrastructure, systems, and business processes that are structured for *response ability*—explored later in this continuing series. And, as will be shown, it is not necessary to reengineer massively or disruptively to gain benefits—because the very nature of agile structuring supports graceful, incremental migration. Agility is, after all, about effective change management.

## Security Risk Management

Energy sourcing aside, the biggest risk management activity is associated with security, as every employee is involved to some extent. The Department of Homeland Security, spurred by 9/11, looks at the Energy and Utility sector as part of the critical national infrastructure, and is concerned about any security breach that can affect service, not just acts of terror. Staggering increases in email and Internet born worms and viruses have elevated the focus as well. Now organized identity theft from customer databases has escalated, with liability on the company that owns the database. And of course now Sarbanes-Oxley, with its various vagaries about what will really be audited and who will really be held responsible in post-event auditing. Security technology and its deployment is clearly not keeping up with the escalation of threat and exploitation. Waiting for magically superior and affordable technical solutions may well be one of those Sarbanes-Oxley gotchas—especially if internal security strategy, composed of policy, procedure, and practice, is found wanting.

Security strategy is a business process, distributed as it may be. The technology portion of this strategy is at the mercy of policy, procedure, and practice—which are people-based systems. Peopled systems in business environments are subject to human behaviors and organizational behaviors, neither of which is effectively constrained by compliance to policy and procedure, or consistency of practice. Both people and organizations can be whimsical, willful, vengeful, criminal, forgetful, distracted, expedient, unknowing, and otherwise act outside of what they *ought* to do.

Security risk reduction is not insured by technology; it is only partially enabled. Policy, procedure, and practice reign—precisely where reality bites. Even *good* policy, procedure, and practice, written in the corporate book, runs up against the realities of organizational, human, and environmental behaviors. Let's look at reality.

### Reality Issues Affecting Security Strategy

The *Enterprise Risk Management—Integrated Framework*<sup>4</sup> from COSO (Committee of Sponsoring Organizations of the Treadway Commission) contains the following caveat: "While enterprise risk management provides important benefits, limitations exist. ... limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives." These reality factors hurt precisely because they are insufficiently recognized when would-be-agile system and process requirements are established. If they are understood for what they are, and addressed with respect, they can be greatly mitigated and sometimes precluded.

Seven compromising areas of uncontrollable behavior have been identified by The Agile Security Forum<sup>5</sup> as a Reality-Issues Framework. They basically stem from forces so natural and dominant that rules and penalties cannot alter their influence effectively. Keeping the Forum's same seven reality-factor areas, I've couched the framework in Utility specific issues here:

**1 - Increasing pace of new-technology** - Upgrading and replacing the IT infrastructure and applications at Utilities is necessary for acceptable-practice parity, and increasingly demanded by regulatory bodies for cost containment and improved customer service. Yet we see new vulnerabilities in legacy systems still being discovered and exploited. Newer technology brings new and different vulnerabilities—that's what new technology does. Decreasing technology life cycles and increasing technology variety amplifies the situation. The historical record is undeniable.

**2 - Increasing complexity of systems** - The march is on in the Utility sector for better integration of systems that support operations. Likewise for more network reach: network node count is growing and networks are interconnecting on larger scales with more sophistication. The complexity of software systems alone have long passed our abilities for analytical predictability. Networked business operations overlaid with a networked global community have added new combinatorics and complexity. We cannot predict with any assurance at all the results of a system change, no matter how small. Companies merge and race to interconnect; they upgrade, replace, and add new technology continuously; competition and opportunity drives evolving customer and supplier interfaces; and business operations are fragmenting and distributing business processes globally. The law of unintended consequences expresses itself naturally in complex systems under change—and is irrefutable.

**3 - Creeping agile-business practices** - Whether a Utility considers itself agile or not, it cannot avoid outsourcing imperatives for IT, billing, call-centers, and other business processes; nor electronic response-enhancing interconnects with energy suppliers, energy brokers, co-generators, demand-response customers, automated meter reading, SCADA (supervisory control and data acquisition) field assets, and wireless-linked field personnel. These alone don't constitute an agile enterprise strategy, but they are, nevertheless, part of today's business strategy, driven by needs for better spot-responsiveness. You can't escape it, yet each move brings new and greater security vulnerability.

**4 - Increasing globalization** - Not a regional game anymore, Utilities are outsourcing business processes off-shore, buying energy off-shore, and merging multi-nationally. Globalization brings more interconnected business operations—and with it, different ethics, different values, different perceptions of risk, different interconnected technology, and different nation-state interests. This means more sources of vulnerability, at the least; but economics and growth-pursuits will not be denied, in any event.

