Lessons of Technical Disasters and Project Management

Brenda McAleer
mcaleer@maine.edu

Joseph S. Szakas
szakas@maine.edu

University of Maine at Augusta
Augusta, ME 04330

Abstract

Design and implementation of IT projects continue to be problematic as the majority of projects fail, or are challenged by budget and schedule overruns. This problem is compounded by the fact that today's projects are increasingly complex. This paper discusses the problems of managing successfully implemented projects. By presenting students with the lessons of technological disasters, i.e. successful projects that then fail, a revised Project Management course could better prepare Computer Information Systems (CIS) students to understand the risks of integrated and complex working systems in today's world.

Keywords: Project Management, risk, complacency, technological disaster

1. INTRODUCTION

Problems continue to be documented in the analysis, design, and successful implementation of IT projects. That most projects fail in the IT area continues to be an ongoing area of investigation. Information technology projects are particularly vulnerable because they require significant organizational change if they are to be implemented well (Glaser, 2005). It shouldn't come as any surprise that IT projects are increasing in scope and complexity, making success difficult to achieve (Reich & Sauer, 2010). The CHAOS Report, originally published in 1994, studied more than 8,300 software implementations, and found that only 31 percent deliver 100 percent of their expected value, were on-time, and on-budget; 16% were abandoned or cancelled, and 51% were labeled "challenged" (Tichy & Bascom, 2008). This statistic has not effectively changed since 1994 (Stanleigh, 2006). In a study of 176 projects conducting in 1997 by KPMG, IT project failure was considered rampant. Among the projects analyzed, 61 percent failed to meet business-sponsor (client) expectations, 75 percent missed scheduled completion dates by 30 percent or more, and 51 percent substantially exceeded their budgets (Tichy & Bascom, 2008). Price Waterhouse Coopers found only a handful of projects initiated ever achieve success. Only 2.5 per cent of global businesses achieve 100 per cent project success (Stanleigh, 2006). Twelve percent of IT project are cancelled before implementation, 33 percent of IT projects overrun their schedules by an average of 71%, and 1/3 of the IT projects undertaken overrun their budgets by 41 percent (Cramm, 2010).

Even with all the failure that abounds, some projects are in fact successfully implemented. But, projects that successfully complete are faced with a myriad of pitfalls and vulnerabilities leading to failure. When failure happens to a working system, the effects can often be magnified and results may in fact be catastrophic. So, it is this concern of failures of working systems and how the lessons of past technological disasters can be conveyed in the IS 2010 curriculum model to improve future Project Management. The Project Management course would be an appropriate place to address these concerns, provide students exposure to fail-safe system methodologies such as model-based failure management (Ermagan, Krueger, Menarini, Mizutani, Oguchi, & Weir, 2007) and safety-critical systems (Medikonda & Panchumarthy, 2009), and show the consequences if students do not heed these lessons to properly manage implemented systems. We will discuss Project Management, what is taught in a Project Management course as discussed in the IS 2010 curriculum, lessons learned from technical disasters after Project Management implementation, technological risk, and the role of complacency issues in project failure.

2. BACKGROUND

Project Management is half of a partnership with systems analysis in the IT project effort and is the focus of this paper. To be clear, there is often no systems analyst or project manager overseeing a successfully implemented and running system. One of the paper's goals is to better state the goals of Project Management and, more specifically, within a Project Management course. As defined in current Project Management texts, a project is a complex, one-time process or "a temporary endeavor undertaken to create a unique product or service" (Pinto, 2010). Projects are limited by budget, schedule, and resources and are developed to yield a tangible result. And, projects are terminated upon successful completion of performance objectives or terminated for various reasons, as in go/no-go decisions or business strategy changes. Projects are defined by limited life cycles and are initiated, completed and the project team dissolved. As defined in Project Management textbooks, Project Management is an ad hoc endeavor with a clear life cycle. Project Management provides the tools and techniques necessary for the successful initiation, planning and execution of a project (Heldman & Mangano, 2009). Projects are successful if they come in on time, within budget constraints, and operate according to specifications. A fourth criterion has been added recently to the three typical constraints and that is "client acceptance", that the client is satisfied with the completed project (Pinto, 2010). Project Management, as defined, focuses up to the point of implementation and hand-off, not on building to maintain the project after initiation. To be clear, our position extends the definition of successful Project Management to include maintenance of the project after implementation.

The need for a well defined project methodology is tied to the Capability Maturity Model (CMM). If success is not repeatable then complex projects are doomed to failure (Whitten & Bentley, 2007). When projects are complex, there is more pressure upon the project manager. And in today's world, projects often have more, not less, complexity, which can increase the risk of failure. Our deepening dependence on ever-more complex systems also brings with it the risk of security vulnerabilities (Goldsmith & Hathaway, 2010).

