CHAPTER 1

SUBVERSION

We use several approaches to explore subversion. The first section covers case studies and examples of subversion on software projects; the background information for the material is drawn from the computing and popular press. In the second, and longest, section of this chapter, we present the findings of our unique research survey, one in which we surveyed practitioners to determine how often subversion happened in the software world, and in what ways. We are particularly proud of this section, in that we present the results of exploring a major topic in the field of computing and software that no one else has explored. (An abbreviated version of this material was published earlier in a leading computing journal). Finally, in the third major section of the chapter, we present the hitherto unpublished results of a follow-up survey, one in which we asked responders to the first survey for additional input.

Now, on to the case studies.

1.1 INTRODUCTORY CASE STUDIES AND ANECDOTES

Some Motivational Examples. A sprinter is preparing to break a one-hundred-meter record. During the race someone on the edge of the track disturbs him by throwing pebbles at him and holding up funny pictures. The sprinter's chances of breaking the record are diminished because of the distractions. If the person who is causing the disturbances is an experienced sprinter himself, he might do it in a more sophisticated way—for example, tens of seconds before the official start he might imitate the sound of the starting signal. The sprinter is thus likely to fail in breaking the record and, what is more, he may even fail before the start of the race. The analysis of the failure of the project concludes the following: "Study after study reveals that sprinters have the most problems in the fractions of a second around the start, that is, at the very beginning of the race" (also known as the "requirements phase"!).

Such a situation in sports verges on the ridiculous. However, it happens quite frequently in software projects. A great number of software projects involve people who wish the project to fail. How is this possible?

The Dark Side of Software Engineering, by Johann Rost and Robert L. Glass
Copyright © 2011 IEEE Computer Society

1.1.1 A Faculty Feedback System

A college wanted to introduce an online system that allowed students to give anonymous feedback to their teachers. The feedback system was intended to provide an outlet for the evaluation of the quality of lectures and even reveal possible problems. It was hoped that, in the long run, the system would help to identify ways to improve the average quality of lectures.

A superficial analysis revealed three stakeholder groups: the students, the professors, and the college management. The students and the management supported the planned system for obvious reasons: The quality of the lectures and thus the reputation of the college were expected to improve through this project. In theory, both the students and the management would benefit from increased influence; the management would have gained access to additional ways of control. The students were concerned, however, that the anonymity could be broken one way or another, resulting in potential disadvantages for students who had given negative feedback.

A broad consensus of opinion indicated a concern that the feedback needed to be secured against potential manipulation. To prevent the possibility of results tampering by the students, each student was provided with only one opportunity to vote for each lecture. The chances for a very angry student to submit the same negative feedback more than once (thus dramatically lowering the average evaluation feedback for that particular lecture) were reduced. To prevent the possibility of a professor illicitly tampering with the system (for example, giving excellent feedback to his own lecture by pretending that he was a student), other safety measures were introduced. The system had to prevent all these kinds of potential manipulations of information. However, the aspect of protection against falsification required some authentication, which could be a conceptual conflict to the prerequisite of anonymity.

The professors' responses were multifaceted and therefore required further analysis. Some professors who were well known for their outstanding lectures welcomed the plans for the feedback system enthusiastically for quite obvious reasons: They expected excellent feedback for their lectures. Officially, there was no connection between the students' feedback and the career opportunities of the professors. It was obvious, however, that continuous good feedback would be taken into consideration if a higher position in the college management became vacant.

Other professors were more reluctant about the feedback system. Some teachers bore the responsibility of teaching difficult (and mandatory) lectures such as math. Since these lectures were known to be unpopular with many students, the teachers expected negative feedback: Even an excellent lecture of this type (for example, in statistics) would never get feedback as good as a "special interest group" lecture in which only students who are fascinated with the topic participate.

Additionally, some teachers, who were running a small consulting business in addition to their teaching duties, were concerned that the feedback system might force them to spend more time preparing the lectures, something that could eat into their time for professional engineering consulting. This college allowed additional consulting income as long as the teaching duties were not affected. However, this type of sideline was only tolerated but not fully accepted.

Other teachers had secret concerns that the feedback system could reveal deficiencies in their teaching abilities. These teachers feared they might be unable to solve the problems fast enough (or worse, might be unable to solve these problems at all); the teachers had serious concerns about the negative impact of the feedback system on their careers. Some teachers even advocated the cancellation of the project system plans due to the anticipated negative impact of the system on the working atmosphere among the professors, in addition to their concerns about possible data misuse. Most professors, however, kept their opposition secret, hoping that the project would fail or that the topic (an online feedback system) would simply disappear from the agenda one way or another.

After the project was under development, a growing discussion arose around the issue of who "owned" the data and what would be done with the results. The students were of the opinion that student representatives should administrate the data. They claimed that the feedback was given by students and that for this reason the students are the legitimate "owners" of the data. Moreover, the students suggested that all results should be made public automatically. The teachers were not particularly fond of this idea. Publishing the results in an automatic way implied certain risks, particularly if the results were very negative. (For example, if the system was manipulated, it would be difficult to completely rehabilitate the reputation of the [unjustly] denounced teacher.) The results could be borne out of methodical weaknesses—that is, if only one or a few students provided feedback for a certain lecture, these few opinions might be negative even if the lecture was, in reality, more or less okay. However, in certain cases where the lecture was really poor and the negative feedback was more than justified, the college management would have a more efficient way to solve the problem (rather than pillory the particular teacher). It became clear that negative results would need further analysis and that the decision to stop the automatic publishing if necessary should be placed under human authority.

Some teachers suggested that the results should be accessible only to the professor whose lecture was given feedback. Others suggested that the results should be accessible to a committee consisting of professors, management, and perhaps students. The committee would analyze the results and decide what should be done with them. But here were disadvantages to this solution. For example, if this committee had exclusive access to the data, some of the professors (i.e., the members of the committee) would have had access to very delicate information about other professors (i.e., their colleagues). This knowledge would give them additional influence and power. The shift of power might prove to be a disadvantage for the "group dynamic" of the college.

Then, a prototype of the system was presented publicly at the college. The meeting was meant to encourage decision making regarding the fate of the project and whether it should be continued or not. During the presentation, it became completely clear that a large group of professors were totally against the project and wanted it cancelled (perhaps even the majority of professors shared this sentiment). This group, however, did not have enough of an argument against the system. That is, they did not have enough of a legitimate argument. Of course the professors had more than enough (secret) reasons to wish for the cancellation of the project. Those reasons, however, could not be brought into discussion—the reasons had to do with the sideline consulting business.

So this group of opponents changed their strategy: They did not try to cancel the project anymore. Instead they tried to destroy it. Notice the subtle but important difference between "cancel" and "destroy." When a project is "canceled," an authority decides that the project will be discontinued. Usually this decision requires logical reasons that are considered legitimate in the particular group. When a project is going to be "destroyed," the project goes on—at least for the time being. The subversive stakeholders, however, try to influence the project in a way that finally leads to its failure (usually for "technical reasons"), thus enabling them to keep their true motivation secret. Unlike a "cancelled" project, a "destroyed" project (which "fails" for allegedly technical reasons) does not require any additional arguments to be discontinued.

The group of professors who were against the project followed the above-mentioned subversive strategy: When it became clear that they (the group of professors) could not bring the project to a halt by using political arguments, they apparently "accepted" that the project would continue. From this moment on, the political discussions seemed to fade away in the background. But by making various suggestions, they tried to influence the project in a way that would finally cause it to fail, that is, be terminated for technical reasons. The discussion was centered on purely technical decisions. (Nevertheless, the opposing group of professors never lost the desire to stop the project.)

The Achilles' heel of the project was the conceptual conflict between the anonymity of the feedback and the security against manipulation. The resolution of this problem would require non-technical processes (that is, processes that happen on paper, not in software) and trusted individuals who could mediate negotiation and compromise on the part of all responders. But the opposing group of professors rejected all possible solutions for various reasons. Officially, the reasons were based on purely technical arguments. Unofficially, the group of professors just did not want to proceed with the project, hence the rejection of all possible solutions.

Using entirely technical arguments to achieve a political goal is highly conspicuous in many projects. Subversive stakeholders sometimes use this strategy to block out senior management from making decisions. Note that senior managers usually cannot follow a purely technical discussion. This means that senior management cannot control the decision—they cannot control what they cannot understand. This specific project was particularly "lucky" because one of the managers had enough knowledge of software technology to see through the subversive strategy and save the project. But it was merely a lucky coincidence. Many projects lack such a member who has just the right combination of political instinct and software skills.

How would the post mortem report look if this project had failed? That depends on whether it is written by a software developer or by a manager.

An average software developer (without political instinct) might give the following feedback: "The clients and our superiors were constantly changing their opinions. It was simply impossible for us to find out what their expectations and plans concerning this project were. There was an endless back and forth of opinions. After a series of pointless meetings the project was finally cancelled."

An average manager (without skills in software technology) might write something similar to the following: "The software engineers did not understand the real needs of the users at all. They were completely lost in pros and cons over some technical decisions. When it became clear that this project would definitely not be completed and that we were beyond the point where we could expect any beneficial results, it had to be cancelled. Otherwise, even more money would have been invested on a hopeless project."

In this software project (and in many others), there is a wide rage of interests among various stakeholders. The range of separate interests might include some stakeholders' intentions to destroy the project. Such attempts may either be made out in the open or, more often than not, behind the curtain (depending on whether the reasons of the particular stakeholder are considered legitimate or illegitimate within the group). If the reasons are considered legitimate, they become a subject of open negotiation. If the reasons are considered illegitimate, however, they cannot be discussed openly; hence, they are not liable to negotiation. So the stakeholders would have to find other ways to reach their goals.

In the case study that was just discussed, some professors had motivations that were not considered legitimate in this group (such as maintaining the sideline consulting business or the fear that the teaching performance might turn out as unsatisfactory according to certain standards). Such motivations were against the true objectives of the project. So the professors had to find alternative ways to arrive at their goals without revealing their motivations—they used subversion.

1.1.2 An Unusual Cooperative Effort

A big organization and a small consulting company formed a consortium to develop a new software product. The partners agreed that they would equally share the efforts and benefit from the results together. For the small company the project was considered huge; it consumed the lion's share of their resources. For the big organization, however, the effort was somewhere between a small and medium project, compared to the size of the organization.

The project failed for technical reasons. Subsequent analysis revealed that most problems were within the big company's scope of responsibility. There was even suspicion that the big company had damaged the project deliberately.

That is the essential issue: Did the big company deliberately damage the project, and if so, why? Both companies suffered significant financial losses because they had to pay for their efforts, but did see any results to benefit from. The two companies, until the point of failure, apparently shared the same fate. But the effects due to the failure had completely different results on the two companies. The quarterly incomes of the big company were only slightly lower than expected. Conversely, the small company was almost ruined. The small company had to be sold. And—surprise, surprise—the big company became the new owner of the small company. The bigger company bought the smaller one at a rather cheap price because it (the small company) was in a difficult position. In hindsight, it became obvious that the big company had initiated the project from the very beginning with a view to ruin the small company—so that they could buy it… a strategy that turned out to be a complete success.

After the takeover was completed, the big company did not have any more reasons to obstruct the project. They restarted it, corrected their "mistakes" and finalized the project with moderate success. They even balanced most of their earlier losses by the profits made during the last part of the project.

1.1.3 Lack of Cooperation due to Self Interest

A German company with its own software development department decided to initiate cooperation with an "offshore" software company in Romania, where software engineers would not demand as high compensation as in Germany. In order to establish the basis of future cooperation, the German company first ordered a pilot—a rather small project of minor strategic importance.

The German software manager (middle management), however, refused to cooperate, providing information only when he was forced to do so by senior management. Even on such occasions the information was scarce and delivered at an extremely slow pace. His "official reason" for doing so was his demanding engagement in other tasks which were apparently too time consuming to allow him to contribute to the project. Nonetheless, the others suspected that he considered his job to be threatened by the software produced by Romanian engineers at lower costs. Due to the fact that the German software manager had considerable influence in his organization and his responsibility in other projects was far reaching, senior management did not want to put too much pressure on him to cooperate. But taking into account the promising economic prospects of the offshore cooperation, the German company decided to initiate the project, regardless of the lack of support on the part of the middle manager.

Eventually, the project failed. The final report analyzing the causes of failure concluded the following: "The project failed because of incomplete and inadequate requirements that did not meet the real needs of the client." On one hand, this statement is true because the requirements were indeed of unsatisfactory quality. On the other hand, the poor quality of the requirements was caused by the blockage of access to important information withheld by the uncooperative manager. At the beginning, the project team and the top management were unaware of the crucial nature of the manager's information. When this problem became apparent it was already too late.

1.1.4 An Evil Teammate

One responder of the survey that we will discuss later in this chapter related the following anecdote. This case study is of particular interest because it shows how the attacker uses technology to achieve a political goal. Usually these technical details are “below the radar” (and beyond the understanding) of top management. Thus they are not aware of the political dimension of the problem.

The attacker was a subordinate developer who was very keen on landing a position in higher management. First, he planned a subversive attack on the project lead and carried it out, step by step by using the bug tracking system in an interesting way.

In the beginning of the project, the bug-tracking system was applied only for its usual purpose—tracking bugs. The subversive developer was ceaselessly involved in the minutiae of the bug-tracking process and insisted that the bug-tracking system should be used as the adequate forum for various discussions—not only for the rather narrow purpose of reporting bugs and tracking bug fixes. This was a gradual process, starting with the forms of language used in problem descriptions, advancing to the definitions of problem categories, and finally gaining effective control over the policy settings for developers and projects leads in the configuration of the bug tracking service itself.

The project manager and the loyal colleagues were not aware of the danger of the attack and did not invest the necessary energy to stop this process early enough. That’s how the subversive developer was able to defeat the utility of the tracking system for its intended function (measuring the change in quality of the software and charting the progress of the project). Instead, the bug tracking system supplanted e-mail, telephone, and verbal dialogue as the central messaging system for communicating deceptive information to the corporate directors about schedule, resource usage, and project status. Developers and project leads could no longer use it for tracking bugs without filling it with material that the subversive stakeholder could use to stir counterproductive controversy, which attracted negative attention from corporate directors and management.

The attacker used blind carbon-copy e-mails to management and clever PowerPoint® presentations to increase the social tensions and doubts of senior management regarding the project lead’s qualifications. It didn’t help that management gave the direction, in a doomed effort to stop the controversy from consuming project time, to start keeping double books of bugs rather than reckon with the subversive stakeholder’s attacks. Then, when the project lead was replaced and the disloyal stakeholder assumed her position, he attacked the manager in a similar way.

The subversive stakeholder in question was not particularly technically skilled—but he was well versed in Machiavellian political strategy, and he exploited a weakness in the organization’s defense mechanisms against such subversive attacks. They were utterly defeated by it.

Here is what they should have done: Recognize the methods employed by the subversive employee as those of a political attacker and respond accordingly. There is a large body of knowledge (which is hundreds of years old) about how to thwart the efforts of political tricksters. An effective defense would have first required learning some of it. The project lead, her peers, the management, and the other members of the technical staff were all ignorant of the patterns, ignorant of political attackers, or simply unaware of the attacks.

Here is what they did: The project lead had a nervous breakdown and hasn’t recovered since; the manager quit in disgust and retired from the industry. The other project leads and members of the technical staff were mostly dumbfounded—they had never encountered this behavior before. The person who shared the anecdote reacted by learning about organizational psychology and political strategy.

1.1.5 Thwarting the Evil Union

The trade union wanted to delay (and finally destroy, perhaps) a project. They met once in two months to talk about new software, and no software could be installed without the union's "OK."

