

EDITORIAL – MAY 2007

Transparency vs. Security! A growing Dilemma for Project Managers & Organizations

By David L. Pells

For the last few years, I have been on the “more transparency is good for project management” band wagon. It has seemed to me that project stakeholders should be better served when project plans and progress are more visible, where project risks, project performance and return on investment can be observed and monitored. This, it seemed to me, was the more honest and professional approach. And I was convinced that more transparency would improve project planning, management and performance. I think that might still be true.

However, in this ever more unstable and insecure world, the issue of security must now be considered more seriously than ever before. In fact, I think this is a new major issue, and dilemma, in the world of professional project management. It is an issue that should now be addressed on every project and included in every project risk management plan, with appropriate activities planned and budgeted to protect project and organizational assets, data, facilities and people.

In this editorial, I attempt to identify some of the issues to be considered in the trade-off between more transparency on programs and projects on the one hand, and on the other hand, adequate security to protect the projects, people and organizations involved. This is an area that now deserves more research and discussion. It might also be an area where new techniques or tools may be needed.

The Need for More Transparency

Since the corporate scandals highlighted by the Enron collapse, and with the passing of the Sarbanes Oxley (SOX) legislation affecting public corporations in the United States, there has been an increasing call for more transparency in financial reporting. The increased attention on and drive for more transparency has affected many organizations in the USA, both public and private, and many program and project managers. Is the demand for more transparency justified? In my opinion, more transparency on projects and related to project management is promoted for some or all of the following reasons:

- **To ensure financial accountability** – more visibility of financial plans and performance allows stakeholders to see where the money is going.
- **To ensure and demonstrate that standards are met** – Are legal, financial, professional and other standards being met on the project? Customers,

executive sponsors, project team members, and suppliers might care a great deal or need to know.

- **To ensure and demonstrate that projects are adequately planned** – often the only way to know if a project has been planned is to see the plan. Making project plans visible and public can ensure that projects are adequately planned; this has become especially important for programs and projects financed with public funds.
- **To reduce risks** – in theory, greater visibility of project plans, performance reports and other information should reduce risks. Uncertainties can be identified by more stakeholders, better planning should result, performance should improve. This may be more perception than reality, depending on the quality of the people and project management processes used.

In general, the argument is that more transparency should ensure better project management, improve financial accountability, and force executives and organizations to make better decisions – when they are more visible and individuals can be held accountable.

The Need for More Security

Now comes today's world of global terrorism, cyber-crime, identity theft, sabotage, spam and other dangerous actions by dangerous people. As the world has become more interconnected, through global communications and the worldwide web, the risks from these dangers have increased. Now it seems that additional security is needed on projects today for some of the following reasons:

- **To protect citizens and society** – every program or project associated with public infrastructure or services must be reviewed and protected against terrorism, both locally and globally. This obviously includes projects associated with transportation facilities like airports, seaports, and rail facilities, in every city, state and nation. It also includes public utilities, healthcare and many other programs and facilities.
- **To protect organizational assets** – projects that involve or might reveal valuable assets (electronic, intellectual, physical) should be reviewed against dangers and risks from competitors, criminals, hackers or saboteurs.
- **To protect people from cyber risks** – care must now be taken with regard to revealing individual names and email addresses, for project team members, executives, customers, suppliers or other participants. Personal information on websites and in reports might need to be limited.

- **To protect project data** – this is an issue for every project risk management plan. Extra steps might need to be taken to ensure backup and/or protection of project or organizational data. System security must ensure that valuable project data is not lost, damaged or destroyed by cyber-criminals or errors.
- **To protect systems and technologies** – this calls for more serious and robust system security for all projects and organizations, to protect valuable project and organizational systems, tools and data from unwelcome or dangerous access or visibility.

In many cases, the need for additional security will require new policies and procedures. All project and program managers, however, should consider and address these risks in project risk management plans, security strategies, project plans, and in budgets and schedules.

The Dilemma for Project Managers

The dilemma facing project and program managers, and executives in public entities, is related to what project information to make public and how to do it. In response to calls for more transparency by investors, shareholders and politicians, some organizations have been leaning towards more disclosure of project plans and information. This is especially true for public agencies, where taxpayers and special interest groups lobby for access to information. In many cases, public agencies are legally required to disclose project plans, progress reports and other information (for example, organization charts, contact information, personal data, etc.)

How does a program or project manager or responsible executive balance the requirements for more transparency with increasing risks and security concerns?

Some Considerations and Options

So what is the solution to these questions? Here are some possible steps:

- **Identify, review and understand current transparency and security issues** – someone in every organization should identify and review the electronic and physical doors and windows into the organization. What information is currently made public, visible or accessible, especially on websites or via email? Are there any open lines to critical databases or systems? Is any project information subject to unwanted access or manipulation?
- **Update security policies and procedures** – policies, procedures and practices related to security should be reviewed and updated, as needed, to ensure that assets, data, organizations and people are safe and protected throughout the life of the program or project.

- **Establish policies and procedures related to project management** – those policies and procedures can be made public, or more visible, reducing the need to reveal actual project plans and information.
- **Improve project risk management** – a risk management plan should be prepared for every project. All risk management plans should now address transparency and security issues, to protect the project and project stakeholders. Risk management becomes more critical in a dangerous world.
- **Publish summary information only** – summary information should not contain sensitive data or information that can affect security. Titles can be used instead of individual names. Detailed information can be provided to project sponsors, team members, customers and others internally or in secure ways. Everything does not need to be posted on websites.
- **Establish visible project governance** – governance includes oversight and accountability. For large projects, independent oversight committees or reviews can be used. For smaller or more proprietary projects, a Project Management Office or consultant might be used. Project governance activities, committees, and policies can be visible, while project data and information remain protected and secure.

More research needed on these issues

Additional research is needed on these topics. In what industries should project data and information be subject to more or less transparency or security? What are some experiences or practices by large organizations in this area, in both public and private sectors? What are some solutions? How should security risks be planned and managed? How can they be quantified? I hope this discussion has been useful – please let me know your comments.

Good luck on your projects!

David L. Pells

Managing Editor

PM World Today

www.pmworldtoday.net

www.pmforum.org



David L. Pells
Managing Editor PM World Today



David L. Pells is the Managing Editor of PM World Today and of www.pmforum.org one of the world's leading online sources of project management news and information. David is an internationally recognized leader in the field of professional project management, with over thirty years' experience in project management related activities and positions. His professional experience includes a wide variety of programs and projects, including engineering, construction, transit, defense and high technology, and project sizes ranging from several thousand to ten billion dollars. He served on the board of directors of the Project Management Institute (PMI®) twice, and was awarded PMI's Person of the Year award in 1998 and Fellow Award in 1999. David can be reached via email at: editor@pmforum.org