SKYVIEW PARTNERS, LLC

Sarbanes-Oxley Act: Security-Relevant or Not?

Why was Sarbanes-Oxley Act (SOX) Enacted?

The Sarbanes-Oxley Act or SOX is a direct response from the United States Congress trying to prevent publically held corporations from experiencing an Enron- or WorldCom-like fiasco. Realizing there were numerous failings at Enron and other corporations that have been less-than-forthcoming regarding the truthfulness and accuracy of their financial statements, the bill assigns responsibility and addresses the accountability for the accuracy a company's financial reports. SOX also encourages separation of responsibilities. As a result, many corporations are splitting or have already split the positions of President and CEO between two people. In many corporations, these positions were held by one individual. Being held by two people can provide for more checks and balances as well as not allowing any one person to hold too much decision-making power. SOX also has sections specifically addressing the role of accounting and auditing firms both for SOX compliance as well as for traditional audits. It also addresses accounting practices and procedures, as well as the ramifications for corporate officers should compliance not be forthcoming as well as ramifications for auditing firms should they not follow the terms of the Act.

What Specific Areas of Data Security Are Addressed by SOX?

The simple answer to that question is: None.

Unlike HIPAA (Health Insurance Portability and Accountability Act) and GLBA (Gramm-Leach-Bliley Act) – two other U.S. Government Acts which have received lots of attention by the IT Security world – SOX does not specifically spell-out any data security requirements. Both HIPAA and GLBA are quite explicit about in their requirements, but not SOX. If SOX is not explicit on the data security requirements, why are some claiming that it has IT implications? Most likely, it's because of SOX' original use of the term "internal control". Before the Act was finalized, this term was not well defined and it led people to define "internal control" to mean many things including auditing every electronic transaction on a computer and securing the database in which the company's data resided. Realizing the confusion this was causing, this term has been re-worded as "internal controls over financial reporting." Now if you look at the term "internal control" it is always used within the context of some aspect of financial reporting and usually is stated as "internal controls over financial reporting" thus eliminating much of the confusion. So rather than internal controls having the potential to mean any process within a corporation, it is clearly scoped to pertain to financial reporting.

Does this Mean I Don't Have to Worry About Sarbanes-Oxley?

SOX is about evaluating the business risk associated with ensuring the accuracy of a company's financial reports and ensuring processes and procedures are in place to validate and verify what's claimed as a company's bottom line. Does managing this business risk and ensuring appropriate processes are in place preclude IT's involvement or preclude the need for data to be secured appropriately? Absolutely not. Are some CFOs (Chief Financial Officers) going to investigate IT's processes and require adherence to a more restrictive security policy? Yes.

More than the CFO, however, we're seeing many of the SOX auditing firms driving the IT security issue. That's because many of them have or had an IT security practice so they understand the need for a security policy and robust security implementation. Since the accounting firm performing the SOX audit also has to sign off on the company's financials, many auditing firms are requiring that good security practices be in place.

It is up to the company to determine how best to mitigate the risk to its financial data and how best to ensure its accuracy. Namely, there are no specific implementation details provided in the Act. Also, SOX clearly allows businesses to base risk mitigation actions on the size of the company, cost of the solution and resources required to implement it. In other words, the Act recognizes that one solution will not satisfy every company's requirements. I would be cautious about products that claim to help you become Sarbanes-Oxley "compliant." I would be cautious because, with the exception of discussing generally acceptable accounting principles, SOX does not specifically spell-out how to be in compliance. Could these products help you in your company's compliance? Possibly. But only if the people in your company responsible for the integrity of your financial data deems, through a business risk analysis, that the product addresses an area of risk. Or, an auditing firm finds a deficiency in your processes or your security implementation, writes up a finding and you determine a product that solves the particular issue.

Will SOX Ever Address IT and Specifically Data Security Issues?

Just because SOX does not currently address IT in general or data security in general, does that mean it never will? No. Acts can be modified. And if there is too much confusion about this issue, it's likely that the Act will be modified to address IT and/or data security. But like the final ruling for HIPAA, it's almost guaranteed that the requirements will be general in nature and not dictate a specific solution or product. The Government does this, recognizing that the ruling must accommodate the fact that companies are literally using every operating system possible and that not all solutions are available on all platforms. For example, two of the requirements could be that all users must be authenticated and there must be accountability for users' work. Translated into OS/400 terms, that would mean that users cannot share the same user id and password (accountability) and that they must have a valid user id/password or network authentication mechanism (such as Kerberos) or a one-time use password or a digital certificate to prove that they are who they say they are (authentication.) As you can see, even in OS/400 terms, you have choices for the actual implementation.

If You Want to Be Proactive

What if you want to make sure you have your ducks in a row before your CFO comes knocking at your door? Try looking at data security best practices. ISO standard 17799, while not all that popular in the U.S., started out as a British Standard and has become widely accepted throughout Europe and Asia as the security standard to be followed.

If you aren't into researching an ISO standard and how it applies to your shop, here are some suggestions:

- If you haven't got a security policy, now's the time to develop one. A well-written security policy assigns responsibility for various actions and clearly spells out what is acceptable behavior (and what is not)

- Move the responsibility for determining who can access data (financial and otherwise) from IT to the data owner. IT should be the custodian and implementer of the data owner's policies. It should not be the one making the policy.
- Implement the concept of "least privilege." That is, only give users access to data and applications that have a direct need. To relate this directly back to Sarbanes-Oxley, say that you have an AR (Accounts Receivable) or AP (Accounts Payable) application running on your system. With few exceptions, why should anyone outside of the Accounting department need access to this financial data? The Accounting department can be given explicit authority to the application libraries and individual exceptions can also be given explicit authority. Then the libraries containing the application can be secured – that is, set to *PUBLIC *EXCLUDE preventing the rest of the company – those without a "need to know" – from accessing this financial information.
- Turn on OS/400 auditing to provide a track-record of what has occurred on the system.
- Document your processes. SOX is all about making sure the proper controls are in place. So auditors are typically looking for IT processes to be documented. Examples include the process HR uses to communicate to IT when an employee leaves the company, how requests for access (to OS/400) are approved and processed, etc.
- If you decide that your security scheme needs an overhaul, document the current settings, document your step-by-step remediation plans and get management sign-off on the plans before changing any settings.

For More Information

Before you g swept up in the Sarbanes-Oxley furor over its implications on IT, I encourage you to do some research of your own. I've found the explanations of the Act at www.sarbanes-oxley.com to be very insightful and helpful in clarifying the issues and the intent of the Act. The site http://www.corpgovonline.com/ provides timely news regarding the Act and has a good document which discusses Frequently Asked Questions regarding "internal controls." And if you'd like some good bedtime reading, the Sarbanes-Oxley Act itself can be found at http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf

Carol Woodbury is co-founder of SkyView Partners, a firm specializing in security consulting and remediation and the assessment product, SkyView Risk Assessor for OS/400 and i5/OS. Carol has over 14 years in the security industry, 10 of those working for IBM's Enterprise Server Group as the AS/400 Security Architect and Chief Engineering Manager of Security Technology. Carol can be reached at carol.woodbury@skyviewpartners.com