Here is what the contributor of this anecdote had to say:

> "I had heard that they [the union] lacked information about the system and would not give their OK before they had this information. So I asked several people what kind of information it could be and when the meeting would take place. It was early on a Monday morning. I had been told not to contact them; they would contact me. They did not. The week before, I had gathered the addresses of the responsible people (the addresses were available on the company′s Web site). I started writing e-mails to the union, but the e-mails were not answered. Then I called and tried to get someone on the phone, but they were constantly in meetings and they did not call back (although this was promised). But the union could not totally ignore my attempts to contact them—and on Friday afternoon at four o'clock, I got a phone call. The lady on the line was amazed that I still was in the office. I suppose she expected that I would already have started out for the weekend. She told me openly what information they needed from me. It was a lot! I asked for the details. After the phone call I wrote a protocol, sent it by e-mail, and promised to deliver the information by Monday morning, nine o'clock. It was not possible to gather all of the information, especially because it demanded the help of developers and others who were already in their well earned weekend. But I was prepared. I knew what information would be needed, and I had spent the last three weeks getting it from the different people. Now only some details were lacking. But I knew I could provide them myself, and at eight in the evening, everything was done. I could send the missing information to everyone who was involved. So it was official: I talked to the union and sent all the information they needed. And on Monday morning, they gave the 'OK.' How did I know that they were subversive at all? No one told me, but during the user training sessions, some of the union members were in my course, and I felt strong resistance. It was during the user training that I learned they had concerns about certain topics; therefore, I researched the topics."

As usual, subversive stakeholders cannot be subversive openly; one can use this against them. But it is very hard and one single error can spoil the whole fight.

1.2 THE SURVEY: IMPACT OF SUBVERSIVE STAKEHOLDERS ON SOFTWARE PROJECTS

"Subversive stakeholders" are software project stakeholders who want the project to fail. This section of our book discusses our survey which we designed and conducted to explore incidents of such activity—how frequently it occurs, why it happens, how such incidents are discovered, and what can be done about it.

The survey finds that the problem is widespread: Over 50% of responders have encountered the problem of subversive stakeholders on software projects, impacting about 20% of projects. The findings also suggest that the subversive stakeholder is successful or at least partially successful in a non-negligible number of cases.

To the best of our knowledge, this is the first formal survey of the problem.

1.2.1 Introduction

Studies of software project success and failure factors frequently appear in the software literature (some recent examples include Verner [2006], Jeffrey [2006], KPMG [2005], Nelson [2005], Ewusi-Mensah [2003], and Glass [1998]). Failure factors commonly include such things as unstable requirements and faulty (under-) estimation. It is also found that management problems cause failure more often than technical problems.

The literature in the field of software project management is particularly rich (some recent examples include Humphrey [1997], Morasco [2005], Glen [2003], Miller [2004], Boehm and Turner [2004], and Thomsett [2002]). These publications do an excellent job, in general, of identifying best practices in software project management and in providing treatments and cures for project difficulties. Failure and its causes are frequently topics of concern in this literature. Thus one could expect that, even though software project failure factors are frequently presented in the failure literature, the means of addressing those failures are well provided for in the management literature.

The risk literature in particular is a place where these concerns are often addressed, for example, Moynihan (2002), Jones (1994), Charette (2004), Charette (1997), Britcher (1999), Cockburn (1998), McConnell (1998), Ropponen and Lyytinen (2000). Project risks are identified in this literature, and means of addressing those risks are discussed. The second citation, Jones (1994), is a virtual medical handbook approach to software project problems and their solutions.

However, there is an interesting problem here. For all the discussion of failures, their causes and cures, mentioned above, there is one failure factor that is rarely included in any of these literatures: failure caused by subversive stakeholders. It is the purpose of this survey to identify this failure factor, to explain why the existing literature does not cover it, to discuss its prevalence, and to present ways of overcoming the problems it causes.

Here is our definition of that term: "Stakeholders" are people inside or outside the project who have any interest whatsoever in the software project and some influence over it. (That includes developers, project leads, architects, patrons, customers, consultants, and various user groups as well as managers outside the project). A "subversive stakeholder" is a person who wants the project to fail—that is, a stakeholder who wants to sabotage, to disturb, or to destroy the project. Only people who act intentionally to the detriment of the project are considered "subversive." Stakeholders who disturb the project due to incompetence or who are not aware of the consequences of their actions are NOT considered subversive in this survey.

Interestingly, while almost everyone in the software industry can share stories of projects that they have been involved with and which suffered from subversive activity, somehow that failure factor rarely, if ever, surfaces in the software literature. There are reasons for that, of course: There is something faintly embarrassing about failures that happen deliberately; there is usually lingering uncertainty as to whether the failure was deliberate or not.

We have encountered enough examples of such behavior that we believed it was important to explore its prevalence and frequently how such behavior served to the severe detriment of the project on which it occurs.

This is, so far as we know, the first formal survey of subversive software project stakeholders as failure factors (informal reports have appeared in such articles as Rost (2004), Rost and Glass (2005), Thibodeau (2005), and Nelson and Simek (2005); note that only the first two of these informal reports are specific to the field of software). An abbreviated version of this survey was published in the leading journal *Communications of the ACM* as Rost and Glass (2009).

1.2.2 The Survey

The survey involved contacting software practitioners and presenting them with a series of questions about their experiences with subversion.

Questionnaire

1. Have you ever encountered subversive stakeholders in software projects?

2. How frequently do projects include subversive stakeholders? That is, according to your experience, what is the percentage of software projects affected by the subversive interests of certain stakeholders?

3. What were the motivations and goals of the subversive stakeholders? Why did they do it?

4. What was the percentage of cases in which the subversive stakeholders finally achieved their goal (at least partially)? What fraction of the subversive attacks was finally

4a. fully successful?

4b. partially successful?

5. What role did the subversive stakeholders assume within the projects? (For example, developer, user, consultant, project lead, or manager).

6. How were the subversive attacks discovered? How did you find out that a subversive attack was being prepared?

7. How can projects be defended against subversive stakeholders? What did the project leads or the loyal stakeholders do against the sabotage?

8. How much experience do you have in industrial projects (outside of university)?

- More than seven years
- Between two years and seven years

- Less than two years
- Other pattern of experience (For example, three years fulltime plus ten years of occasional consulting). Please specify the pattern of experience.

9. Which role do *you* usually assume within software projects (For example, developer, user, consultant, project lead, manager).
10. Do you have any additional remarks left uncovered by the questions above but which might help to clarify the issue?
11. Do you want to receive a copy of the final report?

Development of the survey instrument went through two rounds of trial use, with feedback from 14 initial subjects resulting in instrument improvements.

The final instrument was then submitted to a broad population of computing professionals. Subjects were chosen from a variety of sources. Candidate responders were identified by using Google to search on such software-focused terms as “project manager” or “team lead.” Following that, online bios were studied to determine potential responders. Authors of relevant papers, professors with practitioner experience, industry “gurus,” and a large number of practitioners formed the chosen population. Attempts were made to have a wide geographic distribution, including the United States, western Europe, Russia, Romania, India, and China, and to have a wide variance in subject experience.

Identifying a sufficient number of responders and the responder response rate were both problems (see Section 1.2.7).

The questionnaires were distributed, and the responses were made by e-mail. Due to the use of this method, it was possible to link each set of answers to a certain responder and to ask for additional information where worthwhile. Consideration was given to collecting the data via a Web interface instead. However, during the pre-test, some “fierce” and very emotional answers were received, leading to the fear that some responders might want to sabotage the survey by abusing the Web interface and inputting “junk” data. Thus e-mail was used instead.

The result is a set of numeric findings, but, perhaps more importantly, a rich set of quotations and opinions from the responders. Both the quantitative and qualitative findings are presented below.

1.2.3 The Survey Findings

Ten questions were asked of the subjects of the survey. They involved the issues of the existence of subversive activity, the frequency with which it occurs, the motivations/goals of the subversive stakeholders who engage in such activities, the frequency of failures caused by such activity, the methods by which the subversion was detected, and approaches projects can use to defend themselves against subversive activity. Two of the questions resulted in primarily quantitative responses, and those responses are presented in Section 1.2.3.1. The other eight questions resulted in qualitative responses, and those are presented in Section 1.2.3.2. Finally, some responses to the questions revealed patterns of subversion; those are presented in Section 1.2.3.3.

1.2.3.1 Questions and Quantitative Responses In this section, the core quantitative questions in the questionnaire are presented, followed by an analysis of the responses to that question.

Have You Ever Encountered Subversive Stakeholders in Software Projects? Fifty-four responders (a little over 50%) reported that they have encountered subversive behavior in software projects. Thirty-eight (35%) said they have never seen this problem. Fifteen (14%) responded but refused to answer the questionnaire (follow-ups suggest that some of them were precluded from doing so by corporate policy, and others felt they had insufficient experience for their input to have value). The findings are presented in total and broken down by experience level of the responders. See the table below for details.

The figures in the cells of the table are the number of responders in that respective group. (That is, 21 colleagues with more than seven years experience have never seen this problem). Note that years of experience tend to correlate with encountering the problem.

How Frequently Do Projects Include Subversive Stakeholders? There are several interpretations of the responder answers to this question. The median of all responses is that 20% of projects involve subversion. However, many responders gave qualitative answers rather than a percentage—for example, “twice in ten years,” “once or twice in ten years of experience,” or “one out of seven projects.”

The responses showed varying levels of frequency of subversive behavior: Sixteen responders are aware of subversive activities but consider them rare (≤5% of the projects); another 31 felt they were common (5%–80% of projects); and seven reported that this problem interferes with their projects rather frequently (>80%). Thus about 40% of the practitioners are acquainted with the problem of subversive stakeholders and have encountered it in a significant part of their projects (>5%) while the other 60% considers subversion a minor problem or one that has not confronted them at all.

In Table 1.2, the column “Number of responders” indicates how many responders gave the respective answer. The sum of 16 + 31 + 7 = 54 matches the respective number in Table 1.1.

These results raised an interesting question: Why have a significant fraction of experienced responders never encountered subversive behavior, while others reported this problem as “rather frequent”? To clarify this issue, additional questions were sent to the responders who had never or rarely encountered subversive activity. Here are those follow-up responses:

- Some organizations are more “political” and therefore prone to subversive activity than others. Six responders considered their respective organization’s well-defined processes to be an important reason why subversive behavior is at a minimum.
- Some people are more sensitive to political processes and subversion. Eight responders considered it somewhat paranoid to search for subversion behind behavior that might simply be the result of incompetence or mishap. Another

TABLE 1.1 Have you ever encountered subversive stakeholders in software projects?

Experience	0–2 years	2–7 years	7+ years	Other patterns	Unspecified Experience	Industry Gurus	Sum
Have encountered subversive stakeholders	0	6	37	3	3	5	54
Never seen subversive stakeholders	2	5	21	3	6	1	38
Answered but refused participation	0	0	2	1	7	5	15
Sum	2	11	60	7	16	11	107

TABLE 1.2 How frequently do projects include subversive stakeholders?

	Number of responders	Sum
Have never seen subversive stakeholders	38	38
Have encountered subversive stakeholders in at most 5% of the projects	16	54
Have encountered subversive stakeholders in more than 5% but less than 80% of the projects	31	
Have encountered subversive stakeholders in at least 80% of the projects	7	

responder, however, wrote: “One can choose to perceive or not to perceive subversive behavior, but if the behavior has a subversive effect, it really doesn’t matter whether one chooses to perceive it or not. The effect is real.” Increasing awareness of subversive activities requires a certain overview of the project’s politics. Subversive activity is less conspicuous to those in certain roles (such as developers).

- Eight responders admitted that the reason for which they had never or rarely encountered subversive activities might be that they are lacking relevant experience or their projects had specific properties that make subversion very unlikely.
- Four seasoned project managers wrote that they know potential sources of subversion and they are aware of the symptoms of such an attack. If they notice mildly subversive behavior, they have enough influence and experience to fix the problem. Consequently they reported that subversive behavior is not a serious issue on their projects.

1.2.3.2 Questions and Qualitative Responses The survey led to a number of qualitative, as opposed to quantitative, responses. In this section we present a summary of those results, which is derived from the remarks and anecdotes that we received from the responders. In each case below, we provide the question that prompted the qualitative response, then a summary of these qualitative responses.

What Were the Motivations and Goals of the Subversive Stakeholders? Responses to this question were grouped informally into 11 classes (derived bottom-up from the responses). Under each class umbrella are some of the responses that caused that class to be invented. A more complete presentation of these responses is given in Section 1.3.1.

Egotistic Motivations Conflicting with Corporate Goals. Often, individual project members thought that the project should be conducted in a different manner from the way in which it was actually conducted; alternately, the project members would have preferred project outcomes to be more in line with their own personal wishes. Responders noted concerns about things such as project success leading to more work, more (undesirable) accountability for the subject, or a personal preference for project failure over project success.

Job Security. Defending one's own position was a motive for subversion. Responders noted concerns about things such as the successful project eliminating or drastically changing their job.

Revenge and Disgruntled Employees. Getting even for some past occurrence was another motivation. Responders noted concerns about things such as disgruntled stakeholders seeking revenge for past problems or harming a project simply through a bad attitude.

Challenge of Authority and "Ego-Reasons." For a variety of reasons, people lower in a hierarchy sometimes try to attack those above them. Responders noted concerns about people who sought to make themselves look especially good (for example, hiding incompetence), or making specific others look bad (for example, shifting rewards in their favor). Attempting to diminish the power base of someone else, or seeking more power for themselves, was another factor.

Competition Between Individuals, Rivalry, and Animosity. The motivation was often at the individual level, a person-to-person kind of thing. Some example responses concerned battles over whose idea the project was, or conflict between backers of new ideas versus older ones.

Competition Between Departments and Organizations. It is not unknown for the motivation to be organizational rather than personal. Some responses noted the seeking of benefits from competing incentive plans, pushing others toward being scapegoats if the project fails, or agitating control struggles.

Competition for Budget and Resources. Organizational motivation might be about resources, budget, and time. Responses included the following: "There is a competitive world out there.... There will always be turf wars. Budget cutting caused by stakeholders outside the project (non-stakeholders) is probably the number one killer of good software."

Resistance to Change. Some people are motivated by a wish to keep things as they are (such as wanting to keep the old product in order to avoid having to learn something new).

Disagreement on Some Major Architectural or Technological Choice. Some people are motivated by strong feelings about technical issues. Technical people, mainly programmers, sometimes become saboteurs when they want to use a different tool/technology/methodology than the one(s) mandated for their project, or they want to eliminate constraints/standards that they see as counterproductive.

Disloyal Partners. Sometimes it is the people from outside the enterprise who are motivated to sabotage it (such as partner firms, contractors, and outsourcers who want to improve their contractual position, or who want to win a culture clash battle at all costs).

Split in Upper Management. Sometimes it is the senior people in the enterprise itself (for example, the upper manager nurturing the project may have enemies who want the project to fail, sometimes simply because of who is nurturing it!).

What Was the Percentage of Cases in Which the Subversive Stakeholders Finally Achieved Their Goal (at Least Partially)? Even though the subversive stakeholders constitute a small minority, they can make a lot of trouble, causing incredibly high costs for their organization. There is a broad consensus that most attacks are at least partially successful. A number of responders confirmed that the attack *always* causes delays, additional costs, and/or may motivate good people to leave. Most responders agreed that only a smaller fraction of subversive attacks are fully successful—that is, actually disastrous for the project.

Some responders reported that certain patterns of attacks are much more dangerous than others (such as a senior manager from outside derailing the project from a distance). Attacks on the part of management may be an indication of a split or political war at the level of higher management. This is frequently (or almost always) disastrous for the project. Attacks from below (such as one from a user base or from developers) can be efficient if they are coordinated.

How Were the Subversive Attacks Discovered? Once again, there were several classes of responses, grouped in bottom-up chosen categories. A sampling of those responses is given below; a more complete presentation of these responses is given in Section 1.3.2.

