From: http://www.homelandsecurity.org/journal/articles/beartrap.htm

Homeland Defense: Avoiding the Bear Trap

Mark Lefcowitz, managing and principal partner of Mark Lefcowitz, LLC

June 2002

Mark Lefcowitz[1] is an expert in information technology management processes and facilitated processes. He has over 25 years' experience in information systems, consulting, and management for private and government clients. In the past, he was involved in dispute resolution, having served as a non-attorney member of the Pennsylvania Bar Association's Committee on Dispute Resolution. He was one of the founding members of the Pittsburgh chapter of the Society for Professionals in Dispute Resolution and served as its first president. He is the developer of Facilitated Rapid Development Processes,SM author of several books and articles on facilitated processes, and a guest speaker on facilitated process issues. He is the publisher of the *Homeland Security Business Process Reengineering Report.*

There were many twists, turns, and subplots in the demise of the Soviet Union from the late 1970s to its formal dissolution in 1991. Most analysts agree, however, that poor budget choice and planning—both domestically and militarily—by the Politburo were substantially driven by an attempt to keep pace with the United States' military and technological advances. The Soviet infrastructure, its decision-making style, and its implementation process all failed to measure up to the challenge. Ultimately, the Soviets spent themselves into bankruptcy.

Forcing any group to spend huge amounts of capital and human resources on project choices that they would rather avoid is a "bear trap," a maneuver long practiced by legal and military strategists. Since 11 September 2001, the United States has been in real danger of walking down the same path.

The federal government of the United States is spending approximately $1 billion daily on its attempt to eradicate al-Qaeda leadership and its followers. In all likelihood, the attempt will never be completely successful. Discrepancies in wealth and culture are now more apparent. The unintended consequences of technology are making themselves felt throughout the world. New leaders and new groups will emerge. The ability of relatively small terrorist groups to recruit and convert new soldiers for a long, drawn-out war of attrition against the United States and its allies will continue. Pandora's box has long since been opened. It is clear that the possibilities for sustained, low-tech attacks, supported by high-technology access to

information, upon vulnerable and interdependent segments of our society are too tempting. When God—or a moral equivalent—is on your side, all acts are justified.

How can we, forced to fight foes bent on our destruction, avoid spending ourselves into bankruptcy? There are no simple answers, but part of the answer is to be smarter about using the resources we do spend.

As the numerous homeland defense initiatives and projects roll out over the coming months and years, information technology (IT) will be an essential element in our fight for survival. It is all too tempting to throw caution to the wind and throw money at the expanded role that IT will play in the coming decades.

Unfortunately, the IT success record of accomplishment for projects that meet their cost, schedule, and performance goals is abysmal. Several independent studies suggest that the IT failure rate over the past decade may be as high as 80 or 85 percent. The Standish Group's biannual "Chaos Report," an ongoing study based (to date) on surveys of more than 32,000 projects, estimates the financial damage to the United States at about $100 billion annually. This estimate remains substantially the same in the soon-to-be-published 2002 "Chaos Report." From other sources,[2] it is clear that almost all of this waste can be directly attributed to numerous management issues and the lack of adequate process implementation. With the increased spending that homeland defense will require on governmental and nongovernmental IT, it appears that many times this amount will be wasted in the future unless something radical is done.

A case in point illustrates part of the problem:

Several years ago the Bureau of Alcohol, Tobacco, and Firearms (ATF) approached the U.S. Customs Service for access to data stored in its system. The Department of the Treasury manages both agencies. To the uninitiated, it would seem that the impetus for teamwork and cooperation would abound. Sadly, this was not the case. After a great deal of onerous and contentious negotiations, Customs finally granted permission to its sister agency. A provision of the interagency agreement was that Customs would neither change the structure of its existing database nor be forced to facilitate in any way the implementation of the necessary data interface with ATF. In effect, Customs told ATF to go pound sand and wasted precious time and resources in the process.

Similar stories are abundantly available concerning other agencies and are well known to political observers. However, this story does illustrate one of the most serious weaknesses of the United States' ability to fight terrorism: To coordinate information collected by numerous, independent, large organizations requires a great deal of cooperation and teamwork. Within the context of homeland security, the necessary effort to coordinate the multiple levels of federal, state, and municipal governmental efforts, as well as private and volunteer efforts, only further complicates this veritable Gordian knot.

But what do you do if you have a room full of 500-pound gorillas, all attempting to sit wherever they want? The answer is to go get a 1,300-pound gorilla and a process to allow the others to work cooperatively.

Among the techniques available to IT managers is the facilitated process, a requirements- gathering and risk-assessment methodology initiated at the front end of a project. Facilitated processes are no panacea, but are considered by many, including the Government Accounting Office, to be a “best practice.” Facilitated processes are a concentrated effort by project stakeholders (led by a neutral third party—a facilitation leader) to identify and work out a common understanding of the project requirements. Through a step-by-step process lasting 5 to 6 weeks, the stakeholders come to understand their own and each other’s role and responsibilities within the context of the overall project. The effect each stakeholder has on the work product and performance of others is mapped out. Risks and mitigation strategies are fleshed out; these take into account technical feasibility and mission-critical business requirements.

