Conflict of Interest

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

The collapse of Enron, formerly the seventh-largest company in the United States, and recent revelations of widespread destruction of company documents by its auditors and bring to mind the difficult position of auditors in any business. Auditors face a challenge because in some sense, they inevitably have a conflict of interest. In the financial world, auditors ostensibly serves the interests of stakeholders, including shareholders employees, suppliers, and clients of the organization they Audit. Inevitably, financial auditors also serve at the discretion of decision makers within the very firms they are auditing.

In the Equity Funding fraud, discussed in recent columns in this series, the auditor who testified to the probity of that corrupt firm derived some 80 percent of his revenues from Equity Funding; he was willing to accept unverified reports that were delivered late – late because they had been fabricated the night before by a management team. The auditor had a very serious conflict of interest: offend his client by issuing a negative report and a major portion of his income would disappear.

In the Enron case, it appears that the company’s auditors were also supplying extensive consulting services in addition to their auditing services. Attempts in recent years to pass legislation making it illegal to provide both financial auditing services and consulting services to the same clients by a single firm have been strongly resisted by a number of large firms; lobbyists have paid large sums to the re-election funds of many politicians who subsequently voted against such restrictions to reduce conflict of interest.

Providing favorable treatment of special interests because of large “campaign” contributions sets up an inevitable conflict of interest between the protection and promotion of voter interests and protection and promotion of contributor interests. Legislators have recently admitted as much in public hearings about the Enron failure.

In a corporate environment, setting the information security function as a subset of the information technology function potentially establishes a conflict of interest. We know that it is unacceptable to have the head of quality assurance report directly to the head of programming; similarly, I argue that it is unacceptable to have the head of information security reporting directly to the head of information technology. For example, the explicit or implicit goals of a chief information officer (CIO) may center on a short time horizon such as the quarterly bottom line in the profit-and-loss statement. Such a narrow focus may originate because that’s they way the CIO was trained in business school or because the CIO plans to leave the company soon; either way, spending money on information security will not suit the purposes of such an officer. In contrast, the goals of a chief information security officer (CISO) need to be long term and to encompass business requirements, not merely technology issues. Protecting corporate information assets may conflict with the cheapest method of accomplishing a specific task; the interests of the CIO and of the CISO will therefore conflict.
In my opinion, a CISO should report at the same level and have the same level of authority as the other chief officers – the CEO, the CIO or the chief technology officer (CTO), the chief operating officer (COO) and the chief financial officer (CFO).

I’d be interested in receiving comments on this stance from readers, especially those backed up with case studies.

* * *


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 <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 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.