Some Attacks Are Carried out Overtly. Perhaps surprisingly, not all subversive activity is carried out in secret. Responders spoke of subversive activity being in the open, such as during meetings or via e-mail. Some reported subversive stakeholders even boasted openly of their success.

Informal Network. Other subversive activity may be handled by a cadre of people (for example) via the exchange of faulty information or via groups intimidating those who might report the subversion.

It Is Not a Single Event—It Is a Process. Sometimes it is hard to identify a single event that can be called subversive; the designation of some event as a "subversion" comes from patterns of behavior over time. Such subversion rarely rises to the level of project progress reports.

Case-Specific Discoveries. Sometimes subversion is identified through things unique to the project: subversives withhold information, attack the project in status reviews, report progress where little or none is being made, or report none when the project is moving forward.

How Can the Projects Be Defended Against Subversive Stakeholders? Here we present the bottom line on the subject of subversion and ask the following question: "What can be done about it?" This sampling of responses is about solving the problem. A more complete presentation of these responses is given in Section 1.3.3.

Applying Quality Project Management Practices. A nice and hopeful answer to the problem is that "good management will win out in the end." Techniques suggested include a robust development process, project audits, and the use of appropriate checks and balances. One responder noted that *"in a well- managed company this sort of political in-fighting does not happen."*

Quality Communication. Another hopeful answer is that communication is the key. Such communication should be open, honest, inclusive, and focused. Methods include project reports, audits, and less formal involvement of all project players.

Psychology. And then there's the hopeful answer that common sense, via psychology, will prevail. Improve the hiring/firing process, particularly focusing on psychological and not just technical factors. Make a priority of identifying/keeping cooperative and capable people.

Support from Senior Management. Sometimes it's necessary to call in higher powers. Move up the management ladder when necessary to solve problems, involving senior management if the problem is sufficiently severe.

Taming. At times, one can tame the savage subversive beast. Involve and include the subversives, seek their cooperation, convince them if possible, comfort them if they need help.

Or Fighting Back—If Taming Fails. But in some cases, the opposite must be tried. Eliminate them, work around them, fire them if possible.

Pessimistic Opinions. And, unfortunately, sometimes nothing will help—there are no hopeful, or common sense, or taming approaches. Responders provided the following statements: “You can’t fully defend any project against sabotage, either from within or without”; “There was probably nothing I could have done, except perhaps to get all tasks to be performed and the reasons for performing them, in writing”; “If the subversive stakeholder is quite powerful, the project lead and loyal stakeholders may lack countervailing power”; “There is no solution, not in the environment I work in”; and “I have tried several defense alternatives. However, I must admit that they never worked thoroughly because the subversion was not evident enough to really fight against.”

1.2.3.3 Patterns of Subversion Our survey results have revealed a number of patterns of subversive activity. This section explains these patterns. It also includes anecdotes related to these patterns that provide a framework for structuring the anecdotes.

The patterns

1. Rivals and enemies of the project lead (inside or outside of the project). The project lead might have enemies within the organization, some of whom might be competing with him/her for positions in higher management or in order to assume his/her role as project lead (that is, a subversive insider). Others might even have a personal conflict with the project lead.

2. Subversive stakeholders within the project.

2.1 Subversive project leads. Subversive project leads are people who are officially assigned the role of project leads and who act intentionally to the detriment of the project’s success (that is, NOT out of incompetence).

2.2 Subversive subordinated team members. This group consists of people who are part of the project team but who are not project leads (such as developers and testers).

2.3 Disloyal consultants. Consultants can be subversive in a way similar to the subordinated team members. The difference, however, is that the consultant tries to interfere with the project in such a way that s/he can continue billing—or can even extend the billable time.

3. Customers and users

3.1 Uncooperative users. Some users might be subversive because they reject the project for various reasons: They are concerned with keeping their jobs, they expect additional work, and they do not want to change established work processes.

3.2 Other dysfunctional persons on the customer’s side. Dysfunctional customers are subversive stakeholders on the customer’s side apart from users (such as a customer representative or manager).

4. Subversive stakeholders outside the project

4.1 Promoters of other projects who are competing for budget allotment. Subversive stakeholders can be motivated by the project budget. If the project is cancelled, the remaining project budget can be assigned to other projects. Thus the protagonists of other projects might gain an advantage from the project's failure.

4.2 Other subversive managers outside the project. This group consists of managers outside the project, who are NOT promoters of competing projects (see last item). The managers are not directly involved in the project's day-by-day business. They fire/launch missiles against the project from a safe distance. They do not have to "pay" in any way if the project fails.

4.3 Unfair partner companies. Unfair partner companies are legally and economically independent organizations who have some influence on the project's development and who behave subversively. The subversive behavior in this pattern is in fact a corporate decision

5. Other patterns of subversion.

5.1 Coordinated attacks. Several apparently independent stakeholders (for example, different user groups and/or developers) attack the project in a coordinated way (such the spreading of negative rumors about the project that reach senior management from apparently independent sources). Sometimes the coordinator is a manager from outside the project.

5.2 Split in higher management. The danger stems in fact from a split in higher management: Senior management is segregated into two or more factions that are at war with each other.

1.2.4 Conclusions

The strongest conclusion we draw from this survey is that incidents of subversive stakeholder activity on software projects are all too frequent. Over 50% of responders have encountered such activity. Unsurprisingly, such incidents have occurred most frequently among responders with more experience (presumably because they had had more years in which such incidents could arise).

There was an interesting disparity of findings in regard to the frequency of problems occurring. Some responders gave qualitative rather than quantitative responses to this question, but the median for all responders indicates that perhaps 20% of software projects are contaminated by subversive activity.

The remaining issues studied in the survey involved qualitative/opinion rather than quantitative responses. However, a strong and potentially useful collection of opinions were presented.

Eleven different categories (regarding the motivations of the subversive stakeholders themselves) were presented. The collected opinions noted that subversive stakeholders were motivated most frequently by ego (especially when it conflicted with corporate goals), intentional challenge of authority, and disagreement on major issues. Less significant were revenge and resistance to change. (A complete listing of specific answers to the survey question about motivation and goals is found in Section 1.3.1).

Four opinions were presented regarding how subversion was discovered. Perhaps surprisingly, the most common way the discovery happened was due to the fact that the subversive stakeholders were overt in their activity or because open rumors of such activity were pursued and found to be true! (A complete listing of specific answers to the survey question about discovery of subversion will be found in Section 1.3.2).

The (possibly) most important question in the survey ("What can be done to defend against this activity?") yielded five categories of responses. Several of them had to do with what would normally be considered good management practices, such as applying quality management approaches, keeping lines of communication open, seeking support from senior management, and the use of positive psychology. Some responders suggested what to do if all else failed (generate a work-around or dismiss the subversive person), and several responders expressed the belief that very little could be done. (A complete listing of specific answers to the survey question about what can be found about subversion is found in Section 1.3.3 of this chapter).

1.2.5 Impact on Practice

These survey results should be useful for several reasons:

1. They highlight a problem that is apparently very real and all too common.
2. They suggest ways that practitioners can discover the problem and suggest approaches that can be used to defend against it.
3. They present the motivations and goals of those who engage in subversion, which may make it easier to identify such patterns in advance.

1.2.6 Impact on Research

Researchers may find this survey interesting for several reasons:

1. It identifies an issue worthy of further survey, especially given this subject has not been studied before.
2. Although management problems have generally been seen as the most significant cause of software project failure, there has been little breakdown of "management problems" into more useful subcategories. There may very well be other subcategories of "management problems" besides subversion worthy of further survey.
3. Certainly this should not be the final survey of subversive stakeholders. Additional research and analysis of those results could explore the accuracy and usefulness of this first set of survey results; all of this gathered information can help to hone-in on causes and solutions to the problems.

1.2.7 Limitations

The biggest limitation of this survey pertains to the response rate of those contacted. As is typical with practitioner surveys, the response rate was disappointingly low, less than 5%. (Because the survey was announced in some mailing lists, it is impossible to give an accurate response rate). However, that rate is not the entire picture.

To achieve a richer set of responses, follow-ups were sent to some of the responders, wherein clarifications were sought and deeper discussions were initiated. Those responders who participated in this follow-up contact constituted both a significant number and contributed in large measure to the findings reported here.

A note regarding demographics: There is probably an over-proportional representation of industry "gurus." The majority of responders are from the United States and Germany. Interestingly, however, the subgroup did not seem to affect the responses—that is, results broken down by these subgroups tended to be the same as for responders as a whole, with the possible exception of "years of experience," a factor that did seem to affect the responses.

1.2.8 Challenges

All survey studies face certain challenges: Is the sample representative? Can the questions be misunderstood? Factors affecting software survey research are thoroughly discussed in Pfleeger and Kitchenham (2001).

Beyond these issues (which are common to all studies), our survey had its own specific challenges.

Recruiting Responders Is Difficult. This happened for several reasons:

- One obstacle is common to all survey studies: It takes time to answer the questionnaire and the responders ask, "What's in it for me?"
- More important, however, was the fact that this is a very sensitive issue. Some organizations suspected that survey results could be used to their disadvantage. The promise that the results would be used anonymously was not always enough (some responders felt that the survey would collect "doubtful competitive information" about their company).
- It requires a certain degree of trust to answer such a questionnaire. This may contribute to the observation that many responses are from persons personally known to Johann.
- Many responses were very emotional—to both extremes. Some were very enthusiastic. Others deeply rejected the notion that such a survey was being done at all.

Perception of Subversion Is Subjective. Some people choose to perceive its occurrence. Other people choose to ignore signs of possible subversion. For this reason, the results have a range of uncertainty. Another sample of responders or another setting for the survey might lead to different numbers.

There Is a Gray Borderline Between Subversion and Conflicting Interests. Many projects involve conflicting interests. It is not rare that project responders are somehow "forced" to contribute to a project. Alternately, they might experience advantages if the project fails or disadvantages if it is successful. It is difficult to identify all such responders as being subversive. They may not actively sabotage a project, but they behave in a subtle way to hinder its success. (For example, the project will need certain information, but they don't know it yet. Such a responder might think, "Well, they did not ask me and I'm not obliged to inform them." Other project responders might perceive this behavior as "subversive." The suspected "subversive" stakeholder, however, might perceive his or her behavior to be legitimate.

In other cases, the stakeholder might think that the project should not be carried through because it is contrary to the goals of the organization as a whole (or worse, contrary even to goals for human beings on this planet!). The project members who support the project will probably perceive this stakeholder to be subversive.

1.2.9 Acknowledgments

This survey was successful due to the contribution of the many practitioners who were kind enough to spend time filling in the questionnaire and share their valuable experience. Many of them gave extensive explanations and answered additional questions. Each of these contributers deserves inclusion on the list of references. However, promises of anonymity preclude that.

1.3 SELECTED RESPONSES

1.3.1 Sample Answers to the Question: "What Were the Motivations and Goals of the Subversive Stakeholders?"

The survey revealed a variety of reasons for subversion that can be roughly grouped into the categories below. (The categories were formed after we received the answers.) Thus the grouping of answers into categories is done by the authors—not by the responders—and might be considered subjective.

We have included some of the actual responses (provided in quotes). The selected responses may be considered representative. Nevertheless, the responses give a more "qualitative" impression. (Note that we do **not** think the number of contributions to a certain item allows a quantitative conclusion to be made, based on the frequency a reason occurs in practice.)

Egotistic Motivations Conflicting with Corporate Goals. A key observation of subversion is that it occurs in environments dominated by conflicting interests. Conflicting interests are not new: The buyer wants a low price; the vendor wants a high price—that's just one example. The specific factor here, in relation to subversion, is that some of the interests are considered "illegitimate" in that environment. This observation blocks the solution via usual negotiations. You cannot negotiate something when you don't dare speak about this "something." Notice that the same interests could be considered completely legitimate in another context. For example: An employee who optimizes his own personal advantage at the expense of the employing organization would be considered "subversive." If an independent vendor did the same, it would be a very usual and completely accepted business practice. That is, if the independent vendor optimizes its own advantage, it could create a circumstance that is not necessarily to the advantage of the customer.

Two examples should illustrate this issue:

1. An employee goes to his boss and makes a suggestion: "Let's negotiate the technology that we will use for the next project. Some possible technologies are advantageous to me because the usage (that is, having the knowledge to use them) would allow me to apply for well paying jobs." This would be considered a ridiculous suggestion.
2. A partner company suggests the following: "Let's negotiate the technology that we will use for the next project. Some possible technologies have strategic advantages for us." This would be a perfectly legitimate suggestion.

The following statements by several responders of the survey shed light on the issue of conflicting interests:

- "Their interests are better met by the failure rather than by the success of the project."
- "Their motivation comes from something other than success in the project. It is not so much that they want the project to fail, but it is 'OK' with them if it fails because something else is going to succeed for them instead."
- "Some might consider personal profit ("What's in it for me?") [that] overrides the larger company motive."
- "There are considerations, such as strategically involving the firm in certain activities, to attract or forestall takeover considerations or company reorganizations."
- "The successful project would lead to additional work on the part of the subversive stakeholder."
- "It will introduce a [new] learning curve into a procedure that is comfortable as it is."
- "The new system might make people more accountable."

Variations on the theme of conflicting interests range from the subversive stakeholder expecting additional workload to—the other extreme—losing the job.

Job Security. Many software projects need the cooperation and the constructive input of various groups of stakeholders in order to succeed. The persons who are performing the job at the moment are particularly important, especially at an early phase of the project. If they refuse positive cooperation, the project may run into serious trouble.

Quite a few software projects, however, make workers redundant. This is one way in which software projects can cut costs in the long run. In time, many of the dismissed workers find new job opportunities—perhaps even better than before. For the time in between, however, they are face trouble. Thus, it is more than understand-able that people fight against a software project if the most likely result is that they will be fired.

- "Concern about job security is one of the most common reasons we have seen as newly introduced systems would have eliminated many of their duties."
- "People whose jobs will be affected by the new system sometimes prefer to continue as they are, especially if they will have to relocate or lose their jobs."
- "Either they're comfortable with how things work now, or they're afraid of not doing well in the new environment, or they're afraid the new system will cost them their job."

Additional Workload and Unpleasant Working Conditions. Job security is only an issue for those who are affected. Others, however, might end up with a higher work load than before; this is a scenario that, in turn, might lead to overtime and worsened working conditions.

The following contributions provide some examples:

- "The successful project would lead to additional work for the subversive stakeholder."
- "Their goal was not to have much work with the project and not to take responsibility for something."
- "The software team had the goal to have everything with their technical platform. New service would disturb that easiness to maintain."
- "They have an economic interest in it (work shifts to them)."
- "It might introduce a learning curve into a procedure that's already comfortable."
- "They were scared and felt it would be too hard to be successful supporting the new system."
- "The stakeholders might see the project as being boring, causing them to work in a way they dislike (e.g., overtime) or working with parties they dislike."
- "Management's blind eye. If management is only paying attention to the dollars, and not the work environment, the workers themselves may determine their only way out is to cause the project to fail, losing the business, and thereby freeing them from the punishing environment."
- "They will not have to pay any cost for failure and may have no direct responsibility for the project, and yet the project might not succeed without their contribution. This can happen when individuals hold rare or poorly understood skills and management doesn't do 'capacity planning' for the person's time. Ultimately it leads to the person being overloaded when too many demands happen at the same time. This leads the person to flex their power to reduce the workload to a manageable level. The only problem is [that] this ends up undermining any projects that were overcommitted. Thus overwhelmed people with relatively unique skills can end up being subversive some of the time, especially around unexpected requests, or requests that show an utter lack of planning and foresight."

