White Paper

Achieving SOX Compliance through Security Information Management

netForensics®

Contents

netForensics®

Executive Summary

Signed into law by the federal government in 2002, the Sarbanes-Oxley Act (SOX) was enacted following a number of major corporate and accounting scandals involving prominent U.S. companies. With a decline of public trust in accounting and reporting practices, SOX was designed to protect investors by improving the accuracy and reliability of corporate disclosures made in accordance with securities laws. SOX standards must be followed or strict penalties for noncompliance can result.

According to the U.S. Attorney General, "The Act provides tough new tools to expose and punish acts of corporate corruption, promote greater accountability by financial auditors, and protect small investors and pension holders… The United States Department of Justice will play a critical role in implementing the Act and in helping to restore confidence in America's corporations and financial markets." [1]

Properly implemented, a best-practices security information management (SIM) solution provides organizations reliable identity management, security monitoring, and incident management processes surrounding financial applications and data, and the IT systems that support these processes. Additionally, a SIM solution can support a company's broader corporate objectives:

> *"…if companies view the new [Sarbanes-Oxley] laws as opportunities—opportunities to improve internal controls, improve the performance of the board, and improve their public reporting—they will ultimately be better run, more transparent, and therefore more attractive to investors," says SEC Chairman William Donaldson.* [2]

SIM can enable companies to meet SOX regulatory compliance directives of accountability, internal controls, and reporting. By deploying netForensics' nFX Open Security Platform (nFX OSP) for SIM, companies are equipped with a full range of tools for fulfilling SOX compliance requirements.

Introduction: Brief Overview of SOX

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002, and commonly called SOX or SarbOx, is a United States federal law related to corporate governance and financial disclosure. Representing the biggest modification to federal securities laws in decades, SOX provisions detail criminal and civil penalties for noncompliance, certification of internal auditing, and increased financial disclosure.

The legislation is wide ranging and mandates new or enhanced standards for all public U.S. companies, public accounting firms, and firms providing auditing services, along with non-U.S. companies with a U.S. presence. The sections of SOX most relevant to IT professionals include the following:

- Section 302—Corporate Responsibility for Financial Reports. Public company officers must confirm the reliability of quarterly and annual financial statements.
- Section 404—Management Assessment of Internal Controls. All publicly traded companies must submit an annual report to the SEC on the effectiveness of their internal accounting controls. The independent company auditor must also attest to the accuracy of the report.
- Section 409—Real-Time Issuer Disclosures. Public companies must stay abreast

of and declare changes in their financial condition or operations within 48 hours of material events.

- Section 802 & 1102—Corporate and Criminal Fraud Accountability. Public companies can face criminal penalties for altering or destroying financial documents.

Of these sections, IT organizations largely focus their SOX compliance efforts on meeting the requirements of Section 404. Working in coordination with executive management, IT groups must ensure that an internal control framework can adequately assess internal control structures and financial reporting procedures, thus protecting and maintaining critical financial data.

The SOX Challenge: Improving the Accuracy and Reliability of Financial Reporting

SOX details provisions for corporations, including: a public company accounting oversight board, auditor independence, CEO/CFO responsibility, and enhanced financial disclosure. In particular, the SOX legislation establishes that public companies need extensive internal control systems in place for managing and reporting on financial data, as well as monitoring and securing user activities surrounding the data and ensuring security of the data itself.

Though SOX can have a positive effect on corporate governance by improving the accuracy and reliability of financial data, compliance presents significant challenges for organizations, and particularly IT organizations. Internal control requirements fall on IT groups since much of a company's financial data resides on network servers. So IT departments must provide detailed information to internal and external auditors about their financial reporting procedures and control structures. Network administrators need to be able to leverage existing technology and tools to manage and report on access controls across the enterprise, and provide tangible evidence of their security efforts.

SOX demands accountability and requires each organization to examine the adequacy and effectiveness of their entire approach to information security. To be effective, an information security solution should be able to demonstrate at any point in time that security policies and safeguards are in place and functioning. The solution should also ensure that all of the applications and databases that affect a company's financial position are secure.

