

Netwatch

By Jim Carroll

Your guide to business & accounting on the Internet

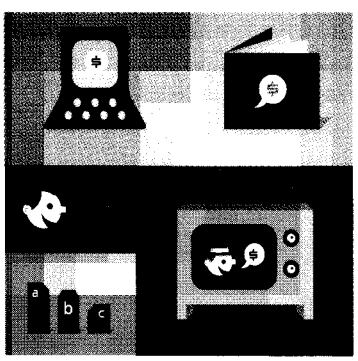
The next governance grenade

While much of the accounting world has turned its attention to the complexities and issues associated with the Sarbanes-Oxley Act and other regulatory developments over the past year, I'd suggest you get ready for the next big corporate governance issue.

Maybe we should call it SOX Round 2.

If you don't move the issue of corporate, infrastructure and network security into the boardroom — fast — you may soon find yourself at the receiving end of some pretty nasty regulatory, not to mention legal, consequences.

For years, computer and network security has been left to information technology folks. Most try to do the right thing, but that's not an easy task when IT departments are largely underfunded and neglected by management. In other cases, IT executives make horrid decisions with respect to critical technology platforms, or do not take the steps to build a reliable, robust and secure platform that will support the company into the future.



The result is IT has been operating in a vacuum. I have yet to encounter an organization where responsibility for the integrity of its business infrastructure is dealt with at the level of the CEO and board of directors.

I've been suggesting for years that it is only a matter of time before we see large-scale legal action against the board and senior management for their negligence in this regard. Even as I write this column, the latest Internet worm, Sasser, is ravaging corporate networks worldwide. Most businesses could have avoided the problem by installing the well-publicized updates and patches but did not bother. Perhaps they were too busy. Maybe they don't have the proper funding. Or the issue might not be important enough to warrant attention at the highest level of the organization.

Such apathy is appalling, given that organizations worldwide are busy integrating their transaction systems with those of their business partners. They are developing new methods of doing business that expose fundamental components of their financial and accounting systems to new risks. Certainly CEOs and boards aren't aware that these critical systems are being built on top of a flaky software platform so riddled with bugs and security weaknesses that they have only managed to escape disaster as a result of simple luck.

This negligence will soon bear serious economic consequences. Heck, if I were a tort lawyer, I'd be licking my lips in anticipation of the opportunities to come in the next few years. If you think this sounds like the ranting of someone who treats security with a little too much passion, consider the recent recommendation of the US Corporate Governance Task Force of the National Cyber Security Partnership (NCSP). It suggested that network and infrastructure security issues become board and CEO-level governance issues. NCSP is not some small think-tank issuing rabid, let's-hype-the-issue proclamations; it was founded in 2003 by the US Chamber of Commerce, the Business Software Alliance and the Information Technology Association of America.

This is your fair warning. Deal with security and infrastructure issues now, before it is too late.

Jim Carroll, FCA, is a well-known speaker, author and columnist. Reach him at jcarroll@jimcarroll.com or log on to his website at www.jimcarroll.com

SYSTEM SECURITY SITES

National Cyber Security Partnership
www.cyberpartnership.org

Organization for Economic Co-operation and Development publication, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*
www.oecd.org/dataoecd/16/22/15582260.pdf