The last item gives an example of how difficult and how subjective the classification of "subversive behavior" can be. It might quite well happen that most team members regard one of their colleagues as "subversive" while this person himself might not have any bad intentions—he just does as much as he can do. For anything beyond his capacities he has no other choice but to say "No!" or delay tasks if a "No!" is not acceptable in this specific environment.

Resistance to Change. Change may lead to better opportunities in the long run. We all know, however, that change also has its challenges, risks, and hazards—and humans tend to take the line of least resistance.

- "The stakeholders wanted to keep the old software. (We suppose their motivation was that they wanted to avoid working hard and learning new technology)."
- "They are fed up with new projects, as the last projects failed to bring the promised benefit."
- "The stakeholder wanted to hide his incompetence. The project would make the lack of competence obvious."
- "Ninety-nine out of 100 people prefer to cling to familiar things rather than to try something new. At least this is my experience. Thus it is obvious that software projects which rely on many stakeholders are openly or covertly attacked to various degrees."

Shift of Power. Many software projects results in some persons are gaining power and others are losing power. The group which is about to lose power might try to disturb and subvert the project. Some responders reported such cases.

- "Why did they do it? Power."
- "They stand to lose (power/budget/money/pride) upon success."
- "The subversive stakeholder thought the outcome of the project might threaten their current standing in the organization."
- "The most heinous and explicitly identified acts of "sabotage" are performed by stakeholders who believe their position (viewpoint, opinion, pet feature) is at risk."
- "One memorable incident was [in relation to] a controller. My belief is that he saw how the financial system being implemented would reduce his power in the organization."
- "Loss of control over business processes which have been handled with own means so far. The project would result in dependency on third parties."
- "Before the project was developed the subversive stakeholder had exclusive access to certain resources within the organization. The new software makes these resources accessible for others."
- "The new project may diminish their importance or shift the power base."

The Project Entails Additional Control

- “A variation of losing power is that another gains additional control over my work.”
- “The project would allow additional control of the stakeholders work.”
- “The new system might make people more accountable.”
- “The software would allow insight into project details and organizational structures.”

Underdog Architects, Visionaries, and Prophets

- “They had proposed an alternative, which was rejected, and they believe that they will be exonerated at least or perhaps even gain praise or influence in the future. This is amplified if they were shamed or disturbed by how the decision was made.”
- “Some stakeholders (e.g., functional departments or customers) have unclear or diverting visions [that] to satisfy [all] in one project is not easy and can result in damage. Mostly it’s conflict of interest or conflicting objectives/visions. Sometimes it’s personal bias and the desire to prove a project will fail (‘In half [of a] year we will see that this was the wrong approach.’).”
- “The subversive stakeholders thought they should be more involved in certain aspects of the project and they didn’t want it to succeed without their contribution.”

Looking Good by Making Others Look Bad?

- “They want to create problems which only they can solve and gain importance.”
- “A very power-hungry employee who had a mix of motivations wanted others to look bad [and] cared more about being ‘proven right’ on various points than about project success.”
- “Mostly to demonstrate their personal superiority.”
- “The stakeholders sought to increase their share of the rewards, though the illusion of brilliance or through extending the work needed.”
- “The project involved someone who didn’t want me to look good. The method was to withhold information.”

Revenge and Disgruntled Employees. A widely agreed upon statement among many responders was the following: “The interests of the subversive stakeholders are better satisfied by the failure than by the success of the project.” (See also the anecdote by Chapter 9).

Even though it seems that this statement forms a generic pattern, from which many other motivations can be derived, it is only one side of the coin. The other side is that destructive behavior can also be motivated by irrational reasons that do not lead to any obvious advantages for the subversive stakeholder.

- "We've seen disgruntled employees who passively damage a project through bad attitude."
- "A middle manager had to leave the project against his will. This former stakeholder sought revenge and failure of the project."

Unwanted Competition Between Departments and Organizations

- "The subversive stakeholders did not agree with the charter or mission of a department and they 'hung 'em out to dry' without management support. Why? Competing incentive plans for upper management."
- "It was motivated by scapegoat strategies, i.e., if marketing wants to eventually blame development for a failed project all they have to do is insist on more requirements than can possibly be built given the schedule constraints. We have not been involved in many projects where there was a typical 'loser user' as defined by Gause and Weinberg."
- "The subversive stakeholder was from another department within our organization. He wanted to keep information close to the vest and provide the project only what he wanted the team to know in order to control the process. It was his way of trying to maintain some measure of control since he was no longer project lead."
- "The attackers didn't want to see [the] success of a different group."
- "The projects that attracted the attention of political opponents were all new projects developing new technology. The people who became political opponents of the projects all had older projects that could potentially be displaced."
- "Their own organization wanted something similar to the service that was developed. ([That is, it was a] struggle for power to be the leading part.)"
- "The subversive stakeholder was a customer who wanted to weasel out of a contract (changed their mind after signing)."
- "Product management [and] marketing representatives within engineering were associated with feature areas. Each fought to have their feature area advanced in each release. even without any correlation with true customer priorities."

Competition Between Individuals, Rivalry and Animosity. Whenever a project runs into a crisis, the position of project lead might become a subject of discussion. When the reputation of the project lead is destroyed the position may become vacant, hence opening new job opportunities for those who are not project leads at the moment.

- "The subversive stakeholder would like to be the project lead and gain total control."
- "The stakeholder had been passed over for a leadership role (in the project) in favor of an outside consultant."
- "The failure of one group may allow for new management to take over, and possibly change direction or do some empire building."

- "Personal animosity to the project leadership."
- "They'd developed some antipathy towards the contractor due to misunderstandings about the business arrangements made over their head and some unfortunate personality conflicts."
- "The project involved someone who didn't want me to look good. The method was to withhold information."

The following statements show that there is no clear-cut dividing line between uncalled for competition between individuals and competition between organizational units.

- "It was because the project was not 'theirs.' In other words, the project was created and motivated by somebody else in the company, someone whom they did not particularly wish to support."
- "Subversive people wanted the project manager on either the supplier's side or the client's side to have a failure. They would have sacrificed the project success for their own intrigues."
- "We have encountered managers of other projects who wanted a project to fail because they viewed it as competition."

Competition for Budget and Resources. A failed project is not necessarily a bad thing—at least not for everybody in the organization. When the project is cancelled, the budget that was allotted to a project becomes available and liable to a new allotment. Others in the organization, those who have not been officially involved in the project (and who do not have to pay for its failure) might be interested in that budget.

- "Internal budget competition."
- "There is a competitive world out there. There will always be competitive priorities and projects. There will always be turf wars. Budget cutting caused by stakeholders outside the project ('non-stakeholders') is probably the number one killer of good software."
- "Sometimes it happens in dysfunctional organizations (e.g., a line organization is not suitable for projects), where such subversion occurs with resource availability to projects."

Disagreement on Some Major Architectural or Technological Choice. This motivation has been reported in the context of the pattern of subversive subordinate team members and developers. Sometimes developers have a strong vision of what the "best" technical solution for a given problem looks like. The reasons for this suggestion may or may not be valid. They might be biased by lack of experience, by lack of relevant experience, by lack of overview of the political and financial background of the project, and—last but not least—by marketing efforts of technology providers. Nonetheless it is sometimes emotionally difficult for technologists to give up their vision (or parts of it) and yield to the decisions of bosses and bozos—decisions that they consider simply wrong.

- "We work with a lot of technical people, mainly programmers, and usually they become saboteurs when they do not want to work to some constraint, technical or otherwise, that has been imposed on the project. It may be something like he/she reads about a new piece of technology or software that he/she really wants to work on or it may be the desire to work to a different methodology than the rest of the team."
- "The stakeholder does not buy the idea."
- "Team members are forced to do a project they do not want to do, or they are forced to do it in a way they dislike to do it (e.g., using a certain technology)."
- "Developers whose ideas have been overruled will sometimes hope that the project fails, so they can feel they were proved right."
- "Ideological differences ([and] in [the]case of technical people, technical ideological differences)."
- "One possible case is where a developer or other staffer is ordered to do a project that for whatever reason they do not want to do. These projects are usually doomed to failure. Apprentice managers learn that you cannot order staff to do things they don't want to do."
- "Technical people, mainly programmers, become saboteurs when they do not want to work to some constraints, technical or otherwise, that have been imposed on the project. It may be something like this: He/she reads about a new piece of technology or software that he/she really wants to work on; or it may be the desire to work according to a different methodology than the rest of the team."
- "The subversive stakeholder wanted to come up with his own solution instead of buying one. So he fought against merely buying the-solution."

Disloyal Partners

- "Third parties are stakeholders, such as partner firms, clients, suppliers, vendors, and a host of others. They typically want a project to fail because it doesn't match their own objectives, or it depletes their resources, or they are not convinced of the benefits of the project. Other reasons can include misunderstanding of the project's objectives. Partner firms are the most common source of subversive elements in a project, in my opinion, because they are likely to resent the loss of their resources, will not likely see as many direct benefits as the party that initiated the project, will have a different culture and will likely not appreciate the project initiator's environment, for example."
- "The most serious examples we have encountered involved ourcustomer's organization: Often there was a "make versus buy" decision. The customer decided to buy our product instead of letting its staff create an in-house solution. So they did it because they hoped our implementation would fail and they could build their own system instead of learning our system.One customer had a hostile IT group. They just didn't [want] to maintain another system. They looked for excuse after excuse to unplug our system. In the end

the customer moved the maintenance of the system from one group to another internally. It seems like the hostile IT group got what it wanted: less work. Internally, product releases were a very political process with competing stakeholders."

- "Sometimes the customer consultant or product management or even individual engineers would blow requirements out of proportion. This also led to skewed priorities with too much time being spent on minor features. Or sometimes, [a major issue was that the project] could not adequately be staffed. Customer consultants would do this sometimes to try to make us fail, either so they could run their own internal project or sometimes just because they refused to compromise on changing existing internal practices."
- "In my opinion, partner firms are the most common source of subversive elements in a project. They are likely to resent the loss of their resources or they may not see as many direct benefits as the party that initiated the project. They may have a different culture and will not appreciate the project initiator's environment."
- "External consultants have changed scope needlessly in order to maximize their billable hours."
- "We have seen subversion in projects between companies. The motivation was that their own company could advance their own solutions without competition."

Split in Upper Management. The tale in Section 9.5 by Anonymous shows that subversive attacks are particularly dangerous if the attacker is a senior manager. According to the opinion of the responders, such attacks are frequently "successful"—that is, [they] end in disaster for the project. This pattern can occur in a context in which the senior management is split in two or more factions [and] are "at war with each other."

- "It can happen that senior managers have competing goals."
- "Senior management may work to discredit a project or remove its funding in an attempt to damage it for political reasons."
- "Management understaffing or underestimating—individual managers would intentionally underestimate work so they could understaff projects they didn't consider important. Again this was a way of undermining agreed upon priorities. Sometimes in collusion with product management. Sometimes they would commit adequate resources in planning but divert them after the project started."
- "They want to deliver a message only failure can achieve."

1.3.2 Sample Answers to the Question "How Were the Subversive Attacks Discovered?"

Here are sample answers to the question "How were the subversive attacks discovered?"

Some Attacks Are Carried out Overtly. Surprisingly enough some attacks are not secret: even persons who are not involved in the conspiracy know of the attacks. It may happen that the entire development team is aware of the subversion and know that the project is doomed to fail. However, the loyal stakeholders are unable to find a way to solve this problem. They might be lacking countervailing power, or the evidence might not be clear enough to address senior management.

- "None of the reported attacks were behind the scenes. The confrontation was out in the open, at least at my level. Not everyone in my organization had knowledge of the confrontation."
- "Attacks were done in the open via e-mail and forums (meetings) and in other private conversations, as we later found out."
- "They were pretty much in the open. [The] project was vulnerable to attacks due to scope-creep enlarging [the] project beyond performance capabilities. Client failed to transfer data correctly and needed a scapegoat, so the new system was identified as the problem; the contractor was paid, but ultimately twenty million dollars was wasted when entire venture was cancelled."
- "Since we was once part of the IT group and knew their procedures, it was very obvious to me that the reasons/causes of delays was abnormal; believable not to raise 'red flags' but very apparent to me."
- "Working with them we heard them expressing their resistance to the project quite openly."
- "They were pretty obvious about wanting it to fail. The attack wasn't all that hidden. Their agenda was well known."

We Found It out Later. In some cases, subversion could be fathomed to a certain extent; however, there was no clear evidence. Later it was indeed found out that the disturbance was in fact a deliberate and well planed action.

- "First we did not know if he did it due to incompetence or on purpose. Later it became clear that he did it deliberately, because he boasted about his tactic in private conversations."
- "It took time to discover what was going on. It was a pattern of behavior that identified the developer's issues. When the business lead was replaced, and the new person did not have [that agenda], … what had happened became apparent."
- "It started with unimportant decisions and rumors about negative talking of a certain person. But we [weren't] sure about the [subversion] before an important decision was delayed and negative."

Social Skills. Many responders to the survey reported that they rely on informal channels of information: friends among their colleagues and careful observation of behavior patterns. Many details are like the pieces of a puzzle: Each single piece of information does not say much; but several pieces come together to form a complete picture.

- "Subversive people rarely put their plans in writing; it's not like you can sneak into their cubicle, look under their keyboard, and find a mastermind plan written in crayon. Such plans are usually uncovered by bringing together datapoints from various groups—getting the whole picture, but from different perspectives."
- "First, the loyal stakeholders become suspicious as a consequence of rumors. Although rumors and doubts are not very reliable indicators of subversive attacks they give an indication that it might be worthwhile to have a closer look to this issue: You hear rumors—they are usually wrong but they indicate where you have to search."

Other responders however warned against an intensified feeling of distrust:

- "We think the project manager is in the best place to see subversion, but actively looking for it is likely to sow seeds of the subversion anyway."

Informal Network

- "We found it out by friendly talking to some reliable people who might have smelled trouble, but were frightened to report it on their own."
- "Among the most important sources are: word-of mouth, informal networks and hallway discussions outside team meetings."
- "The stakeholder will give trusted people a piece of information, and then they will pass it along to those who might be affected."
- "The attacker spread disinformation and negative stories about the project. These rumors finally reached the project team."
- "Finally asked a colleague who, it turned out, knew what was going on."
- "By speaking with other stakeholders. People are naturally sensitive to other stakeholders doing nonsensical or counteractive things. And they naturally compare notes. Such subversive elements **always** come out."

Careful Observation of Behavior

- "You know you've been subverted when…
    - You're given difficult goals by upper management and no way to accomplish them.
    - You're set up to fail in any of countless ways.
    - You don't find out about key objections by the stakeholder until it is too late to do anything about them.
    - There is a credibility gap with the stakeholder, with them denying verbal agreements that were made, or imagining different details in a conversation.
    - The stakeholder continues to change their mind, or delays providing their feedback at every stage.
    - The stakeholder speaks pleasantly to you, but when you aren't there they speak poorly of you or your project to influence others.

  - The stakeholder omits crucial information that might have saved a lot of time and effort.
  - The stakeholder lurks in the shadows until the project reaches a weak point, perhaps right after a bug has been found or there has been a delay in the schedule, and then unleashes an onslaught of negative criticism in the form of rants sent via private e-mails that end up in everybody's inbox."
- "Body language and other social hints given by the saboteur during meetings which gives me the idea to follow this suspicion more carefully."
- "A deliberate or accidental discovery while going though code repository in detail."
- "The person does not participate or provide relevant information when asked to."
- "At meetings in which decisions that had been made without full group participation are uncovered, or via other communications that reveal these prior decisions."
- "Letter sent a few levels above; clash during a meeting; attempt to hire project members."
- "People became unreasonable sticklers, rejecting solutions that were clearly superior to the ones that had been planned earlier in the project. They began to define "success" not in terms of the original project goals, but in terms of (often irrelevant) details. One person was doing incredible damage to morale: getting information from people, then using it to harm them; saying hurtful things to people in project meetings."
- "The subversive worked for me and we found out his feelings in personal conversations and meetings we conducted."
- "Information wasn't distributed by those subjects."
- "We became suspicious because of the project tracking. Late response; rejected product; withdrawn support."
- "The attacks were all political. For example, the opposing manager would attend design reviews and attack the design. They would attend management reviews and attack the product and its implementation."

