After Sarbanes-Oxley: IT Compliance Update

BEN WARDEN

The Sarbanes-Oxley Act changed the face of IT security for publicly traded companies. But subsequent security developments and an increased business focus have engaged IT pros in compliance at organizations of all size.

Social and governmental forces have pushed IT compliance to the forefront of business during the past five years. Banks, hospitals and employers are supposed to be trustworthy fortresses of information, but as many people have found out, they sometimes aren't.

With the passage of the Sarbanes-Oxley Act of 2002, more and more organizations turned their attention to IT compliance to ensure the security of private information. The main catalyst for Sarbanes-Oxley was the financial improprieties of major companies, including Enron, WorldCom and Tyco International. But the act tackles a host of issues related to corporate governance, financial disclosures and accountability of publicly traded companies.

Section 404 specifically relates to IT practices, calling for managers and an external auditor of the company to report on the capabilities of the company's internal control over financial reporting. By far, it's the most costly aspect of the legislation for companies to put into operation, as testing and recording important manual and automated financial controls requires enormous effort.

The act provides a benchmark for a total paradigm shift in IT compliance. Before 2002, enforcement of compliance depended on a loose consortium of laws and protocols. After passage of Sarbanes-Oxley, one all-encompassing act enforced compliance rigidly. Sarbanes-Oxley was a rock thrown in the IT pond, and ripples can still be seen today.

Signing the bill into law changed many IT professionals' worlds overnight, and it became clear society was demanding a more secure cyberspace. Starting with the aftermath of Sarbanes-Oxley, the past few years have been busy for IT compliance.

"The first year was pretty rough for everybody. A lot of hours and costs were put into it, but once a plan

and a blueprint was laid out there, we felt better," said Howard Schmidt, security specialist for (ICS)[2].

"We've managed to go from the first year, refine it for years two, three and four, and we're already on to year five now. Things are a lot smoother, companies know what to expect, they know how to make sure they're compliant and not trying to come back and fix something. Overall, it's more honed to say, 'OK, here's the business need that is somewhat unique, and here's a mitigating control that can ensure the integrity of it.'"

Bill Slater, an IT security expert with more than 30 years of experience, is a program manager at CSSS.NET. He also remembers the early days of IT life under the newly passed Sarbanes-Oxley Act.

"When you're doing something like data center management and change management, you see the effects of Sarbanes-Oxley immediately if it's a publicly traded company," Slater said.

"Every time a change was submitted, we were under increased scrutiny, like if you were going to submit a change to the infrastructure, let's say put a server on the network or take a server off the network. There was increased responsibility for the IT professional to have the documentation necessary to say how we would back this out if it was problematic on the infrastructure."

In the immediate aftermath of the act passing, data protection to prevent a security breach became of utmost importance. Now, either through Sarbanes-Oxley or by increased scrutiny from management, organizations have aimed to integrate business practices with their IT protocols.

Schmidt, a longtime security specialist, former eBay chief security officer and special adviser to cyber security for the White House, said these practices have become much more familiar to IT professionals since the act was implemented.

"As we've seen over the years, some of the shift has moved away from hard security technology and become more business related," Schmidt said.

"Accordingly, our product development folks then put more emphasis on the current environment we live in, which is more business-oriented, as opposed to five or six years ago when it was all about protecting something from outsiders. Now, it's about how to provide something for outsiders, but do it securely."

The compliance required by Sarbanes-Oxley is not as daunting now for IT professionals as it was when the bill was first passed. The tasks today are added into the other daily, weekly, monthly and yearly reports and processes the IT pro completes.

"It has been baked in to the day-to-day business process, as all of a sudden you don't have to pull people from other work to go do this, which you had to do in 2003," Schmidt said.

"Now it's just part of the day-to-day thing. When someone does something, they look at it through the lens of how this complies with Sarbanes-Oxley."

No matter how integrated security is into the overall IT process, breaches still happen, as demonstrated by the well-publicized case of the Department of Veterans Affairs (VA). A VA employee took home a laptop containing the names and Social Security numbers of every veteran discharged since 1975. The laptop was later stolen, a situation unavoidable from a technical standpoint, but not from an employee policy perspective.

The breach was a driving factor in the VA increasing its data security. It hired more security specialists, including Bill Slater. Slater said that the VA isn't leaving anything to chance after the breach.

"What's really amazing is, a year later, the VA battened down the hatches so well that we've become the gold standard of computer security," he said. "They've really come a long way in educating their employees on computer security and putting stuff into place that will prevent data loss.

"They just recently said they're not going to have any more floppies, USB drives or external hard drives without special written permission. They're practically paranoid about data security over here, with good reason. They're dealing with millions of veterans' records and Social Security numbers that can't be compromised again."

Pending Legislation in IT Compliance

BEN WARDEN

Congress is considering the following are pieces of legislation to broaden the scope of Sarbanes-Oxley and make data more secure. While similar legislation is introduced every year, these examples have gained the most steam due to their ability to make an immediate impact on security.

