ASSISTANCE IN ACHIEVING SOX AND PCI COMPLIANCE THROUGH SCO PROFESSIONAL SERVICES

WHY DO I NEED TO BE CONCERNED ABOUT SOX?

Sarbanes-Oxley legislation of 2002 (SOX) section 404 is the IT portion of the SOX legislation. Simply put, it stipulates that a company's management must attest to the accuracy and reliability of their annual public financial disclosures. It is now a fundamentally important part of their annual financial audit.

WHAT IT AREAS HAVE THE SOX ACCOUNTING COMMITTEES DETERMINED TO BE THE MOST IMPORTANT TO EVALUATE?

Although it would be nice to have a very specific and definitive list of IT areas to evaluate, neither the formal SOX legislation nor any associated implementation frameworks generally regarded as acceptable in the accounting community have constructed or approved such a list.

The Public Company Accounting Oversight Board (PCAOB), the authoritative accounting committee founded as a result of SOX, oversees the auditing practices of public companies and has determined—through "control frameworks" such as the Committee of Sponsoring Organizations of the Treadway Commission, a private sector initiative dedicated to improving the quality of financial reporting (COSO), and Control Objectives for Information and related Technology, an open standard for IT control and security (CobiT) — that there are several broad areas of control over financial reporting which impact IT most critically. Thus the following areas of IT may be viewed as a partial interpretation of "accuracy" and "reliability" of financial reporting, as stated in Section 404, within the IT realm:

- ***Security***
- ***Data integrity***
- ***Change control***
- ***Application control***

The SOX-related offerings of SCO Professional Services provide significant, specific enhancements in all the above areas.

The PCI standard has much more specific IT related information and requirements within it. How do SCO products and the SCO Professional Services offerings satisfy the requirements stated in the PCI standard?

Most of the PCI standard, as it applies to a UNIX host, are satisfied by features that already reside within currently shipping SCO products. In some cases, however, the enhancements offered by Professional Services are needed. For example:

- ***PCI requirement #1: Build and maintain a secure network***

The latest SCO operating systems have the ipfilter firewall to restrict data flow on the network, and ipsec to secure the data flow which IS allowed to flow. However, these software components can be backported and customized to earlier versions of SCO operating systems by Professional Services.

- ***PCI requirement #6: Develop and maintain secure systems and applications***

SCO provides security patches on a timely basis for all currently shipping products. However, SCO Professional Services can provide a customized patch distribution tool which can detect the presence of new security patches and automatically distribute them to all SCO systems in your network.

More on next page

> *PCI requirement #10: Track and monitor all access*

SCO provides both system-level auditing and standard syslog logging. However, logging administration can be considerably enhanced by log integration using the MySQL database through the customized enhanced event logging system (EELS) software provided by SCO Professional Services.

> *PCI requirement #11: Test security systems and processes*

SCO provides a configurable file integrity monitor, the File Update Daemon, on UnixWare systems. However, file integrity monitoring can be enhanced by porting an intrusion detection system (IDS) such as Tripwire or AIDE; SCO Professional Services can do this.

WHY DO I NEED CENTRALIZED USER ACCOUNT ADMINISTRATION?

The SOX requirement for application control may dictate that users of critical applications be carefully identified, controlled, and monitored. By centralizing user accounts, you can ensure uniformity and consistency of user accounts over all SCO systems in your network, making it much easier to identify the range of users on these systems. The SOX requirement for change control may dictate that when user accounts are added, deleted, or modified, there must be a well-defined process for doing this on all systems. Centralizing account administration ensures that this process is simple, well-defined, and consistent. PCI requirement #8, pertaining to assignment of unique user IDs, may be greatly facilitated by centralized assignment of user IDs.

WHY DO I NEED LOG INTEGRATION?

The SOX requirement for application control may dictate that you carefully record critical processes involved in application and transactional flow, through syslog logging, process accounting logging, and system auditing, and that you demonstrate maintainability and manageability of the large amount of data inherent in such activities. EELS, customized by Professional Services, integrates syslog, pacct, and auditing into a MySQL 4 database, and provides a log server/client model for merging all log data onto a log/database server on the network. PCI requirement #10 to track and monitor access to data calls for system level logging and auditing, and for review and maintenance of these logs.

WHY DO I NEED A FILE INTEGRITY MONITOR?

The SOX requirement for data integrity and PCI requirement #11.5 may dictate that you employ a host-based intrusion detector such as AIDE or Tripwire, which SCO Professional Services can port to your SCO-based platform.

WHY DO I NEED A TOOL FOR AUTOMATIC UPDATING AND DISTRIBUTION OF SECURITY SUPPLEMENTS?

The SOX requirement for change control may dictate that you employ a well-defined, centralized process for detection and distribution of software updates and changes. The SOX requirement for security may dictate that you address security vulnerabilities via security patches in a timely fashion, through the same process. PCI requirement #6 stipulates the timely updating of systems to address security vulnerabilities and the maintenance of a vulnerability management process which may be greatly facilitated by such a tool.

Need SOX/PCI compliance assistance? Contact SCO Professional Services to learn how we can help.

Professional Services provides expert advice for designing and deploying IT solutions, in addition to SOX/PCI consulting. After more than two decades of planning and implementing deployment strategies, SCO has gained a stellar reputation as industry-leading consultants with professionalism, problem-solving skills, creative and innovative solutions, and attention to detail.

consulting@sco.com

For more information please click www.sco.com/consulting

SCO LOCATIONS WORLDWIDE

CORPORATE OFFICES LINDON, UT
1.800.SCO.UNIX
Tel: +1 801 765 4999
Fax: +1 801 765 1313
info@SCO.com www.SCO.com

Please visit www.SCO.com/worldwide to see additional SCO locations around the world.

FOR MORE INFORMATION, contact your local SCO sales representative, or:

In the Americas, phone
1-800-SCO-UNIX (1-800-726-8649)
or 1-800-726-6561

In the rest of the world, phone
+44 8700 994 992