It Is Not a Single Event; It Is a Process

- "It's rarely obvious. Most of the time you notice that things aren't going right but don't know why. Tasks aren't completed as planned. Quality of work is poor. Deliverables are not signed off by outside stakeholders. There are a lot of minor changes demanded continually."
- "Many small details form together a picture. In time, a pattern of behavior becomes more obvious."
- "You can notice the way people act. Project managers are not at all naive and know it. Of course, subversion is rarely written down in project reports."
- "Implicit conclusion during the attack (usually during meetings and presentations) and later on confirmation via informal network or background details (who is connected to who—the corporate social network)."

- “Personality conflicts are generally visible to people who pay attention in meetings.”
- “For instance, does the subversive element say one thing and do another? Does the subversive element tell you one thing and tell someone else something different? Can you find out how well the subversive element knows their domain, or is it an excuse to hide ignorance? Is there a power grab going on? Where do political winds blow? Is there a promotion, bonus, or performance numbers that make a nonsuccessful outcome more profitable? Is there retribution for some prior act? The rumor mills usually are wrong, but they are often right about where you should go to seek answers. Find out who is in the fold and who is excluded.”
- “It took time to discover what was going on. It was a pattern of behavior that identified the developer’s issues. When the business lead was replaced, and the new person did not have those agendas, then what had happened became apparent.”

Intervention of Senior Management. The first thing that springs to one’s mind is that senior management has to stop such processes. This however is not easily put into practice: frequently enough senior management is not even aware of the problems. Who should inform senior management and based on what kind of evidence? Subversive stakeholders generally use informal channels of information, which do not leave traces. What is more, stakeholders can easily present righteous and honorable justifications for their actions, apparently exonerating them from any feeling of distrust concerning their participation in a conspiracy.

Nevertheless the responders reported some cases where the way to senior management was the key to the solution.

- “The subversive manager had said there was no product, that the project was just wasting money on something that could never ship. Upper management at corporate HQ sent a fact-finding team to see whether there was an actual product. …They fired him.”

Project Audits

- “We think the best solution is a project audit. For large implementations across multiple divisions, implementation team members may make comparisons to determine if stakeholders are being ‘subversive’.”

Case-Specific Discoveries

- “The attacks were all political. For example, the opposing manager would attend design reviews and attack the design. They would attend management reviews and attack the product and its implementation.”

1.3.3 Sample Answers to the Question “How Can Projects be Defended Against Subversive Stakeholders?”

Here are sample answers to the question, “How can projects be defended against subversive stakeholders?”

Applying Quality Project Management Practices

- "The problem is in the definition—malicious sabotage is very rare. In those rare cases where an individual maliciously goes out to sabotage a project, a robust development process will self-correct and the individual is put in line. In fact, a robust development process keeps the potential for sabotage at a minimum. If a stakeholder is hell-bent on driving their agenda, a well defined development process has sufficient checks and balances to make sure this attempt is a) either unsuccessful or b) that the very real and appropriate stakeholder concerns are taken into consideration."
- "In a well managed company this sort of political in-fighting does not happen."
- "I think the project manager is in the best place to see subversion, but actively looking for it is likely to sow seeds of the subversion anyway."
- "Increased ability of project manager to understand situations end to end."
- "Acknowledge it and treat it as a real risk, then use risk analysis techniques to deal with it."
- "Better up front stakeholder analysis, casting a larger net to identify stakeholders, more responsive to stakeholder concerns, early and visible risk management, be more proactive in identifying stakeholder concerns as risks, client leadership taking more responsibility for project success."
- "Don't use system developments projects to solve management problems; the projects just magnify the management problems."
- "Choose the initial course of action very carefully, considering the why, what and how. Don't get locked into paths from which you can't recover from problems predictable from the outset. What is the organization's previous history? Count on it happening again."
- "Develop your team once you have the right people on board. This is a lot of work. It means making sure people are agreeing to all major decisions about the project all the time and communicating well. For instance, don't be surprised if you have a whole band of saboteurs when a major architectural decision is made without the team's entire consent. [Provide incentive.] Usually this is not material or monetary. Instead, give all the members of the team a chance to breath and enjoy their successes. Provide an environment of trust. Positive feedback is never a bad idea."
- "I have never seen measures taken specifically for the purpose of detecting project subversion. I believe that carefully designed project auditing procedures would be effective."
- "It depends on the power structure within the organization. If the subversive stakeholder is quite powerful, the project lead and loyal stakeholders may lack couter-vailing power. My experience is that project audits are especially useful in this situation, as they provide an objective, independent report to the project sponsor, along with findings and recommendations."
- "Strengthen relationships with party that paid for the project, a very influential party. Gain support from people that can influence the subversive stakeholder (in)directly."

- “Again, in a well managed company this sort of political infighting does not happen.”
- “Write good specifications for the project and involve the users/customers in writing the specifications. I use the ivy hooks method of writing specs which means for every specification there is a rationale for the spec and a way to verify the spec was met. I have found that involving subversives in the spec writing process, especially having them provide the rationale for a spec both captures, expert’s knowledge and reduces the resistance to change from the subversive.”
- “Involve users—including subversives—in the software development process. Have them critique screens you develop and make them test users of the new system.”
- “Adopt the Six Sigma team approach to projects. A black belt (project leader) sets up a team including users/customers and they follow a set of steps in doing the project. These steps include define (define the project and determine the risks to the business), measure (set goals for the project and permanent methods to measure the results of the project), analyze (study to find best solution for the project), improve (implement the project), control (make sure the gains made by the project are maintained over time). GE and Caterpillar [are] the two most famous companies I am aware of that successfully utilize 6 Sigma methodology. Motorola initiated 6 Sigma but dropped it I believe due to company financial difficulties.”
- “Against subversive project leads only a new project team can help. Against persons in ‘lower’ position a project team can build collateral structures by setting up information correspondingly.”
- “Expect it and set up processes to protect yourself against it. For example, I had one senior manager who didn’t think a project owned by another senior manager was important, but he needed to sign off on the deliverables. Knowing this ahead of time, I inserted a statement in the management kickoff meeting that unless a deliverable is approved or rejected by management within three days, it is assumed to be approved.”
- “A clear project plan with roles and responsibility is needed to define who does what. Without this, there may be no difference between subversion and misguided efforts. I think the project manager is in the best place to see subversion, but actively looking for it is likely to sow seeds of the subversion anyway. Probably regular one-on-one meetings between the [project manager] and each stakeholder to allow stakeholder concerns/problems to be voiced will prevent passive subversion and should allow the [project manager] to find active subversion over time.”
- “By routine examination of work and peer review. The more that someone tries to shield their work from such examinations the harder everyone else should push to expose that work. Secrecy is rarely in the public good.”
- “Leadership. Open communication of goals and progress. Welcome other people’s ideas and discuss them fully. Manage the impact on affected staff sensitively and openly and generously.”

- “Better integration of all user requirements. Tighter, centralized project management.”
- “Awareness. People need to be aware it can happen, so they are on guard and recognize the symptoms.”
- “The project lead must immediately deal with developers and other contributing elements to keep them producing, and be prepared to replace any element that is not functioning as it should. Loyal management must use the political environment to manipulate the situation when other subversive management peers are identified. Management and developers must be vigilant against anything less than excellence from the project lead. Management in particular must make the project and project lead synonymous within the corporate environment to ensure that the project lead is inexorably tied to the project’s success.”

Quality Communication

- “Communication is the key to reducing people’s feelings of disenfranchisement and alienation. If an individual does not believe s/he has a voice in the decision making process, s/he will find subversive ways to get their agenda pushed. If the development environment does not provide a relatively risk-free context in which people are allowed to express their convictions, then “sabotage” is only one of the probable outcomes.”
- “I think a healthy and open team atmosphere is the best way to avoid subversion and sabotage.”
- “Provide for full visibility within the project.”
- “My experience is that project audits are especially useful in this situation, as they provide an objective, independent report to the project sponsor, along with findings and recommendations.”
- “Inform stakeholders about real events / status / results of the project to tackle misinformation. Strengthen relationships with the party that paid for the project, a very influential party. Gain support from people who can influence the subversive stakeholder (in)directly.”
- “Expose some of the subversive actions. This, however, is not always easy to do—depending on the respective relationship between stakeholders.”
- “Communicate the project progress and minor successes. Install a project leading committee which involves important managers with power. Talk to the subversive stakeholders openly.
    - Escalation 1: Discuss[ing], expression of empathy and searching together for solutions.
    - Escalation 2: Project lead submits clear statement regarding the goals and the importance of the project.
    - Escalation 3: Senior management or steering committee submits a statement regarding the goals and the importance of the project.
    - Escalation 4: Overt statement of the steering committe/senior management: The success of the project is more important for us than your contribution.

  - ◦ Escalation 5: Replace the stakeholder. (This I have seen only once because Escalation 4 usually performs miracles.)”

- “Keep IT and process control individuals together in groups (as much as possible). This gives ownership to all involved and everyone has a stake in the success, or failure, of the project.”
- “In the case of coding sabotage, by having individuals ‘overlap’ module responsibility will help prevent deliberate sabotage, as well as inadvertent bugs.”
- “Do your requirements analysis. Also, figure out who the stakeholders are and map out whether they are positively or negatively disposed to the project. Work to influence negative stakeholders by getting their peers and others around them to influence the negative stakeholder. Turn negative stakeholders into positive stakeholders by making sure their needs are accounted for. Also, let some of the ideas be theirs so they feel like they have made a contribution and are invested, at least psychologically, in the success of the project.”
- “Give always full visibility.”
- “Portfolio management on high level, combined teams with different stakeholders aligned on a shared vision; balanced scorecard approach.”
- “Facilitated workshops to charter the project at the beginning.
  - ◦ Creating role ‘pointers’ which each person creates and discusses as a group stating what their role is, what they expect and need from others, how they will interact with others who depend on their work.
  - ◦ Creating team working agreements at the start, and periodically checking on how they are working and what could be revised.
  - ◦ Creating sponsorship agreements (for how sponsors will actually sponsor the project)
  - ◦ Daily scrum meetings for status stuff.
  - ◦ Having a well-planned, collaborative requirements process which uses early and continual direct involvement from users and subject matter experts.
  - ◦ Ongoing use of well-run inspections and reviews of key deliverables beginning with plans and requirements (so defects can be surfaced early with the right people).
  - ◦ Ongoing use of well-run interim project retrospectives (at the end of each iteration, release, period of time or milestone).
  - ◦ Frequently social activities whereby the team—customer and IT—share food together (onsite and offsite) to build trust and genuine caring.”
- “Work to transparency; when everything is transparent, it is harder to hide.
- “Inform stakeholders about real events / status/ results of the project to tackle misinformation.”
- “Encourage active involvement, get them to feel a true sense of ‘ownership’, both by being financially involved in the company and by having an element to be proud of their work. Also, encourage better communication skills.”

  - ◦ Escalation 1. Convince the stakeholder (if ideological or technical based)
  - ◦ Escalation 2. Comfort the stakeholder (if economic or power based) or offer pacifiers
  - ◦ Escalation 3. Eliminate the stakeholder
  - ◦ Escalation 4. Bring in an external mediator—mostly pre-emptive (assuming that we know about the attack)
  - ◦ Escalation 5. Die together—kill the entire initiative and wait for the corporate dynamics to change before bringing it back again.

Psychology

- "A certain amount of prevention of employee subversion can be accomplished by making sure the hiring process is as concerned with personalities as with technical skills."
- "Have some psychological savvy into picking team members. If two plus two don't add up: what a person says and how they perform, then be suspect and follow up on those concerns."
- "Awareness—people need to be aware it can happen, so they are on guard and recognize the symptoms."
- "Very, very, very carefully screen technical people when you hire them. You must not overlook the social and personal traits of a person in this position (a typical mistake for people doing hiring in my field). Some people are absolutely brilliant technicians on the surface but are extremely selfish primadonnas underneath and this is the most common style of subversion in an IT project."

Support from Senior Management

- "Get support/action from as higher in the organization as possible."
- "In my case senior management intervened and changed the responsibilities"

Taming ...

- "Thorough inclusion of the potential subversive stakeholders."
- "It is important to work with them and not against them. To make them see how they can contribute to the project, and how they may benefit from it. In many cases the right approach may change their attitude."
- "Convince the stakeholder (if ideological or technical based)."
- "Comfort the stakeholder (if economic or power based) or offer pacifiers."
- "At least early information, yet better is early and thorough inclusion of the potential subversive stakeholders."
- "Make the subversive the project leader. The subversive won't be able to complain about the project after it is completed since they were in charge of the project."

… Or Fighting Back—If Taming Fails

- "Work around that person. Continue not to involve him or eliminate the stakeholder."
- "Proof destructive nature of attack."
- "Expose some of the subversive actions. This, however, is not always easy to do depending on the respective relationship between stakeholders."
- "Every stakeholder should be given ownership (from the sponsor down to the developer)—and by ownership, have a reward for success and a punishment for failure. This keeps the group's vested interest focused on the success of the project. If someone starts to subversion practices, it will be noticed sooner and called out. The subversive element should be dismissed from the project and management made aware of what and why."
- "The division president fired him."
- "Get support/action from higher in the organization if possible."

Pessimistic Opinions

- "You can't fully defend any project against sabotage, whether from within or without. You can pay attention to the issues that arise as the project progresses. You can keep in mind the simple maxim: A projects greatest challenge is too much success. Successful project teams behave a lot like successful rock bands. Everyone gets an ego. Everyone falls victim to the fundamental attribution error and assumes that everything that goes right on the project was a result of their work; that everything that goes wrong on a project is somebody else's fault. I see more problems with personality conflicts and self-promotion on successful projects than on others. The best thing you can do to fight this is to work constantly to create and maintain a sense of the team and of team accomplishment while keeping a lookout for personality issues. Bring in the psychologists and team motivators while things are going well. If they go badly it is often too late."
- "It's really hard to know how to deal with this. In my case, there was probably nothing I could have done, except perhaps to get all tasks to be performed and the reasons for performing them in writing."
- "If the subversive stakeholder is quite powerful, the project lead and loyal stakeholders may lack countervailing power."
- "There is no general protection of the project. If the attack is based on disinformation and bad stories some protection is possible if all information is shared project-wide."
- "There is no solution, not in the environment I work in."
- "Communicate the project progress and minor successes. Install a project leading committee which involves important managers with power. Talk to the subversive stakeholders openly. But in fact I must admit that all this never worked thoroughly because the subversion was not evident enough to really fight against or to exchange the subversive stakeholder against a more positive one."

- "In that scenario, the problem was essentially resource acquisition. It failed because no stakeholder had authority or inclination to compel."
- "I have tried several defense-alternatives. However, I must admit that they never worked thoroughly because the subversion was not evident enough to really fight against."

1.4 A FOLLOW-UP TO THE SURVEY: SOME HYPOTHESES AND RELATED SURVEY FINDINGS

How Did This Material Come Into Existence? When studying the first set of responses (summarized in Section 1.2), we noticed that certain statements appeared time and time again in the answers. These statements formed a starting point for what we thought should finally be a kind of "quantified consensus" among the responders of the survey. So we decided to conduct a second-round survey regarding the perceived validity of those statements. We present those statements below as hypotheses, each with the second-round survey responses regarding their validity.

