Insider Attacks: A Thorny Problem

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Prof. Jim Maloney, one of the stellar instructors in the Norwich University MSIA program, recently circulated a pointer to a Gartner Group press release on insider crime <http://www3.gartner.com/5_about/press_releases/pr29may2003a.jsp>. The headline reads, “Gartner Says 60 Percent of Security Breach Incident Costs Incurred by Businesses Will Be Financially or Politically Motivated” and the text includes such warnings as, “By 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated, according to Gartner, Inc. . . . Most of these financial losses will be the work of insiders working alone or in conspiracy with outsiders.” According to Richard Hunter, VP for Gartner, “There is a delicate balance between limiting insider access to information and crippling the ability to create revenue. . . . Generally, this conflict between security and commerce is resolved in favor of creating revenue and therefore facilitating insider crime.”

How do we know insider crime is a problem? How do we know it’s increasing? Alas, we have to work mostly with imprecise information. Word of mouth among security experts consistently suggests that only about 10% of all computer-related crimes are ever reported, but that just refers to those that are detected. By definition, we know nothing about crimes that aren’t detected (except that some old crimes occasionally pop into view months or years later). As for surveys, all of them use self-selected samples, so we cannot rely much on the precise numbers we get; however, they are useful in getting a sense of the range of crimes and costs that the respondents encounter. Surveys that report changes in trends suffer from the fundamental difficulty of all non-random sampling: we cannot tell if the year-to-year changes represent the underlying phenomenon (crime rates and costs) or in confounding variables (willingness to report the crimes and bias in estimating costs).

But all that aside, Mr Hunter hits an important point in his comment above: insider crime is even harder to defend against than external attacks. Protecting information against outsiders is, at least in principle, relatively simple: after all, they aren’t normally supposed to have access to confidential information at all (this simple view does ignore the real complications of supply-chain and customer-relationship management, in which sharing information with trading partners is a key to long-term success). But how do we handle information sharing within our own organizations? How do we maintain an environment that fosters creativity through the free flow of knowledge and ideas while protecting ourselves against damage from Bad People?

I think that the best approach is to use everything we know about proper hiring and management of employees to select trustworthy people and to maintain vigilance against dishonest and disgruntled staff members. As a general policy, I strongly support the view that our default mode in most organizations should be to share information internally unless it needs to be sequestered. That means, for example, that ideas on improving a product would be considered company-confidential and fair game for discussion among employees; in contrast, the specific development details in the engineering department would be classified as department-confidential and restricted to those with a need to know.
I think that with an appropriate balance between security and openness, we can have our creative cake without giving it away to be eaten by our competitors.

* * *

For further reading:

<http://www.nwfusion.com/newsletters/sec/0501sec2.html>

<http://www.mekabay.com/methodology/index.htm> or  


* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.