

The Saboteur Within

Warren Harrison

In Bob Glass's Loyal Opposition column "Political Reasons for Failed Software Projects" (Nov./Dec. 2004), Johann Rost described how subversive behavior can sabotage software projects. As he points out, there are often stakeholders whose interests are best served (or at least they think they're best served) if a project fails. This might range from users who believe the project threatens their job to prominent individuals in the organization who feel the project's success might jeopardize their influence.



In Rost's scenarios, disaffected individuals capitalize on their roles in an organization to cause innocent-appearing events that threaten the project. For example, they might withhold or delay information, voice vague concerns that needlessly occupy a team's attention, or insist on overly detailed explanations and plans.

This is just another incarnation of what the security community has long called insider threats. Insiders exploit their legitimate role within an organization to harm it. Their knowledge of and access to the organization pose a substantial threat—probably greater than external threats. In many cases, the only thing preventing insiders from exploiting their privileged access and knowledge is the perception that their interests and the organization's are aligned. So, if delivering a project on time

or making a customer happy is in the insiders' best interests, you can expect them to contribute and work toward a common goal. However, when individual and corporate goals aren't so clearly aligned, a certain segment of the workforce will have no qualms about passively or actively pursuing their own interests at their employer's cost.

The man in the grey flannel suit

At one time, workers' self-interests were more closely aligned with the organization because of a symbiotic relationship. Workers would defer their self-interests in return for the certainty that the organization would be there for them. A relative of mine worked for General Electric from 1945 until he retired in the late seventies, and his experience was the norm in those days. This gave rise to the archetypical "man in the grey flannel suit," as Gregory Peck portrayed so well in the 1956 movie of the same title. If you expected to be employed by a company for 35 years, doing something that would harm its interests would be unimaginable.

For better or worse, those days are gone. Both companies and individuals focus on short-term gains; both view long-term plans and five-year plans as synonymous. Hardly anyone who joins a company in 2005 expects to still be there in 2020. The concept of long-term shared interests has devolved into increasing the value of your stock options portfolio so that you can make a bundle when your company goes public. Moreover, the fealty that employees once felt to their employer is

DEPARTMENT EDITORS

Bookshelf: Warren Keuffel,
wkeuffel@computer.org

Design: Martin Fowler,
fowler@acm.org

Loyal Opposition: Robert Glass,
rglass@indiana.edu

Open Source: Christof Ebert,
christof.ebert@alcatel.com

Quality Time: Nancy Eickelmann,
nancy.eickelmann@motorola.com,
and Jane Hayes, hayes@cs.uky.edu

Requirements: Neil Maiden,
N.A.M.Maiden@city.ac.uk

Tools of the Trade: Diomidis Spinellis,
dds@aub.gr

STAFF

Senior Lead Editor
Dale C. Strok
dstrok@computer.org

Group Managing Editor
Crystal Shif

Senior Editors
Shani Murray, Dennis Taylor, Linda World

Staff Editor Editorial Assistant
Rita Scanlan Brooke Miner

Magazine Assistant
Hilda Hosillos, software@computer.org

Art Director
Toni Van Buskirk

Technical Illustrator
Alex Torres

Production Editor Production Artist
Monette Velasco Carmen Flores-Garvey

Executive Director
David Hennage

Publisher
Angela Burgess
aburgess@computer.org

Assistant Publisher
Dick Price

Membership/Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Senior Production Coordinator
Marian Anderson

CONTRIBUTING EDITORS

**Anne Lear, Robert Glass,
Molly Mraz, Joan Taylor**

Editorial: All submissions are subject to editing for clarity, style, and space. Unless otherwise stated, bylined articles and departments, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IEEE Software* does not necessarily constitute endorsement by the IEEE or the IEEE Computer Society.