Some hypotheses (such as Number 1 and 2, below) appeared in some of the responses. Some responders emphasized their confidence in the validity of the hypothesis enthusiastically, while others did not mention this hypothesis at all, or they even expressed their doubts. So we included these statements to get a hard number regarding what we had here: a consensus, a controversy—or a fallacy?

A few hypotheses appeared only in a single response (for example, Number 8, below). However, the responders included interesting anecdotes or other thoughts that convinced us that it was worthwhile to have a closer look.

We added another few hypotheses from our own experience. However, the vast majority of them were extracted from the contributions of responders (although we had to change the wording in most cases). These considerations led to a set of 22 hypotheses that we sent back to the responders, asking them to assess the hypotheses. The rating for each hypothesis is a number between 0 and 10. In this range, "0" means completely wrong, and "10" means completely true. The responders left questions unanswered if they did not have an opinion or had no relevant experience.

We calculated the median as the center of the random distribution. The median is a number chosen in a way that half of the responders' ratings are equal or higher than the median and the other half of the ratings are equal or lower than the median. In statistics, it is known that the median is more robust against outliers (that is, values far away from the ordinary) than the arithmetic average. Since we do not have a reliable hypothesis regarding the random distribution of the ratings, the median seemed to be more suitable than the arithmetic average.

The ratings for each hypothesis are summarized in the tables, below. The second line of the table shows the number of responders who gave the corresponding rating (shown in the first line.) For example, in Hypothesis 1, four responders gave the rating "7." The lower half of the table summarizes the results of the upper half. The fourth line shows the number of responders who gave a rating in the interval indicated on the third line. For example, in Hypothesis 1, eight responders gave a rating in the interval “0” to “3” (that is, they expressed their doubts regarding this hypothesis).

Some responders included additional explanations in their responses. If we encountered an opinion that was out of the ordinary, we asked for confirmation and more explanations (to exclude the possibility of a typo). We allowed more space for these opinions, which were somehow different from the ordinary, for the following reasons:

- These opinions might give some insight of issues the majority is not aware of.
- Hypotheses which are supported by the majority of responders are quite likely to also be acceptable for many readers. The interesting point is: what objections are there against these (apparently) obvious statements.

Hypothesis 1—Median Rating: 8 Subversive behavior happens mainly in a dysfunctional environment, that is, when the management processes of the organizational unit are somehow wrongly defined. A robust development process keeps the potential for sabotage to a minimum.

TABLE 1.3

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	4	1	1	2	1	2	1	4	11	2	7	1
Rating	0–3				4–6			7–10				?
Num Part.	8				4			24				1

Responder's Rating [0]: “According to my experience, subversive behavior is more likely to be successful in a dysfunctional organization because there is no strong process to prevent it. However, it is just as likely to be attempted in even the most functional organizations. Subversive behaviors take place among individuals, and you are likely to find them anyplace.

The most dysfunctional organization I've ever worked with is a California Life Insurance Company, where I created their program technology office. The CIO created an atmosphere of finger-pointing and blaming other people for problems by screaming at them in public meetings. I saw more than one long-time employee leave a meeting in tears after being screamed at. Subversive activities were normal, so that people could avoid blame. But everyone knew this was going on, and expected it.

One of the most functional organizations I worked at was financial services department of a large car producer. I developed the PMO for them and organized their project management processes. But even there, I could see a couple of mid-level functional managers who would agree with people in project meetings but then go around afterwards and criticize the project. This was more subtle and difficult to counteract. Company cultures don't create sabotage, people do. And you find these people in every type of company.”

Responder's Rating [0]: “Let's first define a dysfunctional environment. A broad definition would be an environment that lacks leadership and direction, lack of specific functionality specifications, and a lack of (programming and analysis) standards.

The 'leadership and direction' can be lacking and still have a good deliverable if the staff is good. So, let's examine the remaining two elements.

1. Lack of specific functionality specs. Of course and obviously, if the programmer instruction is ambiguous he may interpret the functionality in many (of his own) ways, and if his intent is detrimental to the cause, much complicated code can be created to easily mask intentional and harmful code. Which leads to the next and most important element.
2. Lack of standards. One of the most important features given to us by language developers (VB, C, etc.) is the ability to insert comments in the code. Good code standards require heavy commenting by the code developers. I personally have little use for hard-copy flow charts (except during system design). After the coding starts, I demand pseudo-flow comments in every routine. Basically, this means that the coder first enters comments describing every intimate step of the routine. When finished, the code is entered following each comment. This ensures anybody reading the routines can quickly understand the coder's intent and recognize 'unusual' entries.

   Also, I tend to restrict the overuse of called functions. If a function is to be used again, then it's necessary. But many programmers (especially the old C programmers) design all code in functions, whether or not is used again. In turn, many of these functions call other 'single-use' functions, and so on. This makes the code incredibly hard to follow and thus makes it easier to make mistakes (?). KISS is the rule here (Keep It Simple, Stupid)

   So far, this brief describes what a programmer can do to harm the project. You could substitute 'programmer' with 'business analyst' and change 'code' to 'functional specs.' Again, if no standards are available (or strong leadership), all sorts of 'misinterpretations' can be generated.

   Weak leadership is similar to weak parenting. If a staffer thinks they can get away with their agenda, they may try. Not that I condone 'Gestapo' tactics, but a firm hand on the wheel can prevent accidents."

Responder's Rating [0]: "It strongly depends on the definition of 'dysfunctional environment' that people have in mind. Wrongly defined management processes are a potential part of the problem. I think if you would do a root-cause analysis of the problem you get a picture that is something like this:

- Ingredients that are a must for subversive stakeholders to appear: environment that allows this kind of behavior. This has to do with a combination of unclear or wrong policies or management processes, less attention of people in charge, need for people to derail a project.
- [A] must is also a person or group of people that have a somewhat lower ethical standard 'winning at all costs.'
- Also a kind of stick to hit the project is necessary."

Responder's Rating [0]: "Obviously not true. Not all dysfunctional environments have subversive elements, consider the case of two business partners who don't know jack, but want very badly to succeed. Or, consider the environment which is not dysfunctional but filled with talented individuals; as such, I rewarded them with a $100 bonus for every bug they fix: what happens? They get sloppy, introducing bugs so they can fix them and write themselves bonuses. It is the incentive that caused the problem, not a dysfunctional environment. Is it easier to hide subversive behavior in a dysfunctional environment? Absolutely, but that isn't what was asked."

Responder's Rating [1]: "I do agree that a robust development process keeps the 'potential' for sabotage (I would add 'potentially' here as well) at a minimum. In this case 'development process' means a 'standardized' system/application development life cycle that is integrated with a quality assurance process.

However, I still believe that sabotage of varying levels happens in any environment. I was not clear what you meant by 'dysfunctional'—if that meant not having standards and regulated processes, or if it was referring to a human level of interaction based upon some organizational disparities that creates a higher potential for a 'breeding ground,' if you will, [for] the sabotage.

In either case, I feel that the human element in projects and the smooth accomplishment of processes, with or without standards is so huge that I was unable to narrow its potential to that one view or definition. Hence, the number '1.'

In my view, sabotage can be passive or active. For example, if you ask a developer for an intermediate progress report and they tell you that they will not give you that information: i.e., don't worry about it, I'll have it done by the (final) due date. I view that as passive sabotage. It blocks the project manager's ability to correctly, let alone accurately, track progress.

So, without knowing more of the definition of 'dysfunctional' I would stay with my number (not a typo) because of that human element and the existence of both passive and active sabotage."

Responder's Rating [2]: "Sabotage is at different levels—ideation and project initiation stage, and project execution stage. At the ideation and project initiation stage there are a lot more political impacts than technical impacts. Development processes have less influence on pre-'go-no-go' stage of the project."

Responder's Rating [4]: "I'm willing to grant that a dysfunctional environment may encourage subversive acts, so I won't say the hypothesis is wrong, but I object strenuously to the inclusion of the word "mainly". Subversion, as you appear to define it, can happen anywhere. Sometimes, moreover, it is a good thing. Some ideas are zealously pursued even though they are inherently bad, unethical, or dangerous to a business.

Subverting those projects is probably a good thing, and is more likely in a particular kind of dysfunctional environment: one that stifles disagreement and the presentation of alternatives. One notes again the fine line between subversion and conscientious disagreement. The managers who create this kind of dysfunctional environment would not, in general, regard it as dysfunctional. Indeed, they would regard an environment that encourages conscientious disagreement as dysfunctional because, among other things, decisions take too long (which is the nice way of saying 'my opinion is right and any discussion that might show that my opinion is not right is dysfunctional'). Employees whose disagreement is stifled, by contrast, are likely to regard this kind of environment as dysfunctional, and if they can leave they will."

Responder's Rating [6]: "When subversive behavior happens in a functional environment, it can make the environment dysfunctional very quickly."

Responder's Rating [7]: "Yes…but the minimum is still quite a bit."

Responder's Rating [8]: "—although this may be a truism."

Responder's Rating [10]: "Right on! '10.' I completely agree, and this is a strong thesis point! I cannot emphasize it enough: subversive behavior is one of the unhealthy coping mechanisms of people caught in unhealthy environments. Healthy people in healthy environments are too busy being creative and getting work done to bother with subversion."

Hypothesis 2—Median Rating: 7 The organization can be structured in a way so that subversive stakeholders are not tolerated.

TABLE 1.4

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	3	2	2	1	1	8	0	3	5	4	6	2
Rating	0–3				4–6			7–10				?
Num Part.	8				9			18				2

Responder's Rating [0]: "There is always a subversive behavior from one perspective or another."

Responder's Rating [0]: "Some subversive stakeholders may take the company in new positive and productive directions that were never originally conceived, just like beneficial mutations, evolutions in biology. Nature abhors a dogma."

Responder's Rating [1]: "There are many ways in which people can subvert projects. I have never seen any effective protection against all possible subversions, especially those by managers."

Responder's Rating [2]: "Not the structure, but the coherence of the management as a group can make them responsive to subversion."

Responder's Rating [9]: "I agree mostly. The reason it doesn't get a '10' is that even in very open organizations, some areas are more transparent than others.

Influence can still be gamed, and there are still personal reasons for opposition, such as ownership, control, and who has to rewrite their stuff."

Responder's Rating [9]: "Absolutely. If you don't reward subversive behavior, which means getting rid of performance evaluations and rewarding based upon when the whole is delivered, you make everyone accountable and they police themselves. Will corporations do this? Often not. The subversive element realizes this takes money from their pocket, so if you have a subversive element in upper management, you can't get the change through."

Responder's Rating [10]: "This is absolutely correct, but there is a huge danger in at least some approaches to doing so. The line between conscientious disagreement and subversion can be largely a matter of perception. If one is intolerant of disagreement, one can easily create an environment of groupthink and make huge mistakes as a result. One might easily argue that recent NASA space shuttle disasters are the direct result of an inattention to subversive stakeholders."

Responder's Rating [10]: "Completely true. Subversive stakeholders are rare enough that they can be eliminated in a process that makes an example of them to other potential subversives."

Hypothesis 3—Median Rating: 6 The size of the organization has a strong influence on the frequency of subversive behavior.

TABLE 1.5

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	3	1	1	1	2	3	7	3	7	1	3	5
Rating	0–3				4–6			7–10				?
Num Part.	6				12			14				5

Responder's Rating [0]: "The two most subversion-attracting organizations I can think of immediately are marriage and the telephone company, particularly before the breakup. Perhaps the CIA, or any other agency of enforcement, has a few less subversive stakeholders than the phone company."

Responder's Rating [4]: "I agree only somewhat. Small organizations can become very unhealthy, in ways a larger organization would have a hard time sustaining. So, small orgs can be more vulnerable because they may be more unhealthy. A large enough organization has a hard time staying healthy, especially if there is stagnation in the business. A thriving business gets to create new parts of the organization, which is easier than transforming an existing organization into something different. So a stagnant org has an increasing chance of becoming unhealthy during stagnant times. And, since 'what goes up must come down,' there must necessarily be a plateau or decline for any company. Honestly though, any company that big is bound to have pockets of unhealthiness which could stimulate subversive behavior."

Responder's Rating [6]: "It is certainly the case that the likelihood of subversive acts increases as the number of stakeholders who are invested in other solutions increases, but the kind of subversion that is presented in these questions can happen in any organization."

Responder's Rating [6]: "Subversive behavior correlates with number of concurrent but not coincident projects."

Responder's Rating [8]: "Clearly. The more people in the mix, the greater the statistical likelihood you'll encounter a subversive person. The more people in the organization, the more you get people who don't have jobs producing, but who are being measured on some other criteria. I wonder if people aren't malicious, but greedy."

Responder's Rating [8]: "The larger the organization, the more people are treated by rules, the more lower level management there is that wants to get higher up and the less control by senior management there is over these lower level managers. The lower level manager has a sense of 'power' and will use that to get up higher."

Hypothesis 4—Median Rating: 6.5 Subversive behavior happens more frequently in large organizations

TABLE 1.6

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	3	1	1	4	0	4	4	3	7	3	4	3
Rating	0–3				4–6			7–10				?
Num Part.	9				8			17				3

Responder's Rating [3]: "I agree only somewhat. There are factors that lead a small org to suffer subversive behavior, and other factors that lead a large org to suffer subversive behavior."

Responder's Rating [3]: "I don't think so. Large organizations don't get to be large organizations without finding ways to inoculate themselves against internal threats."

Responder's Rating [5]: "More likely due to numbers, but I suspect it is more a matter of complexity and rewards, than sheer volume. One needs to ask, if this person were to over-achieve in the areas he's being rewarded for, does his success put him at odds with the company goal or hurt the company overall?"

Responder's Rating [10]: "Large organizations are bad. Even worse are multi-part organizations, such as where one firm is in charge of the project and other firms are involved (e.g., closely-allied partners or other firms that share some or all of the project owner's ownership)."

Hypothesis 5—Median Rating: 7 Subversive behavior is rare and unlikely to succeed if the project lead is "strong" (such as professionally qualified, strong personality, trusted by the top management).

TABLE 1.7

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	1	3	2	2	0	7	2	4	6	4	4	2
Rating	0–3				4–6			7–10				?
Num Part.	8				9			18				2

Responder's Rating [2]: "It is less likely, but as a whole you're only going to focus on a localized group within the process. The best development efforts can be entirely undone by upper management shuffling a budget. How many great products can you think of that totally died because the CEO suddenly decided to liquidate and get out?"

Responder's Rating [5]: "I don't know how I feel about this one. I guess a lot depends on how you define 'strong'. Strong leadership that is intolerant of disagreement risks groupthink and backchannel subversion. Strong leadership that treats programming teams like 'mushrooms,' gives employees little ability to either exercise or perceive disagreement, pretty much takes subversion out of the equation (along with creativity or the power to identify and proactively fix problems). Strong leadership that facilitates discussion of the problem, the requirements, and the solution such that it creates team buy in is probably the most likely to avoid real subversion, but 'strong,' in this case, is a set of people skills rather than a set of powers."

Responder's Rating [7]: "I agree. There are many factors that may be out of the control or influence of the project lead. However, if you extend that to mean all management from the project lead up to the CEO, then I'd give it a '9.' The only reason it can't get a '10' is that personal issues can still lead to internal business conflict. People have their own personal motivations and interests that are oblique to everyone else and the company."

Responder's Rating [7]: "It is rare. It can sometimes succeed if the subversive is stronger. Trust by top management is irrelevant."

Responder's Rating [8]: "This is largely correct. These traits (especially the last) are important in minimizing/mitigating subversive behavior."

Responder's Rating [9]: "If the project lead is openly trusted by top management there is much less likely to be subversion. Much subversive behavior is decreased or eliminated when the subversive stakeholder knows that there may be negative consequences of subverting someone in management's favor."

Hypothesis 6—Median Rating: 5 Female project leads are more frequently attacked than their male colleagues.