**5 - Natural human behavior** - Security impacts individual productivity and goal priorities. In so doing, it is often ignored or circumvented in actual daily decision making and practice. We humans are wired the way we are. We make decisions every day, all day long—as IT system administrators, as policy makers, as procedure followers, as users in all departments at all levels, and even as disgruntled employees. Our perceptions of what is right or expedient are biased by hopes and expectations, as well as the latest alligator that influences our immediate priorities and values. We are the source of human error. On top of all of this, we are whimsical. Rules are made to be broken, and they are, in any event, made for others who are less wise than we. Murphy's law is not a joke. And all of this just deals with people who are trying to do the right thing. But the perverse also exist. Optimal by-the-book actions and decisions do not and will not prevail anywhere.

**6 - Natural organization behavior** - Organizations are aggregates of natural human behaviors. On top of that, they have a collective mind of their own. Security impacts organizational productivity and goal priorities. In so doing, strategy is typically designed and deployed inadequately. Among decision makers there are inherent conflicts which remain unresolved, power politics and positions that exert biased influence, and competing interests for limited resources. Research shows that decision makers are ruled first by individual rather than group objectives, mitigate conflict by compromising greater values to achieve consensus, seek solutions that are acceptable rather than optimal, and vary risk-seeking and risk-averse behavior with economic conditions. Shown in my book on decision making reality<sup>6</sup>, neither local optimality (within a company or department) nor global valuation (for the greater community or the company) are standard characteristics of organizational decision making and behavior. It won't be changed—it's the nature of the beast.

**7 - An agile attack community** - Ashby's *Law of Requisite Variety* demands that a response system be at least as agile as the environment that creates the need for response. Scourge technology has advanced to the point where we now refer to zero-hour attacks for the time it takes from release to massive Internet presence. Meanwhile the increasing sophistication of attack development and tool technologies has already reduced the time between vulnerability discovery and exploitation to mere days. Infected machines and public distribution of attack tools mobilizes massive resources quickly. Large scale grass-roots retaliation occurs when independent personal reactions weigh-in patriotically on national disputes or indignantly target companies on the wrong side of a thought-community. Amateur and professional alike benefit from this loosely-connected global collaboration of independent resources. These developments are less than three years old—more are on their way. As more value is made more available for theft and damage, the targets of opportunity become irresistible.

Don't hear all of that as gloom and doom. It is just a dose of reality. There are ways to reduce risk even as these reality forces increase the pressure—but only if reality is confronted for what it is, and the mitigation strategy is at least as agile as the forces it faces. More will be said about how this is done at another time.

**How bad and where does reality bite now?** You've read this far, so maybe you're interested enough for some quick poll involvement. Go to [www.AgileSecurityForum.com/Surveys/SurveyEss066.htm](http://www.AgileSecurityForum.com/Surveys/SurveyEss066.htm) to answer eleven fast check-box questions. Results will be published when 100 responses are received...and likely influence future topic coverage.

----- Send comments to [dove@parshift.com](mailto:dove@parshift.com). ----References:

- CFO Magazine, June 2003: <http://www.cfo.com/article.cfm/3009436>
- CSO Magazine, December 2002: [www.csoonline.com/read/120902/viewpoint.html](http://www.csoonline.com/read/120902/viewpoint.html)
- CIO Magazine, November 2004: [www.cio.com/archive/110104/risk.html](http://www.cio.com/archive/110104/risk.html)
- COSO's *Enterprise Risk Management—Integrated Framework*, [www.coso.org](http://www.coso.org)
- The Agile Security Forum, [www.AgileSecurityForum.com](http://www.AgileSecurityForum.com)
- Perception and misperception in decision making: [www.parshift.com/ValueProp](http://www.parshift.com/ValueProp)
- [www.parshift.com](http://www.parshift.com) on Agility organizational aspects
- UtiliPoint International's IssueAlert® archives at [www.UtiliPoint.com](http://www.UtiliPoint.com)

*Rick Dove is a recognized thought leader and change agent for agile enterprise and agile systems of all kinds. He co- led the seminal effort that defined agility in the early nineties as the survival need of the new millennium. He subsequently organized and led the Agility Forum's industry-collaborative work that identified and defined concepts and principles for achieving agility in all aspects of enterprise. He's developed and managed deployment of agile enterprise business processes and IT infrastructure. He is a prolific writer and frequent speaker on the subject, and the author of Response Ability: The Language, Structure, and Culture of The Agile Enterprise (Wiley 2001) and Value Propositioning - Perception and Misperception in Decision Making (Iceni Books 2005).*