To Submit: Access the IEEE Computer Society's Web-based system, Manuscript Central, at <http://cs-ieee.manuscriptcentral.com/index.html>. Be sure to select the right manuscript type when submitting. Articles must be original and not exceed 5,400 words including figures and tables, which count for 200 words each.

virtually nonexistent. The recent rash of pension bailouts, outsourcing, and downsizing has aggravated the situation. It's no surprise that in such a culture, an employer enjoys no special privileges when an individual decides to "go bad."

Motivations

Employees (or other privileged insiders) who act counter to their organization's interest have a variety of motivations. However, we can classify most motivations as one of three types.

The first is *political*—seldom recognized but by far the most common motivation. The insider perceives that their position in the organization is somehow threatened by something going on—an organizational change, a project, even adopting a new programming language. Even though this event's success might be good for the organization, the insider views the event as not so good for them. They might try to derail it passively (for example, by withholding information) or actively (say, by "accidentally" deleting project files). The insider is simply seen as having a difficult personality, or as a curmudgeon. Insiders can assuage their guilt by rationalizing their actions—after all, they didn't break any laws, did they?

The second motivation is *greed*, plain and simple. It ranges from simply pilfering the office supply cabinets and making personal long-distance calls on the company's nickel to selling customer lists and leaking confidential information (for a price) to competitors.

The third motivation is *anger*. Behaviors we might attribute to political motivation or greed can be due in part to the individual's anger toward the organization. However, the kinds of actions I mean—for example, resetting the system administrator's password or defacing an employer's Web site—have no rational connection to either getting rich or improving the person's position in the organization. These are just acts of vandalism. Statistics tell us that many times these acts occur after an employee is terminated, but evidence often points to long-term planning prior to termination (for instance, adding back doors to

applications or creating bogus accounts with super-user privileges).

Addressing insider threats

To some extent, the first two motivations are easier to address. Anyone with the least amount of organizational savvy can recognize potential political motivation (although, regrettably, some in the high-tech community lack that ability these days). We can easily identify artifacts that people steal to enrich themselves (credit card numbers, valuable trade secrets, customer lists) and take precautions.

On the other hand, actions motivated by anger are much more difficult to address. The very irrationality of these actions makes them hard to preempt. Why on earth would anyone want to put pornographic images on a company's Web site? Why would someone purposely put a time bomb into their code?

Preempting anger-motivated threats

Recently the US Secret Service's National Threat Assessment Center and the Software Engineering Institute's CERT Coordination Center produced a report entitled *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (www.cert.org/archive/pdf/insidercross051105.pdf). The report found that 84 percent of the insider sabotage incidents they studied were at least partially motivated by anger and the perpetrator held a work-related grievance prior to the incident. They also found that a specific work-related event triggered most incidents.

Notably, most of the perpetrators had previously displayed disruptive workplace behavior, including tardiness, truancy, or arguments with coworkers and supervisors. Most of them had also communicated negative sentiments to others, including, in some cases, direct threats of harm to the organization. In the vast majority of incidents, the perpetrator took steps to hide his or her identity.

Unlike attacks motivated by politics and greed, we might best address anger-motivated risks by observing people's behavior and taking preemptive action.

For instance, we should track events such as negative performance reviews, demotions, and even the rejection of training requests. We should evaluate such employees' roles in any ongoing project and take preemptive steps in case they choose to take revenge on the project or organization.

Coordinating negative workplace events so that they occur only during a project's noncritical phases might be wise in many situations. This is especially true when we know individuals have preexisting grievances against the organization.

On the other hand, organizations must learn to take legitimate grievances seriously and make an honest effort to create fair and equitable workplaces. Ultimately, the best way to address insider threats is to ensure that the worker's interests are aligned with the

employer's. Sadly, many companies seem to forget this basic premise of management. Peter Gibbons' observation in the 1999 movie *Office Space*—"my only real motivation is not to be hassled; that, and the fear of losing my job"—is perhaps more true today in the software industry than ever before. Gibbons goes on to observe, "That will only make someone work just hard enough not to get fired." That and be an insider threat.