TABLE 1.8

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	2	0	3	4	2	6	0	5	3	1	0	11
Rating	0–3				4–6			7–10				?
Num Part.	9				8			9				11

This statement has been included because a certain responder of the survey was rather convinced that in her case the gender had a strong influence. The results, however, do not indicate a compelling conclusion. Some few responders confirmed the hypothesis while others expressed their doubts. The high number of responders who abstained is particularly striking.

This issue might need another setting to be analyzed thoroughly.

Male Responder's Rating [?]: "Females often believe they have to prove themselves more/harder than their male colleagues. That may or may not be true, I don't know but this in itself makes them less respected. Personally, I believe a project can be run [in a maternal or paternal manner] with equal results, but 'ma' wanting to be 'pa' doesn't work."

Male Responder's Rating [0]: "I don't see gender as playing a role at all, and have had quite a number of very competent and talented female project leads. There are two possibilities that might be worth exploring: 1) Is this a self persecution complex? Every group feels that it is at the disadvantaged state because the grass always looks greener. Stating the same statement, but substituting in skin color, age, political belief, or religion would most likely get the same degree of passion from the speaker. 2) I have noticed that with some number of women they think in order to complete in a 'man's' world of business that they need to act like a bitch to get respect. Obviously, any inappropriate and unprofessional behavior isn't supportive and will generate ill-will and conflict. True, men can compartmentalize; Bob can tell Dave that he's not carrying his load and is being laid off, Dave gets it without insult, both opt for going out to lunch, and Dave buys Bob a beer. Working relationships are different from friendship ones. I've had a number of women admit to me their gender just can't do that well. It's foreign to them."

Male Responder's Rating [3]: "I can see how this could be a factor, but I cannot say 'more frequently.'"

Female Responder's Rating [5]: "This is valid only in cultures where being male presents a clear and effective leadership advantage."

Male Responder's Rating [7]: "This is a gut feeling on my part."

Male Responder's Rating [7]: "I agree. Some men can be such pigs… Successful female managers can be extremely competent communicators, and have their own arsenal of techniques for dealing with people who cross boundaries. But these kinds of subversive behavior are incredibly costly for the company, because it can lead to lawsuits. It may be easy to show in a court of law that it was sexual harassment. Therefore, in an otherwise healthy organization, this kind of subversive behavior is inherently weak, because if it is exposed the full weight of the company must necessarily side with the female employee, or the company may suffer even worse consequences. Thus, it is weak sabotage, destined to fail, and a strong female manager knows that as long as she sticks to the facts and is competent, the weak subversions will fall by the wayside. So, there is an odd twist to some degree with female managers in some situations, it can also be used to an advantage, as a kind of hysteresis. In other words, it might be easier to launch a subversive attack, but it is inherently weaker. It kinda caps your risk because if the female manager is obviously subverted, she probably will raise the issue with her management, and the subversion will end. Also, some women are naturally collaborative, and that tends to play against subversion in general. That said, some males interact in ways that are more aligned with how females are described above. Similarly, some women interact in ways that are more typically male. Rather than pin behavior to specific body configurations, I prefer to consider how individual personality traits induce or reduce subversion. For example, anyone using an emotional basis for influence is likely to induce subversion. Whereas, using a transparent, logical basis for influence is more likely to reduce subversion. However, someone who is aggressive or strong willed may engender subversion because people are afraid to confront the person directly."

Female Responder's Rating [7]: "This is an interesting question. And a difficult one as well. My gut-feeling is that this hypothesis deserves a '10.' However I can speak only from my own personal experience and do not have an overview of the situation. For this reason I only gave here a '7.'

It is quite possible that women just perceive subversion more intensely because they are more sensitive and they have higher standards of collaboration. In some organizations the subordinates accept only a tough, almost brutal, leadership style. Since I'm not a manager of this kind they interpreted my management style as 'weakness.' So I had to adopt a tough style to get things done.

In addition I'm not even sure that women are more frequently attacked by subversive stakeholders. Anyway, this is certainly not a strict rule—perhaps on an average.

However, I think that persons with a female style of leadership encounter more problems of this kind."

Male Responder's Rating [7]: "This may be true to some extent, but even if it isn't, it is likely to be perceived to be true, especially by female project leads. This is far from a universal truth, but I have certainly encountered female managers and project leads that viewed any disagreement to be an attack, not just on their leadership capabilities, but on the notion that women can be effective managers.

I don't want to oversimplify here. I have encountered many female project leads and promoted a few myself. Most simply did their job. A few were very sensitive to anything that they perceived as undermining their authority. That's true of men as well, but men never attributed the attacks to their being male. They usually attributed it to a lack of loyalty or an inability to be a team player. My point, I guess, is that this may be more a matter of perception than reality. On the other hand, there are some genuinely sexist guys out there."

Male Responder's Rating [9]: "IT is, unfortunately, still sexist. I have no doubt that this leads to **more** subversion of females than of males, even if the difference is small."

Hypothesis 7—Median Rating: 5 Subversive behavior is usually against people, not against projects.

TABLE 1.9

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	6	0	3	3	1	13	2	2	3	2	1	1
Rating	0–3				4–6			7–10				?
Num Part.	12				16			8				1

Responder's Rating [0]: "No. By definition. We are talking about subversion of the projects. The methods employed may include attacks on the personnel involved in the project. It may frequently include that, for all I know."

Responder's Rating [3]: "Often it is about job security and others."

Responder's Rating [5]: "I agree somewhat. Actually, projects are quite crucial. If a project decides to go in one direction, that may orphan or obsolete someone's primary responsibilities and software. There are often two ways that will both work. So the decision gets made on other factors. Then it can get really nasty…"

Responder's Rating [5]: "Equal."

Responder's Rating [5]: "Both. I've seen projects suffer because of someone's personal gain. I've seen a director set up and attack a subordinate in a public meeting because at some point in the past he accidentally surfaced some material that she didn't know the answer to (that she should have)."

Responder's Rating [5]: "It is often the case but not 'usually'."

Responder's Rating [10]: "I was at least one of the people who suggested this, and I still agree, but I start from a perspective, which I don't see reflected in your questions, that there is a difference between subversion and disagreement. When we disagree with people, it is most often because we disagree with them about an issue that relates to the project. When we subvert them, it is because we don't like them. When we disagree about a project, it is generally because we have the ability to do so in an environment where our disagreements will be considered. It is only when we are unable to have our disagreements with a project considered that people subvert projects."

Hypothesis 8—Median Rating: 9 Attacks from a user base or a client can be very effective if coordinated.

TABLE 1.10

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	0	0	0	1	0	3	8	5	14	6
Rating	0–3				4–6			7–10				?
Num Part.	0				1			30				6

Responder's Rating [7]: "Company XYZ wants to revamp its internal software, so it contracts out to have some new software made which will keep track and make people more accountable. Employees at XYZ either perceive or learn through the grape vine that the new software will require them to work harder and be more accountable. So there is an instant disposition not to want to use it. The contracting company delivers the perfect software on time and under budget, it does everything right. Users at XYZ make up complaints that the new software isn't like the old software, and within 72 hours refuse to use it. The users are the subversive element. Company XYZ now has a choice. Mandate that the users will use it (and start firing those who don't). Or, cancel the follow on development contract. Note: the subversive element is affecting the development but is not engaged in the process at all."

Responder's Rating [8]: "Yes, but it should be considered that the most fundamental act of any subversion that has any hope of working is some level of coordination. It is usually the person who is trying to subvert the project that is coordinating things. The people coordinated may well be unwilling dupes who have no idea how they are being used. This is fairly true, but it may not be terribly relevant."

Responder's Rating [9]: "Any coordinated attacks are much, much, much more effective."

Responder's Rating [10]: "I totally agree. But, then, I think I wrote that. ;-)
Yes, that's true. Thank you. Johann"

Hypothesis 9—Median Rating: 9 All subversive attacks disturb the project to some extent.

TABLE 1.11

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	2	0	3	2	3	4	5	15	2
Rating	0–3				4–6			7–10				?
Num Part.	3				5			27				2

Responder's Rating [3]: "Many subversive attacks have little impact on the project at all. Others ultimately kill the project."

Responder's Rating [8]: "Hard to imagine how they couldn't."

Responder's Rating [10]: "I totally agree. If nothing more measurable, then at the least it deflates the enthusiasm that makes people want to keep looking for a creative answer to their business problems."

Responder's Rating [10]: "Yep. Life disturbs the force of universal stasis. In fact, at many levels, growth and development can be equated with disruption."

Responder's Rating [10]: "Absolutely, because it's just one more thing that needs to be dealt with by someone who could be doing something else more productive."

Hypothesis 10—Median Rating: 4.5 Carefully screening of people when they are hired is an efficient defense against subversive behavior. The personalities, the social and personal traits of a person, are equally important to the technical skills.

TABLE 1.12

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	4	2	6	5	1	5	2	5	0	2	4	1
Rating	0–3				4–6			7–10				?
Num Part.	17				8			11				1

Responder's Rating [0]: "Yes. You can screen for and against social and personal traits as well as technical skills, but that's like getting people to pee in a cup for drug screening. The act of peeing in a cup does not guarantee consciousness and consciousness is what is required on the job."

Responder's Rating [0]: "Most subversive behavior I have seen comes from outside the project. Often from functional managers who believe they are negatively impacted by the project."

Responder's Rating [0]: "You can't screen for these people in a job interview."

Responder's Rating [3]: “This only brings you so far. It's required for the staff you bring onto the project, but does nothing about outside parties who have influence on the project.”

Responder's Rating [3]: “While it is certainly true that ‘social and personal traits’ are as important as technical skills, at least at the level where people get to participate in decision making processes, I don't think that this is true at all. The skills that are most desirable for avoiding the problems that lead to subversive behavior are the same skills that would make someone effective in organizing and coordinating a subversive attack. People skills are important to both endeavors.”

Responder's Rating [6]: “Most of your people need decent people skills. But a lack of ‘people skills’ absolutely does not equate to subversive behavior. Some ‘quirky’ engineers are fastidiously dedicated to the company's success. Factoring them out of an organization suggests an expectation of producing an ‘also ran’ product line in a rigid engineering environment where innovation is not necessarily encouraged except within narrow boundaries.”

Responder's Rating [7]: “While possible, in small groups, it is unlikely you'll find any filtering criteria that will catch them with any reliability. What one wants is to make subversive behavior have no reward. However, this will not eliminate subversive behavior caused by personal grievances.”

Responder's Rating [7]: “… it can help … a bit.”

Hypothesis 11—Median Rating: 10 Refusing to give information is a method frequently applied by subversive stakeholders.

TABLE 1.13

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	0	0	1	2	3	7	2	21	0
Rating	0–3				4–6			7–10				?
Num Part.	1				3			33				0

Responder's Rating [2]: “This is IMHO ‘subconscious’ most of the time and therefore not ‘subversive’ in the sense of your definition.”

Responder's Rating [5]: “Or giving misinformation, or putting a spin. News teams, media analysts, networks and people who produce documentaries, can all be subversive stakeholders about the state of our environment/political world.”

Responder's Rating [8]: “Either as the primary attack (40%) or to cover the attack (99%).”

Responder's Rating [9]: “Withholding crucial information means the system will miss certain capabilities or qualities.”

Responder's Rating [10]: "I agree strongly. It takes the form of omission most often. They know what you need to know, but you don't know that you need it yet. And 'it's not their job to tell you.'"

Responder's Rating [10]: "Yes. It can send people down the wrong path. It introduces unnecessary risk to a project. It burns time from the development cycles."

Hypothesis 12—Median Rating: 7 For an experienced software manager inside the project, it is usually rather easy to recognize the existence of subversive stakeholders.

TABLE 1.14

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	2	0	2	5	4	8	7	3	6	0
Rating	0–3				4–6			7–10				?
Num Part.	2				11			24				0

Responder's Rating [2]: "There is a know-how and perspective distance between a manager and [for example] a technician. So a subversive technician can do sabotage which that not be recognizable to the manager. At least, not without the help of another (non-subversive) technician. [That is,] sometimes 'doing what is specified' instead of 'doing what is actually required' can stop progress on a project that starts with poor specifications and subversive technicians. Afterwards, it's tough arguing 'who is guilty', though both the spec writer and the developer can interact in intentionally subversive ways."

Responder's Rating [5]: "It's also easy for an experienced software manager inside the project to misperceive conscientious disagreement as subversion."

Responder's Rating [6]: "The biggest obstacle to recognition is the failure to even consider it."

Responder's Rating [7]: "I should think so. Identifying who is the subversive might be more difficult."

Responder's Rating [8]: "This is usually the point where the company goals, the project goals, and the personal goals are all visible and available for comparison. When someone starts acting counter to the primary objectives, it stands out."

Responder's Rating [8]: "From below, '9.' From above, '7.' From below, you can still be blindsided if you didn't cover your bases when figuring out who is a stakeholder. But from above—you actually might not have enough information. Your project may be subverted from above in ways that may well doom the project.

Um. Ford just destroyed their battery powered trucks. You think the experienced project managers running the experimental truck project saw that one coming? ;-)"

Hypothesis 13—Median Rating: 8 Informal networks are very important for discovering subversive attacks.

TABLE 1.15

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	0	0	1	2	4	11	3	14	1
Rating	0–3				4–6			7–10				?
Num Part.	1				3			32				1

Responder's Rating [8]: "This is pretty true. Most coordinated attacks from the inside are likely to result in related grapevine chatter."

Responder's Rating [8]: "In that case, there will be someone who informs you of a hidden agenda."

Responder's Rating [8]: "Information is very important. Diverse information comes from informal networks."

Responder's Rating [10]: "I'd say they are very important for discovery. Particularly the smoking-room group—cigarette smokers usually find they have a broader range of contacts :)."

Responder's Rating [10]: "I agree. This is sometimes the only way in which enough perspective can be gained to infer the presence an invisible subversive attack, or to raise the flag about the nature of the subversion, and even to mediate the situation."

Hypothesis 14—Median Rating: 8 Understanding subversive mechanisms and awareness of the symptoms are important prerequisites when defending against subversive attacks.

TABLE 1.16

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	0	0	3	1	3	11	3	15	0
Rating	0–3				4–6			7–10				?
Num Part.	1				4			32				0

Responder's Rating [5]: "They are important to recognize attacks; and only then it helps in defending against it."

Responder's Rating [7]: "I don't think you have to be aware of these mechanisms to avoid attacks. I think simple observance of the principles of human relations management will do a pretty good job of preempting most subversion. Subversion is much less likely to occur when everyone feels they have had a chance to evaluate the proposal and contribute to the final solution; when they have had a chance to disagree and have their disagreement considered and addressed. Subversion is more likely to occur when people feel they are being coerced into doing something they feel is wrong, whether for political or other reasons. The human relations approach deals with this. Several well understood methods of problem solving make this an explicit element of their method.

On the other hand, awareness of where problems are likely to come from, and how they happen, can be helpful in understanding the importance of using these kinds of preemptive methods."

Responder's Rating [10]: "Naturally. But the better technique is to avoid them to begin with by using collaborative techniques that engage stakeholders in a way that they share the ownership of success with everyone else, and so no stakeholder is incentivized to subvert the project."

Responder's Rating [10]: "Yes. Experience will often let you see the consequences of actions. Let's face it, developers think in terms of code, not dollars. A budgetary attack will be effective against them. Upper management think in terms of dollars, and information attack will be effective against them."

Hypothesis 15—Median Rating: 5 Project members in the role of developer or technical lead are frequently not aware of subversive activities of managers

TABLE 1.17

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	1	2	3	4	9	4	5	3	0	4	2
Rating	0–3				4–6			7–10				?
Num Part.	6				17			12				2

Responder's Rating [4]: "If the subversion is from their own management, they can usually be fed a line about why the change in activity is necessary. If the subversionis from external management, it might not be on the radar. This, however, is more apt to happen with less experienced personal. The more experienced developer/lead will engage with other groups downstream and upstream and ask how the activities are affecting them, and are there any feedback loops or advanced warnings that would be beneficial to all?"