Such a methodology requires active executive buy-in and sponsorship, rather than a mere executive-level “Go forth and do good things” decree. Facilitated processes, therefore, are not always a comfortable fit for the traditional top-down management style of the mainstream bureaucrats or their corporate counterparts. It requires that real decisionmaking be truly shared and that a broader, project-based team effort be mounted—something senior managers are often reluctant to do.

Many managers are under the misapprehension that the role of management is to direct and organize personnel, to budget, or to assure production and quality. In fact, in the last analysis, all management has only one role: the operation of process. How well we manage the process in the future will determine whether we survive the further onslaught of terrorist forces.

On the federal side, there are areas of concern and of hope.

In his testimony before the Senate Committee on Governmental Affairs, on 31 October 2001, [3] the Government Accounting Office’s Director of Defense Capabilities and Management, Raymond J. Decker, suggested a risk-management approach to homeland security. He highlighted threat assessment, vulnerability assessment, and criticality assessment as three pillars (literally presented to the Committee as a graphic of a pseudo-Greek Revival structure) on which would rest the entire homeland security approach and, from that, a homeland security strategy. Unfortunately, Decker’s presentation neglected to provide any detail about the base of this homeland security structure in his analogy. This focus, lacking the necessary vision details of process from which implementation efforts will emerge, illustrates the general “five-alarm fire” approach one has come to expect from large organizations and joint organization planning.

On a somewhat brighter note, the little-known but highly influential Chief Information Officers Council has struggled mightily on these issues, even before the tragic events of 11 September. A series of interviews with some of the CIO Council’s members and other government decision makers in the area of homeland security make clear that physical system security will be the most immediate homeland security concern. Behind the scenes, efforts to come to some common understandings about best practices and process concerns in this new environment are in their initial stage. The CIO Council has an active Best Practices Subcommittee that is doggedly attempting to get its hands around an immense subject with a very small work force to accomplish the task.

Interviews with a high-level source at the Office of Homeland Security indicate that process needs are very much in the forefront of the Administration's concerns. The Office of Homeland Security plans to push for the inclusion of facilitated processes on the front end of many interagency efforts, using either consultants or neutrals from nonparticipating agencies. Administration plans also include the establishment of an interagency steering committee that will have many of the same functions as the Department of Defense Joint Requirements Oversight Council, the mission of which is to ensure that all DoD projects are compatible with the department's requirement for joint mission capability. The final form this interagency steering committee will take, as well as its mandate and scope of operation, is still in question. However, it's clearly a step in the right direction.

Congress has begun hearings on many of these issues. The hearings will almost certainly lead to actual legislation. It is too early to gauge its final form or focus. One can only pray that it does not cause the usual unintended consequences of unfunded mandates and further complicate an already complex problem.

According to Robert S. Byrd (D-WV), chairman of the powerful Senate Appropriations Committee, "We must rise above the usual bureaucratic turf battles; determine how to address this problem which crosses the jurisdictions of departments and agencies; build a new flexibility into our solidified government structures; and think about federal, state and local relations in a new way."

One does not doubt that the Senator's heart is in the right place, despite his very public call for Homeland Security Director Tom Ridge to testify before Congress. One can only wonder whether Byrd's call to end turf battles includes both sides of the aisle in Congress.

Even among those who should understand the limitations of technology best, there seems to be a reckless disregard for the consequences of failing to deal with these very serious issues. For example, Larry Ellison, founder and CEO of Oracle Corporation, has offered to provide the software to run a federal-wide ID system at no cost to the taxpayers. Both Oracle and a high-level source at the Office of Homeland Security have independently confirmed this.

Let us presume, contrary to much sniping by Ellison's critics, that his motives are purely patriotic. One can only wonder why a respected industrial leader of Ellison's stature could possibly forget the computer adage "garbage in, garbage out"; the most modern and up-to-date system that fails to do what you wish will be nothing more useful than a very large paperweight. Many would feel more comfortable if Ellison would instead assist in setting a process agenda rather than a technology-specific agenda. Let me add that he is by no means alone in his approach. Many other captains of technology appear to be elbowing for a place at the homeland security trough. This nation does not need to invest its government employees' time and effort in a blind technology-specific solution any more than it needs to put its military personnel to work painting all its military equipment camouflage purple. Whether someone happens to make purple paint and is willing to give it away is really beside the point.

At this moment, nine months after the attacks of 11 September 2001, the homeland security effort is little more than a great deal of effort with many willing but uncoordinated participants. There is no doubt that technology will appropriately play

a central role in the defense of our nation; however, failure to improve our ability to organize and efficiently complete large, complex tasks, such as those demanded for homeland security, will have disastrous effects. All we are likely to have in the end is a very large paperweight at the bottom of a very deep bear trap. Only time will tell whether our efforts are to be successful and whether we will be perceptive enough to avoid it.

---

1. Mark Lefcowitz may be reached at (703) 719-7198 or mlefcowitz@email.com.

2. For example, John Bergey, Dennis Smith, Scott Tilley, Nelson Weiderman, and Steven Woods, "Why Reengineering Projects Fail," Carnegie Mellon University (Technical Report CMU/SEI-99-TR-010, RSC-99-TR-010), April 1999; www.sei.cmu.edu/publications/documents/99.reports/99tr010/99tr010abstract.html.

3. Raymond J.Decker, "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," U.S. General Accounting Office (GAO-02-208T), 31 October 2001.