

# With Sarbanes-Oxley, compliance takes center stage for CIOs

Lincoln Brunner

March 7, 2005

If, five years ago, you asked a group of chief information officers for their number-one issue, they might have said storage capacity, security or bandwidth.

Today, the consensus issue is compliance, particularly with the new spate of securities legislation, highlighted by Congress's passage of the Sarbanes-Oxley Act of 2002, or SOX, as it has come to be called. SOX, which was passed largely in reaction to the corporate scandals that brought down the likes of Enron and Adelphia, addresses numerous issues within public companies, which were required to begin complying in November 2004. Among those are corporate ethics, governance practices, fiscal disclosures and executive compensation.

As [EWeek](#) Executive Editor Stan Gibson pointed out at last week's Fusion 2005 conference at Madison's Fluno Center, the "irrational exuberance" of the Internet craze has given way to an age of new regulation, much like Congress's creation of the Securities and Exchange Commission after the crash of 1929. But instead of viewing the new regulations as a curse, CIOs and other executives can look at it as an opportunity, Gibson said.

"You've been given a bunch of lemons, it's time to make lemonade," he quipped. To comply with Section 402 of SOX, for instance, companies must ensure they have integrity of data storage, Gibson noted. Looking beyond simple compliance, complying with Section 402 allows companies to detect internal fraud. In addition, being forced to consolidate data storage gives a CIO a way to market what the IT department is doing to the CEO by showing him or her that rather than being a sinkhole for money, IT expenditures actually increase

shareholder value.

In fact, companies can lose competitive advantage by stopping with the letter of the law, Gibson said. One vendor at the conference agreed.

"Sarbanes-Oxley is just good business sense," said Rick West, director of Midwest regional sales for Waltham, Massachusetts-based Verdasys, a security software vendor. "Be sure that you have controls, be sure that people aren't altering information that you don't know about." To aid in that effort, Verdasys sells software that monitors a company's PCs and laptops at the kernel level so that a company can see what its risk areas are and enforce their information usage policies.

"Everybody spent about double what they wanted to spend last year," West said of SOX compliance. "SOX has been referred to as the Y2K that keeps on giving, because they [companies] have tried to assess those risks, and they haven't really put automated procedures in yet. Every 90 days, you've got to audit those controls and make sure they're all working right. If you haven't really put anything new in to automate stuff, you're going to have some pretty ugly expenses again, this year." Another question is, does a company have its IT leaders at the planning table when it comes to compliance, or are they simply shoveling off tasks at the last minute?

"That's a mistake a lot of organizations make – they try to hand this off to a controller or a manager of IT and say, 'Run with it,'" said Ronald Kral, founding partner of Candela Solutions LLC, a public accounting firm in Madison specializing in governance, internal auditing and other issues. "Last-minute in Sarbanes terminology is six months for year-end. That's not enough time. It's typically an 18-month process."

"It's incumbent on the organization to have the CIO, the chief

technology office, as part of the Sarbanes compliance committee," Kral said. "They need to be integrally involved with planning and be at the table overseeing the entire process. Too many times, I see IT directors handed down a Sarbanes project and they're scratching their heads and saying, 'I'm an IT guy. I've never been an auditor; I don't know how to document. I know IT.' But there's often times a gap that they need to come up to speed on."

In addition, the criminal and civil penalties for noncompliance – up to 20 years in prison for certain violations – has created a new urgency for compliance and more pressure for CIOs to drive compliance, said Rob Neumann, managing director for Burwood Group Inc., a Chicago-based consulting firm.

"Be proactive around taking care of issues that are known, because now we've been through a round of SOX compliance issues as of late last year," Neumann said. "Fix them so you don't waste your time next year. SOX is not going away, and other compliance issues are not going away. As is the case with many issues, people are reactionary as opposed to being proactive. Once the hammer comes down, then they do something about it. The hammers in this case are audits that find issues.

"I think it speaks to an IT organization that does the right things – creating the right documentation, having the right change controls with changing servers or code within servers or other equipment ... so when another group comes in, they know that those changes have been made," Neumann added. "[The report] needs to be put in plain English, so that if an auditor comes in and they don't understand technology, they can understand it."

Lincoln Brunner is a WTN contributing editor and can be reached at [lincoln@wistechnology.com](mailto:lincoln@wistechnology.com).