

Insight into...

## Sarbanes-Oxley Compliance

White Paper

Executive summary:

**Sarbanes-Oxley regulations have a widespread impact on publicly held companies.**

**The regulations are complex and require significant reporting on the processes in place that guarantee the integrity of financial reporting data. Solutions from eIQnetworks provide a comprehensive solution to assist in meeting the demanding monitoring, reporting and alerting requirements of the Sarbanes-Oxley regulations. This Whitepaper discusses the solutions and how they can provide insight into meeting Sarbanes-Oxley regulations.**

eIQnetworks, Inc. ("eIQ") makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. eIQ reserves the right to revise or modify the contents of this document at any time. This document contains information, which is the property of eIQnetworks, Inc. eIQ reserves the right to make changes without notice.

eIQnetworks, SystemAnalyzer, and Network Security Analyzer are either registered trademarks or trademarks of eIQnetworks, Inc. Microsoft, Windows NT, Windows 2000, Windows XP and Windows 2003 are either registered trademarks or trademarks of Microsoft Corporation. Other product or company names mentioned herein might be trademarks of their respective owners.

## Overview

Section 404 of the Sarbanes-Oxley act documents specific regulations required for publicly traded companies to document the Management's "Assessment of Internal Controls" over security processes. The overall requirements of the regulations can be summarized as: (1) documenting commitment to a process, (2) documenting the effectiveness of the process that's in place, and (3) documenting an auditor's assessment of the company's assessment of the process that's in place. There are many aspects of Sarbanes-Oxley that are beyond the scope of this Whitepaper; however, it does cover monitoring and reporting processes from eIQnetworks that help meeting some of the documentation requirements of the regulation.

## Documentation Requirements

In general, the actual process requirements of Sarbanes-Oxley regulations are vague. It generally states that it requires that a process is in place and that the process is shown to be effective by management, but it does not define the process itself. As part of the requirements, it can be assumed that a security management process must exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information. Breaking this requirement down further, an organization should be able to assess the following types of "security events":

- Failed system level login attempts
- Failed application level login attempts
- Exploitation of a system by a virus or worm
- Exploitation of a system by unauthorized individuals (i.e. hacking)
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

## How to proceed

The good news is that both firewall and server systems provide sufficient data for assessing these types of security events. The data is reported by these systems in various audit trails called log files. At first these log files seem insurmountable because they are often very large without any consistent format across different systems and applications. However, solutions from eIQnetworks, including SystemAnalyzer and Network Security Analyzer, provide advanced collection, monitoring, reporting and

event generation across the most popular firewall, server and application systems. The following sections show some of the advanced reporting to help comply with the Sarbanes-Oxley regulations.

An important attribute of the solutions from eIQnetworks is the ability to "Normalize" the information across multiple, possibly disparate, systems. Through the patent pending process FScale, eIQnetworks is capable of collecting and correlating information from multiple, often times different, systems.

## Breaking It Down Further

*eIQnetworks' SystemAnalyzer provides the following information for Sarbanes-Oxley reporting:*

- Failed Login Attempts (system and application)
- Account Misuse
- Changed Passwords
- Account Lockouts
- Deleted/Disabled Accounts
- Security Group Modification
- Loading and Unloading of Drivers
- File and Directory Ownership Changes
- Log File Modification

*In addition, eIQnetworks Network Security Analyzer provides the following reports:*

- Virus activity on the network
- Network intrusion attempts

## Conclusion

Being compliant to regulations is often-times complex. There are usually two sides to meeting a regulation: (1) showing that a procedure is in place to guarantee the integrity and access to information and (2) processes are in place to audit these policies. Solutions from eIQnetworks can help a company put a process in place to audit and report on the integrity and access to the protected information, as required under Sarbanes-Oxley.

*For more information contact us at*

**eIQnetworks, Inc.**

31 Nagog Park, 3rd Floor

Acton, MA 01720

Toll Free: 877-LOGS-R-US (877-564-7787)

Tel: 978-266-9933

Fax: 978-266-0004

e-mail: sales@eIQnetworks.com

Copyright © 2001-2005 eIQnetworks, Inc. All rights reserved