Complexity of projects is determined by many factors: the number of people whose work will be changed by the project and the depth of that change; the number of organizational processes that will be changed and the depth of the change; the number of processes between the organization and other organizations that will be changed and the depth of the change; and the interval during which all of this change will occur. If the change required for the project is too broad in scale, scope, and depth, then it becomes more difficult, if not impossible, to implement well let alone to keep maintaining afterwards (Glaser, 2005). We mention this to remind project managers that implemented systems are vulnerable to failure because of increasing complexity of integrated systems.

3. IS 2010 COURSE – PROJECT MANAGEMENT

A Project Management course, as laid out in IS 2010 curriculum, discusses the processes, methods, techniques and tools that organizations use to manage their information systems projects. The course covers a systematic methodology for initiating, planning, executing, controlling, and closing projects. This course assumes that Project Management in the modern organization is a complex team based activity, where various types of technologies (including Project Management software as well as software to support group collaboration) are an inherent part of the Project Management process. This course also acknowledges that Project Management involves both the use of resources from within the firm, as well as contracted from outside the organization (Topi, Valacich, Wright, Kaiser, Nunamaker, Sipior, & deVreede, 2010).

In this course, students learn to prioritize information systems' projects, understand the foundation of Project Management, manage project teams, communication, schedules, resources, project risk, project quality, project execution, control the projects and close projects. Some of the major topics recommended in the IS 2010 curriculum for the Project Management course include: terminology, project failures and successes, the Project Management lifecycle, its context, its processes, project communication, planning, scope, and implementation (Topi, et al, 2010).

Successful projects are those projects which have delivered their full expected value, and were on time and under budget. One would not think that focusing on successful projects would be a wise use of classroom time when almost all of the literature is on achieving success. But, examples abound of those "success" stories that fail miserably after implementation. The fact is that project success rates have not changed in 20 years yet Project Management courses are still basically taught the same way, the textbooks still include the same topics, and the goals for the course have not changed in IS 2010. Systems are more connected and complex, yet at turnover time, project teams disband and the new technology is thrust into an organization that may not be prepared to deal with the complexity of a new system. Typically IT delivers complex services to customers who do not understand the benefits and risks to the enterprise (Cramm, 2010). Students pursuing an IT degree focusing on system analysis and Project Management career path face an increasingly challenging environment as previously mentioned. The success ratios for IT projects already continue to be threatened even more so after a system is up and running. Dependable and seemingly safe systems fail in practice for a number of reasons including an incomplete understanding the process of making a system "safe", failure to consider the larger system which is affected by the newly implemented subsystem, and ignoring failure points that will cause the safe system to become unsafe when implemented (Medikonda & Panchumarthy, 2009).

A review of a number of Project Management texts used in college courses show that the textbooks and courses are closely aligned with the IS 2010 curriculum objectives. Again, Project Management texts have not changed focus in many years; yet, there is still the same percentage of low success rates for IT projects over the last 20 years. And, more importantly, no text reviewed recommended retaining the project manager or the knowledge of the project development in the organization after the project was delivered.

Knowing what the expectations are for a course in Project Management, and the learning outcomes, where in Project Management courses are guidelines taught to manage successful projects through not only implementation, but after the project is deemed complete and the project manager moves on? To summarize, there are a number of "successful" systems which are increasingly more and more complex. Maintenance and required changes to existing systems form a recipe for technological disaster. This area is not discussed in Project Management texts nor anywhere in the IS 2010 model curriculum, though this course is where complete understanding of implementation resides. The lessons learned from past technical disasters should be addressed in a Project Management course. With these lessons, students can develop the ability to consider possible and probable risks to a complex project, and plan accordingly. Effective failure management means having an understanding of the types of failures which could affect the system, how to detect and mitigate the potential failure, and development of a process for the fail-safety of an implementation (Ermagan et al, 2007).

Where in IS 2010 are these threats and potential failure points addressed? What can we do to better prepare our CIS students to deal with this challenging environment from an IS 2010 point of view? What needs to be done differently in our IS curriculum to prepare students for the challenge of maintaining complex, interconnected systems? Business faculties have found case studies to be an effective learning tool for students to experience real-world situations in the classroom. Studying technological disasters can assist CIS students in the same way. The lessons to be learned are discussed in the next sections.

4. LESSONS FROM TECHNOLOGICAL DISASTERS

People seem willing to trust technology to help us, but we often back away from it when we witness human misuse of that technology, often inappropriately blaming the technology for the outcome. Titanic, Three Mile Island, and Columbia/Challenger have extraordinary parallels because all involved unfortunate learning about the human role in evolving technologies (Mittelstaedt, 2005). Technological disasters are not "Acts of God", which are unpredictable and unpreventable but rather "Acts of Man", thought to be both predictable and preventable. An example is the recent oil drilling disaster in the Gulf of Mexico. BP has experience in oil drilling offshore, but not in using the same technology at 5,000 feet deep in the ocean. The same processes that work in shallow water obviously were not as adaptable to deep water pressure as originally believed, and the emergency stoppage measures were at best ineffective and at worst futile.