Feedback welcome

We'd like to find out what you think. Have you observed any acts of workplace sabotage? How frequent do you think it is? What proportion of the projects you work on is at least partially affected by insider sabotage? Please write me at warren.harrison@computer.org.

EDITOR IN CHIEF

Warren Harrison

10662 Los Vaqueros Circle
Los Alamitos, CA 90720-1314
warren.harrison@computer.org

EDITOR IN CHIEF EMERITUS:
Steve McConnell, Construx Software
stemcc@construx.com

ASSOCIATE EDITORS IN CHIEF

Education and Training: Don Bagert, Rose-Hulman Inst. of Technology; don.bagert@rose-hulman.edu

Design: Philippe Kruchten, University of British Columbia; kruchten@ieee.org

Requirements: Roel Wieringa, University of Twente; roelw@cs.utwente.nl

Management: Don Reifer, Reifer Consultants; dreifer@earthlink.net

Quality: Stan Rifkin, Master Systems; sr@master-systems.com

Experience Reports: Wolfgang Strigel, QA Labs; strigel@qalabs.com

EDITORIAL BOARD

Christof Ebert, Alcatel
Nancy Eickelmann, Motorola Labs
Martin Fowler, ThoughtWorks
Jane Hayes, University of Kentucky
Warren Keuffel, independent consultant
Neil Maiden, City University, London
Diomidis Spinellis, Athens Univ. of Economics and Business
Richard H. Thayer, Calif. State Univ. Sacramento
Rebecca Wirfs-Brock, Wirfs-Brock Associates

ADVISORY BOARD

Stephen Mellor, Mentor Graphics (chair)
Maarten Boasson, Quaerendo Invenietis
Robert Cochran, Catalyst Software
Annie Kuntzmann-Combelles, Q-Labs
David Dorenbos, Motorola Labs
Juliana Herbert, ESICenter UMINIOS
Dehua Ju, ASTI Shanghai
Gargi Keeni, Tata Consultancy Services
Karen Mackey, Cisco Systems
Tomoo Matsubara, Matsubara Consulting
Dorothy McKinney, Lockheed Martin Space Systems
Bret Michael, Naval Postgraduate School
Susan Mickel, Lockheed Martin
Ann Miller, University of Missouri, Rolla
Deependra Moitra, Infosys Technologies, India
Melissa Murphy, Sandia National Laboratories
Suzanne Robertson, Atlantic Systems Guild
Grant Rule, Software Measurement Services
Girish Seshagiri, Advanced Information Services
Martyn Thomas, Praxis
Rob Thomsett, The Thomsett Company
Laurence Tratt, King's College London
Jeffrey Voas, SAIC
John Vu, The Boeing Company
Simon Wright, SymTech

CS PUBLICATIONS BOARD

Michael R. Williams (chair), Michael R. Blaha, Mark Christensen, Roger U. Fujii, Sorel Reisman, John Rokne, Bill Schilit, Linda Shafer, Steven L. Tanimoto, Anand Tripathi

MAGAZINE OPERATIONS COMMITTEE

Bill Schilit (chair), Jean Bacon, Pradip Bose, Doris L. Carver, Norman Chonacky, George Cybenko, John C. Dill, Frank E. Ferrante, Robert E. Filman, Forouzan Golshani, David Alan Grier, Rajesh Gupta, Warren Harrison, James Hendler, M. Satyanarayanan

Next Issue:

Software Engineering Project Management

- How Standards Have Aided Adoption of Project Management Practices
- Management Challenges to Implementing Agile Processes in Traditional Development Organizations
- Successful Software Management—Steering and Balance
- A New Paradigm to Address IT Project Failures
- The Evolution of Distributed Project Management
- Project Management in a Software Product Line Organization
- Professional Certification of Software Engineers

Also:

- Rich Media Scenarios for Discovering Requirements
- Lazy Types: Dynamic Strategy Selection of Object Methods

Visit our Editorial Calendar at
www.computer.org/software/edcal.htm