The protection of financial information is a complex task requiring a broad security strategy. Organizations are faced with the enormous task of not only achieving SOX compliance—but also maintaining it year after year. From a security governance perspective, organizations must actively participate in the following to comply with SOX:

- Determine if an audit trail exists of all emergency activity and that it is independently reviewed.
- Ensure that the IT security administration monitors and logs security activity and identified security violations.
- Review a sample of problems or incident reports, to consider if the issues were addressed (recorded, analyzed, and resolved) in a timely manner.
- Determine if the organization's procedures include audit trail facilities for tracking of the incidents.
- Review a sample of problems recorded on the problem-management system to consider if a proper audit trail exists and is used.

- Ensure that system-event data are sufficiently retained to provide chronological information and logs to enable the review, examination, and reconstruction of system and data processing.
- Determine if sufficient chronological information and logs are being recorded and stored and are useable for reconstruction of the system if necessary. Obtain a sample of log entries to determine if they sufficiently allow for reconstruction.

Though no single software product can enable full SOX compliance, the right SIM technology can help companies efficiently manage internal controls. An effective security management solution provides public companies the tools to implement, maintain, and report on internal access and security controls with minimal utilization of resources.

Security Information Management: The Foundation that Enables SOX Compliance

Today, the financial reporting processes of most organizations are driven by IT systems. Though federal regulations do not dictate the particular technologies that a company must employ to fulfill SOX compliance obligations, IT clearly plays a vital role in compliance and especially internal control. The Public Company Accounting Oversight Board, a private-sector, non-profit corporation created through SOX to oversee the auditors of public companies, states:

"The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting." [3]

A comprehensive and specific approach to meeting compliance with SOX requirements must start with leveraging the right SIM solution—one that enables real-time monitoring and historical, on-the-fly reporting. But technology alone is not the answer. An in-depth approach that integrates existing assets—including people, processes, and policies—with technology is the most viable means to successfully attaining compliance.

Assuming the following responsibilities to prove diligence in managing information security risk helps organizations meet SOX requirements, as well as those of other privacy and security regulations:

- Define a policy-driven security management program that can be incorporated early on into business processes — Identify the people and technology controls needed to satisfy the organization's security mission and ensure compliance. Also, ensure that security initiatives are integrated into business processes at their onset, rather than after the fact.
- Validate security controls — Provide for the monitoring and reporting of controls on human actions and decisions, process controls, and information technology controls.
- Implement a risk management approach to information security — Comprise active monitoring of risk as defined and measured by key control indicators (KCIs) and key risk indicators (KRIs), correlating the relative value of information assets, the threats to the confidentiality, integrity, and availability of the assets, and the vulnerability of the systems and architecture that store and carry the assets.
- Demonstrate due diligence in the application of internal controls — Create a link between the security infrastructure and policy by capturing all security events from all network hosts, devices, and assets in an auditable database.

- Develop and implement an effective security-incident management process — Demonstrate that the proper steps were taken to correct systems and adjust policy if a non-compliant situation is identified.
- Enable reporting that can help demonstrate compliance — Demonstrate the ongoing security of compliance-related assets over a period of time, recreating the organization's security posture in the event of an audit, and enabling security performance management against metrics that can be leveraged for corporate governance initiatives.
- Establish capabilities for archiving and data preservation — Preserve near-term and long-term data in its purest form for forensics and evidentiary presentation.

By implementing effective, comprehensive policies and procedures for establishing accountability and consistent reporting practices, organizations can successfully meet SOX regulatory compliance directives.

The Case for Security Information Management

Career Education Corporation (CEC), based in Hoffman Estates, Illinois, is tasked with managing information security across 80 geographically distributed schools. The $1.5 billion provider of post-secondary education needed to find a security solution to manage vulnerabilities, improve its overall security posture, and provide the security monitoring to ensure SOX compliance.

CEC successfully installed the nFX OSP software, integrating and correlating security data from a wide variety of devices and custom applications. Through nFX OSP, each school is equipped with visual data portals that enable accountability for self-reporting and analysis, while CEC is able to centrally manage security operations by collecting event data from disparate security devices. With risk-based analysis, real-time monitoring, and in-depth reporting, CEC can meet the auditing requirements of SOX.