An examination of these and other technological disasters found that the principal causes of technological disasters are:

- Human factors, including complacency
- Technical design factors,
- Organizational systems factors,
- Socio-cultural factors (government regulation, etc), and
- Technological terrorism (Evan & Manion, 2002).

Outside of the terrorism issue, which is often discussed with regard to computer security, the first four factors listed above also contribute to project failure after implementation, yet these factors are not included nor discussed in most Project Management texts nor in the IS 2010 curriculum guidelines.

One theme common to technological disasters is that highly skilled professionals ignored conspicuous warnings of dangers involved and pushed the technology they controlled beyond its limits. Technological disasters are not mere accidents – they are disasters directly related to human action (Evan & Manion, 2002).

As computers are the pervasive technology of our time, computer related errors occur too frequently. Some theorists have suggested that all errors are human errors, both active and latent errors. Failure to design safety-critical systems can be attributed to a mismatch between a technological system and a human operator. Human factors are critical to whether the system will operate, be understood in adverse conditions, and how preventative measures may be taken (Kopec & Tamang, 2007). Large scale disasters rarely develop instantaneously; there is an "incubation period" before the disaster that begins when the first of the ambiguous or unnoticed events occurs (Turner, 1978).

A project doesn't stop changing when it is delivered to the final customer. As users adjust to using the new technologies, users may become complacent in their ability to use the technology and believe they have reached a higher level of sophistication where they can adapt the technology to uses for which it was not intended (Brooks, 1975). As systems are so interrelated, a change in usage for one system impacts the interactivity of all.

Obstacles to effective communication between top management and project managers and lack of understanding of complex IT systems by senior management lead to decisional inertia. IT project managers typically come from a technical background and are not always trained to assume a managerial role in Project Management (Reich & Sauer, 2010). Lack of effective communication between top management and rank-and-file employees is said to be a potential cause of technological disasters, as lack of communication deprives management of the information and knowledge necessary for rational and prudent decision making. Another cause leading to failure to act in a timely manner is top management's ignorance of information systems management (Evan & Manion, 2002).

One topic examined in a Project Management course is risk. Traditionally, the risk addressed is risk factors affecting the project's successful completion. Risk assessment can indicate existing or potential system vulnerabilities. But, hazards can never be completely eliminated from all systems. Project Management risk assessment covers areas such as cost estimate risk, schedule (delay) risk, operating risk, organizational risk, integration risk, and Acts of God (Pinto, 2010). Project managers rate the probability of these risk events occurring and put forth effort towards those factors that have a high rating of probability. Then, project managers can decide whether to accept some minor as inevitable, try to minimize risk, share the risk among partners in the project, or transfer the risk to an outside organization, such as buying insurance to cover financial loss (Pinto, 2010). As IT projects (systems) become more and more networked and interconnected, the risk of failure of the expanded system grows and the impact of that failure is positively correlated. IT projects more often fail when project managers think of, and plan for "probable" risks, but accept "possible" risk as a cost of doing business. All risk is risk; students should know that possible risk can, and often will, happen, potentially leading to a catastrophic event.

IT risk is business risk, because technology failures can interrupt core business functions. expose sensitive data to unauthorized access, and result in bad decisions based on bad data. IT risk management is becoming more complex given the expanded regulatory oversight, increased interdependence of technological systems, and emerging 24/7 business models (Cramm, 2010). All sorts of information assets are migrating online and are now subject to malware attacks (Creeger, 2010). What is missing is risk assessment of maintenance, not just risk assessment of completion. Who addresses project problems after implementation? And who is responsible if, or more probably when, systems fail, thereby interrupting the flow of business? When organizations hire external project managers (outsource), they lose project knowledge when the project manager leaves; at least an internal project manger would still be on hand with the knowledge and expertise to assist as successful projects start to show signs of failure.

5. COMPLACENCY ISSUES IN FAILURE

Managers in an organization that is implementing new technological systems have to constantly fight a sense of complacency among those who use the system and become accustomed to using it. There is a sense that a working system will keep working and employees develop a sense of comfort with the technology. Managers need to take specific action to move employees out of their comfort zone to address and prepare for areas of possible risk (Tan, 2007). One of the root causes of human complacency in organizations is weak leadership. Weak leaders are afraid to inform staff of poor performance or non-compliance (Tan 2007). Frequently leaders contribute to failure by permitting poor Project Management and by not showing publicly commitment to the undertaking (Glaser, 2004).