Federal Agency Data Breach Protection Act

A few years ago, the House Committee on Oversight and Government Reform reported that more than 1,100 laptop computers had gone missing from the Department of Commerce since 2001. From those reported missing, nearly 250 were from the Census Bureau and contained such personal information as names, incomes and Social Security numbers. Representative Tom Davis, R-Va., introduced the Federal Agency Data Breach Protection Act bill, which, according to his office, would set "policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information and for which harm to an individual could reasonably be expected to result." This means if there are similar breaches in the future, the U.S. government will have to immediately and vigorously inform individuals who've had their information stolen.

Social Security Number Misuse Prevention Act

After it wound up dead in the past two Congresses, the 110th Congress is again attempting to pass this legislation introduced by Dianne Feinstein, D-Calif. The act expands the federal criminal code to prohibit the display, sale or purchase of Social Security numbers without the expressed consent of the individual, except in specified circumstances. The bill also requires the attorney general to research and report to Congress on all the uses of Social Security numbers under any federal law to help cut back on the everyday use of a Social Security number. Also, on the consumer side, the bill prohibits a commercial entity from requiring an individual to provide a Social Security number when purchasing a commercial good or service.

Cyber-Security Enhancement Act

Rep. Adam Schiff, D-Calif., and Rep. Steve Chabot, R-Ohio, introduced this piece of legislation in May as an effort to pump $10 million a year into federal law enforcement efforts to crack down on cybercrime. The money would go to training law enforcement officials at all levels and providing them with computer forensics tools they need to investigate online scams, identity theft and other computer crimes. The bill also would enhance punishment and sentencing guidelines for cybercriminals and make potential offenders think twice.

CERTSCOPE®

Check CertScope to read more than 100 articles and link to 233 Web sites on IT compliance.

Washington has introduced a host of legislation that broadens the scope of Sarbanes-Oxley and aims to prevent similar incidents. Congress currently is considering the Federal Agency Data Breach Protection Act, the Social Security Number Misuse Prevention Act and the Cyber-Security Enhancement Act, among others.

While none have been signed into law yet, the sheer volume of IT-security legislation demonstrates Washington's attention to the issue. For Slater, however, his security work with the VA is personal.

"I'm also a veteran, so have a direct stake in doing my job well because I'm one of the veterans that benefits from me doing my job well," he said.

"The entire organization was put on notice that [we] will be more vigilant about data, data security privacy protection, and all these education programs got put into place."

While the VA breach grabbed Washington's attention, the media coverage raised awareness of IT security that reaches beyond the proposed legislation and into the business world. While Sarbanes-Oxley mostly affects large publicly traded companies, organizations of all sizes, public and private, are now more alert to situations like the VA breach. And IT professionals have a broader understanding of data protection concepts and are focused on fine-tuning the specific implementations.

"I think of it as different types of fuels in a car," said Schmidt. "The basic engine and mechanism of the vehicle itself is the

> "Now it's just part of the day-to-day thing. When someone does something, they look at it through the lens of how this complies with Sarbanes-Oxley."

same; we're just now using fuel in there that's more efficient and causes less pollution.

"The same thing applies here, the core vehicle of the certification has been there and will be there for years and years to come, and all we have to do is go, 'OK, we'll do this additive instead of this additive this time because that's how the landscape has changed.'"

"I think of it as different types of fuels in a car. The basic engine and mechanism of the vehicle itself is the same; we're just now using fuel in there that's more efficient and causes less pollution."

Worldwide Compliance

IT compliance becomes even more of a challenge in light of increasing globalization. With organizations doing increased business abroad, both in operations and job hiring, the mixing of domestic IT compliance processes with other countries' programs may create problems.

Increasing ethical stipulations on IT security is a step in the right direction, but it all might be in vain if it doesn't apply to the organization's international contingent. It's a tricky situation, where an outsourced employee working, for example, in India would have to follow the rules set forth by his or her employer's country of origin.

"The real challenge [comes] as the workforce changes and becomes more diverse and internationalized within corporations inside the borders of the United States that are accountable under the laws of the U.S.," Slater said.

"The biggest challenge over the past seven or eight years has [been to] make sure that these people who are not affected by our laws learn that corporations are accountable under these laws, and they need to abide by them if they're going to work there."

The passage of Sarbanes-Oxley raised the stakes for IT compliance, but subsequent developments have raised awareness of the issue even further. Whether through news coverage of the VA breach or just general media coverage of the risks presented by data theft, people have learned to keep a close eye on their personal information.

This shift has caused many businesses to rethink their IT strategies. A company or organization with perceived weak online security will take a hit in its pocketbook and struggle to regain public confidence. Even with the current flurry of legislation, the link between security and business results is an equal, if not greater, driver of IT compliance.

"From the beginning, it has been looked at as not just an IT problem but a business problem that had IT, financial and specific technology components to it," Schmidt said. "Society is now saying, 'We want you to protect our privacy. We want you to make sure our data isn't out there published on the Internet on your Web site with my Social Security number in plain view.'"

– Ben Warden, bwarden@certmag.com