The netForensics Solution: Aligning with SOX Objectives

netForensics enables an efficient strategy for examining the adequacy and effectiveness of information security policies, procedures, and practices. nFX OSP automates the collection and correlation of the immense volumes of data created through security initiatives. The platform also provides periodic assessments of the risk and degree of harm that could result from unauthorized access, modifications, or destruction to information and information systems that support the operations and assets of the organization, as required by SOX.

More specifically, nFX OSP provides organizations the following tools and technologies to meet SOX requirements:

- Compliance dashboards that provide real-time monitoring of the status of an organization's security posture at the network, asset, and business unit levels.
- Embedded knowledge base that provides guidance in analyzing, documenting, and reporting on security issues, including newly discovered vulnerabilities, malware, and vendor-specific vulnerability data.
- Centralized application and device monitoring tool, enabling comprehensive collection, correlation, analysis, reporting, and retention of audit events from disparate applications, security devices, network devices, servers, and desktops, thus transforming data into actionable intelligence.

- Security operations performance measurement, with reports that focus on vulnerability, threat, and incidence response for all compliance-related assets in the enterprise.
- Risk assessment based on asset value, threats, and vulnerabilities.
- Incident-resolution management, integrating incidence response processes with existing enterprise workflow systems, and thus enabling accelerated incidence response through its collaborative approach.
- Strong correlation of intrusion-detection system events, including vulnerability correlation, statistical correlation, historical correlation, and rules correlation.
- Detection and reporting on viruses, worms, and other malicious code; on all system status and configuration changes; and on privilege and authorization changes.
- A highly scalable and redundant security architecture that grows as organizations grow, and changes as business needs change.

Using these tools and technologies, IT organizations can effectively manage information security, and consequently demonstrate SOX compliance.

Conclusion

SOX requirements have elevated the need for organizations to improve the security of IT systems, applications, and data. SOX calls for leveraging information-security best practices to meet numerous objectives related to corporate governance and financial disclosure, including CEO/CFO accountability, authority, and oversight of compliance. Executive management needs to work closely with IT organizations on risk assessment and the implementation of security policies and operations. Overall, a security program that integrates people, policies, process, and technology is the best approach to meeting SOX compliance.

A fully implemented SIM solution like nFX OSP, along with alignment of human, process, and information controls, enables organizations to meet SOX objectives. By leveraging existing technology and tools, organizations can identify, assess, and report on the status and security of financial-related processes and information, and can provide tangible evidence of their information security initiatives.

References

1. “Memorandum for the Director, the Federal Bureau of Investigation; the Director, Executive Office of United States Attorneys; All United States Attorneys; All Special-Agents-in-Charge: Implementation of the Sarbanes-Oxley Act of 2002.” Office of the Attorney General. Washington, D.C. 1 Aug. 2002.

2. Chairman William H. Donaldson, U.S. Securities and Exchange Commission. Remarks to the National Press Club. Washington, D.C. 30 Jul. 2003 <http://www.sec.gov/news/speech/spch073003whd.htm>

3. PCAOB Release No. 2003-017. “Proposed Auditing Standard – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.” 7 Oct. 2003 < http://www.pcaobus.org/rules/docket_008/2003-10 17_release_2003-017.pdf>

About netForensics

netForensics transforms all security related information into actionable intelligence, enabling more than 450 enterprises and government agencies to better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes.

By harnessing the power of our award-winning Security Information Management platform that manages more security events at more organizations than any other product in the marketplace, we help customers deliver security management solutions that rely on the availability of timely and relevant information security information.

We facilitate these actionable security intelligence (ASI) solutions by rationalizing security information from strategic applications and critical compliance-related assets, as well as the perimeter devices that protect them. ASI solutions make this information available to technology domains and users within the security organization and beyond — by unifying network and security organizations, while supporting IT governance, enterprise compliance, and risk management initiatives.

200 Metroplex Drive • Edison, NJ 08817 • p 732.393.6000 • f 732.393.6090
www.netforensics.com • info@netforensics.com