Three types of at risk behavior (complacency):

- Intentional – when the employee knows full well that the activity is unsafe, and there is significant risk involved. However, the benefits of performing the task unsafely (in violation of a policy or procedure) seemingly outweigh the risks.
- Unintentional – employee is unaware of the risks.
- Habitual – employee is aware of the risks but has been doing the activity so long that he is no longer as alert to the risks. (Higbee, 2006).

Ideally, project managers may be guided by the principle of minimizing risk, but for top management, efficiency often trumps safety. To minimize risk and include reliability into systems, analysts/designers need top management's commitment to safety as an organizational goal and the need for personnel and engineering redundancy. Rooting out complacency and dealing with it is definitely a management issue.

6. CONCLUSION AND RECOMMENDATIONS

So, what can a project manager do? Specifically, what can an IS 2010 Project Management course do to prevent project failure after implementation? There are lessons to be learned from technological failures of the past and a realization of increasingly complex integrated systems. Management and maintenance of existing systems are critical. The lessons listed need to be introduced as an essential topic. Risk and consequences of failure in each functional requirement need to be examined and a plan put in place to handle and mitigate any problems. If nothing else, any IT employee/student should be exposed to these issues and understand that possible and probable do in fact happen, no matter how rare and remote. The government's token response to increased cyber risk forces organizations to rely on themselves and each other for security solutions. The focus of time and money in Project Management is in direct conflict in the short-term with safe and secure systems; system security from risks is expensive and its benefits are hard to quantify (Goldsmith & Hathaway, 2010).

When is the project manager's job completed? If a project manager has been hired externally, when that project is delivered, the project manager's job is now over. Our findings do not support the belief that Project Management can be outsourced. The scope of Project Management needs to be matched to its increasing complexity, making the project manger's job more challenging. Some would argue the job of a project manager never ends. By getting students to think in terms of plan B's in their design/implementation and maintenance stages, successful systems may just stay that way.

7. REFERENCES

Brooks, F. P. Jr. (1975). The Mythical Man-Month. Addison-Wesley Publishing Company, Reading, MA

Cramm, Susan. (2010.) Eight things We Hate about I.T. Harvard Business Press, Boston, MA.

Creeger, Mache. (April, 2010). CTO Roundtable: Malware Defense, Communications of the ACM, 3.

Ermagan, V., Krueger, I, Menarini, M., Mizutani J., Oguchi, K., & Weir, D. (2007). Towards Model-Based Failure-Management for Automotive Software. Fourth International Workshop on Software Engineering for Automotive Systems (SEAS '07). IEEE. 2007

Evan, W. M., & Manion, M. (2002). Minding the Machines. Preventing Technological Disasters. Prentice Hall, Upper Saddle River, NJ.

Glaser, John. (2004) Management's Role in IT Project Failures. Healthcare Financial Management, October, 2004.

Goldsmith, J., & Hathaway, M. (June 13, 2010) "High Price vs. High Risk", Maine Sunday Telegram, June 13, 2010.

Heldman, K. & Mangano, V. (2009). PMP. Project Management Professional Exam Review Guide. Wiley Publishing, Inc. Indianapolis, IN

Higbee, Gary A. (2006) Workplace Complacency – Reduction Techniques http://www.higbeeandassociates.com/articles/workplace-complacency.pdf

Kopec, Danny & Tamang, Suzanne (2007, June). Failures in Complex systems: Case Studies, Causes, and Possible Remedies. SIGCSE, 39 (2)

Medikonda, B., & Panchumarthy, S.R. (March 2009). A Framework for Software Safety in Safety-Critical Systems. SIGSOFT Software Engineering Notes, 34 (2)

Mittelstaedt, Robert E., Jr. (2005). Will Your Next Mistake be Fatal? Wharton School Publishing, Upper Saddle River, NJ.

Pinto, J. K. (2010). Project Management. Achieving Competitive Advantage. 2nd Ed. Prentice Hall, Upper Saddle River, NJ

Reich, B. H., & Sauer, C. May, 2010. Roles of the External IT Project Manager. Communications of the ACM, 53.

Stanleigh, Michael. (2006). "From Crisis to control: New standards for Project Management". Ivey Business Journal, March/April 2006.

Tan, Victor S.L. (2007, May 5) Ways to Eliminate Complacency, New Strait Times.

Tichy, L., & Bascom, T. March, 2008. "The business end of IT project Failure". Mortgage Banking. March 2008

Topi, Heikki, Valacich, Joseph S., Wright, Ryan T., Kaiser, Kate M., Nunamaker, J.F.Jr., Sipior, Janice C., & de Vreede, G.J. IS 2010 Curriculum Guidelines for Undergraduate degree programs in Information Systems. http://www.acm.org/education/curricula/IS%202010%20ACM%20final.pdf

Turner, B. (1978). Man-made Disasters. Wykeham Publications, London.

Whitten, J.L. & Bentley, L.D. (2007). Systems Analysis and Design Methods. McGraw-Hill Irwin, Boston, MA