



Peter G. Neumann

# Risks of Insiders

**T**his month we consider some of the risks associated with insiders. An insider is someone who has been (explicitly or implicitly) granted privileges authorizing use of a particular system or facility. This concept is clearly relative to virtual space and real time, because at any given moment a user may be an insider with respect to some services and an outsider with respect to others, with different degrees of privilege. In essence, insider misuse involves misuse of authorized privileges.

Recent incidents have heightened awareness of the problems associated with insider misuse—such as the Department of Energy's long-term losses of supposedly protected information within a generally collegial environment, and the Bank of New York's discovery of the laundering of billions of dollars involving Russian organized crime. The RISKS archives include many cases of insider misuse, with an abundance of financial fraud and other cases of intentional misuse by privileged personnel in law enforcement, intelligence, government tax agencies, motor-vehicle and medical databases. In addition, there are many cases of accidental insider screwups in financial services, medical applications, critical infrastructures, and computer system security administration. Accidental misuse may be effectively indistinguishable from intentional misuse, and in some cases has been claimed as a cover-up for intentional misuse. Related potential risks of insider misuse have been discussed previously on this page, such as in cryptographic key management and electronic voting systems.

Although in the past much concern has been devoted to penetrations and other misuse by outsiders, insider threats have long represented serious problems in government and private computer-communication systems. However, until recently, the risks have gone largely ignored by system developers, application purveyors, and indeed governments.

Today's operating systems and security-relevant application software frequently do not provide fine-grained differential access controls that can distinguish among different trusted users. Furthermore, there are often all-powerful administrator root privileges that are undifferentiated. In addition, many systems typically do not provide serious authentication (that is, something other than fixed, unencrypted reusable passwords) and basic system protection that might otherwise prevent insiders from masquerading as someone else and making subversive alterations of systems and data.

Too often it is assumed that once a user has been granted access, that user should then have widespread access to almost everything. (Even when that assumption is not made, it is often difficult to prevent outsiders from becoming insiders.) Audit trails are typically inadequate (particularly with respect to insider misuse), and in some cases compromised by privileged insiders. Existing commercial software for detecting misuse is oriented primarily toward intrusions by outsiders, not misuse by insiders (although a few ongoing research efforts are not so limited). Even more important, there is typically no definition of what constitutes insider misuse in any given system or application. Where there is no such misuse definition, insider misuse certainly becomes difficult to detect. There are many reasons why it is difficult to address this problem.

Insiders may have various advantages beyond just allocated privileges and access, such as better knowledge of system vulnerabilities and the whereabouts of sensitive information, and the availability of implicitly high human levels of trust within sensitive enclaves.

We need better definitions of insider misuse in specific applications (accidental and intentional, and in the latter case malicious and otherwise), better defenses to protect against such misuse, better techniques for detecting misuse when it cannot be prevented, better techniques for assessing the damage once misuse has been detected, and then better techniques for subsequent remediation to whatever extent is possible and prudent—consistent with the desired security requirements. Techniques such as separation of duties, two-person controls, split-key encryption, and enlightened management can also contribute. A comprehensive approach is essential.

A Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse was held in Santa Monica, Calif., Aug. 16–18, 1999, sponsored by several U.S. government organizations. The purpose of the workshop was to address the issues outlined here. The workshop report is available at [www2.csl.sri.com/insider-misuse/](http://www2.csl.sri.com/insider-misuse/). It surveys the problems presented by insider misuse and outlines various approaches proposed at the workshop. The report is recommended reading for those of you concerned with these problems. ■

PETER G. NEUMANN ([www.csl.sri.com/neumann/](http://www.csl.sri.com/neumann/)) is the moderator of the online Risks Forum ([comp.risks](http://comp.risks)).