Responder's Rating [6]: "… may be aware but unable to respond."

Responder's Rating [6]: "This is particularly true of developers in 'mushroom' environments. It should be less true of technical leads, even in 'mushroom' environments. It is generally not true in rapid development environments in which the whole team has a role in evaluating the problem, generating the solution, and making project related decisions. Indeed, I have occasionally found project members to be aware of problems (via the grapevine of chatter with people on other projects) before anyone in the management or technical leadership of a project was aware of those problems. If this happens, by the way, the damage is probably already done and may be irreversible."

Responder's Rating [8]: "… they are kept in the dark on purpose…"

Responder's Rating [10]: "I agree strongly. '10.' Techies get set up and hung out to dry regularly. We call it a 'change of priorities.'"

Responder's Rating [10]: "Yes. Yes yes yes."

Hypothesis 16—Median Rating: 8 Defending the project against a subversive attack requires at least one loyal person with end-to-end understanding of the project and influence in the organization.

TABLE 1.18

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	1	0	2	2	2	4	0	2	7	5	11	1
Rating	0–3				4–6			7–10				?
Num Part.	5				6			25				1

Responder's Rating [2]: "I'd say that the people with the broadest knowledge tend to be found towards the less-influential end of the power spectrum, and that 'higher-ups' with a higher-altitude less-detailed view would have more influence. Perhaps more in the case of subversion-from-above, a higher-up ally would be important. But in the cases of same-hierarchical-level competition, higher-ups might be disinterested in taking sides of contests at that level. Having said that, contest-by-proxy would involve the higher manipulating the lower. In that case, one's project would be a proxy target for some other higher-up project stakeholder. Attack deflection in such a case might, for example, be helped by shifting the attacked stakeholder laterally away from one's project so as to terminate the attack. Such a shift would need the cooperation of a higher-up, whatever their motivation, with or without knowledge of one's project. But this all reflects my cynicism in supposing that an organization would not in general try to eliminate such interference at all levels; in several places I've worked, this kind of thing is very much a part of the business process. Some organizations seem to encourage this so as to have an atmosphere of competition and consequent supposed enhancement of performance. This apparently is the case where I am currently, but there is an excellent ring-fencing of development away from such turf-wars, so at least on my floor, there is a very cooperative collegiate atmosphere.

But I've no experience with such politicking; I keep my head down and get my invoices in on time. :)," Responder's Rating [4]: "This can help, but it is no panacea."

Responder's Rating [7]: "Agree somewhat. You can do it without that, but that would be pretty useful. Actually, without that, you have to work the wheels of direct and indirect influence. In the worst cases, going public with an accusation of subversion could have devastating consequences. If there isn't a clear line of interested authorities up to the level where budgetary decisions are made for both parties involved in the conflict, then there is no guarantee of a resolution, and the situation could fester. If it festers the cost in terms of lost time and productivity naturally increases, perhaps dramatically. It may also be harder to resolve as time goes on, since decisions will have been made in the mean time which perhaps should have been made differently had the subversion not been in effect. Still, an experienced person who witnesses a subversion can in some cases bring this to the attention of multiple people who can act together to accomplish the same thing that a single person with end-to-end understanding of the project might accomplish."

Responder's Rating [8]: "Influence in the organization, yes. End-to-end understanding of the project, not really."

Responder's Rating [8]: "Either loyal or someone who is compensated to having the thing succeed. However, all you may get is detection. Defense requires resolving the problem or neutralizing it."

Responder's Rating [8]: "… at the very least.."

Hypothesis 17—Median Rating: 3 Change projects are more prone to subversive attacks than new projects.

TABLE 1.19

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	8	1	5	5	1	4	1	1	1	0	4	6
Rating	0–3				4–6			7–10				?
Num Part.	19				6			6				6

Responder's Rating [0]: "They are subject to different kinds of attacks and can be defended on very different grounds, but new projects are certainly much more vulnerable to subversion than projects that have an established business value based on existing products and processes. Change projects can find an opposition that new projects won't have in those who would prefer the status quo, but new projects face a constant uphill battle of maintaining the case for building something that has no established business case (known market, established customer set, necessary process). The accountants are more likely to subvert new projects. The old guard is more likely to subvert change projects. The old guard, at least, can be brought into and given a stake in the success of, change projects."

Responder's Rating [0]: "It's not the kind of project, but who gets what if things win, fail, or drag on."

Responder's Rating [2]: "Also new projects imply change."

Responder's Rating [3]: "Not really."

Responder's Rating [3]: "I disagree. There are factors that affect both. Change projects suffer from stagnation in unhealthy organizations; whereas, new projects are like 'fresh meat' and people want to carve out their territory."

Hypothesis 18—Median Rating: 8 Projects which will change the structure of the organization are particularly prone to subversive attacks.

TABLE 1.20

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	0	0	2	1	1	2	14	4	9	4
Rating	0–3				4–6			7–10				?
Num Part.	0				4			29				4

Responder's Rating [4]: "I'm not sure that there is any project that cannot be attacked from some direction, but projects that change the structure of the organization and raise the possibility that people will lose their jobs and/or power as a result of the change are certainly likely to be resisted. Getting buy in from stakeholders that are likely to be effected this way will be particularly difficult. I think, however, that the most likely projects to be successfully subverted are new projects that are predicated on an imagined business case rather than a real market, customer set, or process."

Responder's Rating [4]: "Rather, these projects are more likely to have vested interests opposed to them."

Responder's Rating [8]: "They imply insecurity about one's job, unless the future is clearly communicated."

Responder's Rating [8]: "This kind of project generates more resistance."

Responder's Rating [10]: "I agree. If this won't prod a subversive attack out of your organization, nothing will. ;-)"

Hypothesis 19—Median Rating: 7 Subversive stakeholders are frequently experienced managers with a lot of political understanding.

TABLE 1.21

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	2	0	1	2	2	4	4	4	8	4	3	3
Rating	0–3				4–6			7–10				?
Num Part.	5				10			19				3

Responder's Rating [4]: "I have seen more engineers as subversives."

Responder's Rating [6]: "From their political understanding of what is achievable; they can make a good judgment aboutthe foundation for the project. I do not find this subversive, as killingan unsupported project early may be better for the organization."

Responder's Rating [7]: "I agree. The rest are for personal reasons. But, if the organization is changing, and there are people who 'aren't keeping up' (either in management or otherwise), then those people are more vulnerable to exhibiting subversive behavior as a result of the inherent conflict of interest they are experiencing. On one hand, they are expected to make rational decisions. On the other, their livelihood, or at least the comfort of understanding what their job is and how to do it, may be at stake."

Responder's Rating [7]: "In my case, it was a developer with little management experience, but lots of political understanding.I have no other points tocompare."

Responder's Rating [8]: "Certainly the most successful ones are."

Responder's Rating [8]: "**Effective** subversive stakeholders are."

Responder's Rating [9]: "These guys are more dangerous and capable of manipulating the system, but it isn't wholly limited to them."

Hypothesis 20—Median Rating: 6 Managers outside of the project who shoot missiles against the project from a safe distance are a frequent pattern of subversive attacks.

TABLE 1.22

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	2	3	8	2	4	6	1	4	6
Rating	0–3				4–6			7–10				?
Num Part.	3				13			15				6

Responder's Rating [?]: "Are those managers really 'stakeholders?' Or are they just bystanders?"

Responder's Rating [5]: "… or they are desirable critical thinkers whose input can temper the project output."

Responder's Rating [6]: "Though, less effective. Ask what they have to gain by doing so."

Responder's Rating [7]: "e.g., from competing project and affected teams and so on."

Responder's Rating [8]: "I agree. That is how they are perceived. The connotation of a missile is that is has a big impact and is unexpected. That is exactly what it is like to have a VP from another part of your company say in a public meeting that they see no point in your project and they think it should be cancelled and the people assigned to other projects. That's a missile. It can hardly be viewed as any way but subversive to the people in the project. However, it may very well be exactly the right thing for that VP to be thinking. If it is the right thing to be thinking, it is incumbent upon the VP to communicate this through appropriate channels and not just to lob a missile. But, some people who are VPs are VPs because they have connections [and] not because they are particularly good at healthy techniques for influence and governance."

Responder's Rating [8]: "Yes, especially when their project or power is at risk or they see the principles in the project they are attacking as competitors or enemies."

Hypothesis 21—Median Rating: 8 "Attacks from above" are frequently successful. That means if the subversive stakeholder is a senior manager, the attacker is likely to succeed.

TABLE 1.23

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	0	0	1	2	3	8	2	4	6	1	4	6
Rating	0–3				4–6			7–10				?
Num Part.	3				13			15				6

Responder's Rating [?]: "I have no idea. It strikes me as odd to imagine a senior manager engaging in subversion of a project. Why not just kill the project openly?"

Responder's Rating [5]: "It depends on the projects support."

Responder's Rating [7]: "… unless stopped by peer senior managers."

Responder's Rating [8]: "I agree mostly. It isn't a guarantee of success, but unlike other kinds of subversion, attacks from above can be 100% effective sometimes. A strong attack from above is likely to succeed unless there is a yet stronger supporter above."

Responder's Rating [9]: "Very likely. No amount of process or talent can defend against he who holds the purse strings."

Responder's Rating [10]: "Of course."

Hypothesis 22—Median Rating: 8 The interests of the subversive stakeholder are met better by failure of the project than by success.

TABLE 1.24

Rating	0	1	2	3	4	5	6	7	8	9	10	?
Num Part.	1	0	0	1	1	6	2	2	6	2	12	4
Rating	0–3				4–6			7–10				?
Num Part.	2				9			22				4

Some responders criticized me for including this hypothesis in the first place: "This is a truism. It is so obvious that you should not bother us with asking such questions". The high number of "10" ratings indicates that many responders were completely convinced of the validity of these statements. Nevertheless, other contributors expressed their doubts and gave extensive explanations for their reasons.

Responder's Rating [0]: "Not true. The stakeholder may be interested in just dragging it out, getting more resources, calling attention to himself as a hero, or be manipulating the circumstances to financial gain—in some cases the project must still succeed. Failure is not always the goal."

Responder's Rating [3]: "I'm aware that my rating might be out of the ordinary. But here [are] some explanations.

1. For certain categories of subversive stakeholders, yes the project's failure is directly better for them (managers who will lose influence, staff who will lose their jobs, suppliers who will lose a customer, customers who will wind up paying more—to mention just a few).
2. But for a great number of subversive elements (mostly employees and certain "caretaker" managers), the success or failure is immaterial, it's "change" that they oppose.
3. Then there are the consultants, staff, project managers, and outsourced parties or suppliers who want to see the project's implementation grow or be delayed

so that they can continue riding the gravy train. The ultimate success of the project is important to them, but if it can come now or in six month's time at $120/hr, let it be in six months time.

4. And lastly, it is my impression that a variety of subversive stakeholders are in most cases pursuing a strategy of competition with the project's stakeholders, and though the project's success might very well be a direct benefit to them, they would rather see it fail than see the rival behind the project succeed. That is, the subversive element sees the failure of the project's **stakeholders** as being in their interest, not the failure of the project."

Responder's Rating [4]: "Let's say there was a project that could save the company a lot of money. Everybody wants to see it succeed, except Fred. Fred sabotages the project. When the president finds out what happened, that Fred screwed it up, Fred is fired. I would say that Fred's interests were not very well met. ;o)

Even if you are not fired, you are known as a foot-dragger this can impair your career path in many other subtle ways."

Responder's Rating [5]: "I'm guessing sometimes yes, sometimes no. Sometimes, the interests of the stakeholder are met simply by engaging the project in subversion. The success or failure of the project is irrelevant—it's the effect of the subversion that the subversive is trying to produce."

Responder's Rating [5]: "If we all could foresee the future… One man's effective strategic defense against subversive attacks is another man's buggy whip company."

Responder's Rating [6]: "I agree somewhat. Often this is true, especially when a crucial decision between alternative approaches or technologies is at stake. It can be a zero sum game. However, when the subversion is for human reasons (as mentioned in answers above) there are several other possible outcomes, including:

- The subversive person changes stripes and supports the project once their human needs have been met (such as recognition or the respect of being asked for their opinion before decisions are made).
- The subversive person relinquishes once it is revealed that they are doing it for personal reasons.
- The subversive person rethinks their behavior and changes their behavior.
- The subversive person is themselves the target of effective influence and they elect to subdue their subversive behavior.
- The subversive person is put on report and has to fight to keep their job."

Responder's Rating [9]: "… almost by definition."

Responder's Rating [10]: "That is, at the very least, their perception."

REFERENCES

Boehm, Barry and Turner, Richard. *Balancing Agility and Discipline*, Addison-Wesley, 2004.

Britcher, Robert N. *The Limits of Software*, Addison-Wesley, 1999.

Charette, Robert N. “The Rise of Enterprise Risk Management and Governance,” *Executive Report*, Cutter Corp., Nov. 2004.

Charette, Robert N. “Managing the Risks in Information Systems and Technology,” *Advances in Computing* 44:1–58, 1997.

Cockburn, Alistair. *Surviving Object-Oriented Projects*, Addison-Wesley, 1998.

Ewusi-Mensah, Eweku. *Software Development Failures*, MIT Press, 2003.

Glass, Robert L. *Software Runaways*, Prentice-Hall, 1998.

Glen, Paul. *Leading Geeks*, Jossey-Bass, 2003.

Humphrey, Watts S. *Managing Technical People*, Addison-Wesley, 1997.

Jeffrey, Joel. “A Data-Driven Analysis of What Goes Wrong in IT Projects,” *The Software Practitioner*, July 2006.

Jones, Capers. *Assessment and Control of Software Risks*, Yourdon Press, 1994.

“Global Management Survey,” KPMG, 2005.

McConnell, Steve. *Software Project Survival Guide*, Microsoft Press, 1998.

Miller, Roy. *Managing Software for Growth*, Addison-Wesley, 2004.

Morasco, Joe. *The Software Development Edge*, Addison-Wesley, 2005.

Moynihan, Tony. *Coping With IS/IT Risk*, Springer-Verlag, 2002.

Nelson, R Ryan, “Project Retrospectives: Evaluating Project Success, Failure, and Everything in Between,” *Management Information Systems Quarterly Executive*, Sept. 2005.

Nelson, Sharon D., and Simek, John W. “Disgruntled Employees in Your Law Firm: The Enemy Within,” http://www.senseient.com, 2005.

Pfleeger, Shari Lawrence and Kitchenham, Barbara A. “Principles of Survey Research,” *ACM SIGSOFT Software Engineering Notes*, Nov., 2001.

Ropponen, J. and Lyytinen, K. “Components of Software Development Risk: How to Address Them. A Project Manager Survey,” *IEEE Transactions on Software Engineering*, 26(2), Feb., 2000.

Rost, Johann. “Political Reasons for Failed Software Projects,” *IEEE Software Loyal Opposition* column, Nov. 2004.

Rost, Johann and Glass, Robert L. “Subversion and Lying: the Dark Side of IT Politics,” *Cutter IT Journal*, April 2005.

Rost, Johann and Glass, Robert L. “The Impact of Subversive Stakeholders on Software Projects,” *Communications of the ACM*, July 2009.

Thibodeau, Patrick. “Firms in India Seek Better Background-Check System,” *Computerworld*, April 18, 2005.

Thomsett, Rob. *Radical Project Management*, Prentice-Hall, 2002.

Verner, June. “A Study by the National Information and Communication Technology Institute of Australia (NICTA), *Software Practitioner Newsletter*, July 2006.