

Improving Sarbanes-Oxley Internal Compliance with Effective Content Protection Controls

Business White Paper

Robert R. Moeller



***Inspect** Content Flows.*

***Detect** Unauthorized Disclosures.*

***Avoid** Costly Compliance Incidents.*

***Protect** Your Reputation.*

Table of Contents

Introduction	1
“Reasonable Assurance” Requirements – Impact on Senior Management	1
Information Loss and the ChoicePoint Security Breach	2
Preventing and Detecting Private Information Loss Breach	2
Internal Controls and SOX Section 404 Requirements	3
SOX Section 302 Requirements	4
SOX and Content Protection Controls	4
Implementing Effective Content Protection Controls	5
Conclusion	7

ABOUT THE AUTHOR

Robert R. Moeller is an expert and consultant specializing in compliance issues and internal controls. He has led teams to help organizations achieve Sarbanes-Oxley compliance and also is the author of several books including *Sarbanes-Oxley and the New Internal Auditing Rules* and *Brink’s Modern Internal Auditing, 6th Edition*, both published by Wiley. Moeller has an MBA in finance from the University of Chicago and has accumulated a wide range of professional certifications including the CPA, CISA, PMP, and CISSP.

INTRODUCTION

A key requirement of the Sarbanes-Oxley Act is the definition, documentation, implementation and assessment of effective internal controls. These controls are seen to ensure the integrity of corporate financial information and the prompt reporting of material events which may affect the financial performance of the firm. While initial compliance efforts have been focused largely on financial reporting, this paper argues that the scope of Sarbanes-Oxley is far broader and requires corporations to develop effective internal controls for protecting their key digital assets in a number of areas. We refer to these controls as “Content Protection Controls”.

The paper begins by discussing content protection controls from a senior management perspective. It then presents a more detailed discussion of compliance issues associated with digital assets and introduces a new class of information technology product designed to automate content protection policies with continuous monitoring of corporate content flows.

“REASONABLE ASSURANCE” REQUIREMENTS – IMPACT ON SENIOR MANAGEMENT

The Sarbanes-Oxley Act (SOX) places new levels of responsibility on enterprise management and has been viewed as particularly impacting Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs). While these senior managers once just informally told their board of directors, its audit committee and external auditors that their internal controls were “adequate”, today they must document, assess and test those internal controls under SOX Section 404 rules. In addition, taking words directly from SEC regulations referenced by the SOX legislation, senior financial management is required to “provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statements.” (United States Security and Exchange Commission — Regulation 13A) These provisions of SOX also directly affect IT management professionals including Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and Chief Risk Officers (CROs), who are managing the automated internal control processes to build and establish appropriate information integrity and security controls in support of the SOX rules. Senior IT management now has responsibilities to provide better tools to bolster the CEO and CFO in their SOX internal controls assertion requirements.

This “reasonable assurance” requirement places broad responsibilities on financial and IT management. SOX’s broad category of “assets” requiring protection includes digital assets such as computer program source code, trade secrets, corporate financial information, patent information and any other category of sensitive information where unauthorized disclosures could have a negative impact on the company’s stock price or its financial integrity. Thus, organizations are required to closely monitor the usage of those digital assets and be able to detect leakage events in real time or near real time.

“Data is becoming an asset which needs to be guarded as much as any other asset. The ability to guard ... data is the key to market value, which the board is responsible for on behalf of shareholders.”

- Haim Mendelson

The General Atlantic Partners
Professor of Electronic Business and
Commerce, and Management,
Stanford Graduate
School of Business

Quoted in *The Economist*
June 25, 2005

INFORMATION LOSS AND THE CHOICEPOINT SECURITY BREACH

News accounts regularly report on information security breaches, such as the actions of hackers who break into a computer network to steal data or an employee who improperly reveals customer account data. Based on survey results, the Computer Security Institute estimates that the loss of proprietary business information and intellectual property by employees and other trusted insiders cost businesses over seventy billion dollars in 2005. Industrial espionage and the theft of proprietary intellectual property by employees is emerging as a major concern. Sometimes, the loss event appears to be just a case of sloppy internal controls. For example, in March, 2005, Bank of America announced that backup computer tapes containing information on 1.2 million of its customers were missing. The consequences of these events have ranged from attempts to locate and prosecute the hacker to a major public relations “black eye” for the enterprise. Although in violation of the SOX Reasonable Assurance guidelines discussed above, these types of information theft exposures often have not had major consequences. The recent ChoicePoint security breach has really changed the playing field.

ChoicePoint, Inc., based in the Atlanta area, is a data brokerage company that sells information and data services to the insurance industry, government agencies, direct marketers, and other businesses. Describing itself on its web site as “the nation’s premier source of data to the insurance industry,” ChoicePoint has gathered over 19 billion records about virtually every adult in the United States.

In 2004, a criminal who claimed to be a collection agent was allowed to access and download a massive amount of customer information. The fraudster was apprehended, and ChoicePoint announced that they had informed 145,000 individuals that their personal information had been stolen. However, the SEC investigated this massive data security breach as well. The result was a \$10 million fine against ChoicePoint, a requirement the company set up a \$5 million trust fund to protect other data loss victims, and a requirement for a massive security monitoring program¹. ChoicePoint’s market capitalization fell significantly after this breach and ChoicePoint reported the breach and several lawsuits that it generated in its 10-K filed for the fiscal year ended December 31, 2004. Although ChoicePoint was charged under the Fair Credit Reporting Act (FCRA), the SEC charges that “it did not have reasonable procedures in place” to protect its data, sounds very much like the requirements of SOX.

PREVENTING AND DETECTING PRIVATE INFORMATION LOSS

Preventing and detecting the loss of private information becomes much more complex as more information is stored in digital format and as technology advances provide more varied and inexpensive ways to copy it and transport it. Critical data can be easily transmitted outside of the enterprise through an email message or uploaded to an external site. While an enterprise wants to support the free exchange and transmission of the data and information to appropriate persons, this same material should not be allowed to fall into improper, unauthorized hands. An enterprise needs to implement monitoring capabilities, policies and protections against:

- Loss or leakage of key business information: There are always risks that plans, analyses, financial reports, strategy documents or documents can be stolen or inadvertently shared with others via email or the web.
- Loss or leakage of key intellectual properties: Similar to business information, the loss of intellectual property can often present a greater risk. This category of information can include such items as research results, product plans, computer source code, digitized design documents, or even internal progress reports. It is increasingly the target of industrial espionage efforts—both planned efforts and spontaneous efforts conducted by disgruntled employees. Sometime treated with a lower level of formal security restrictions than business information, an enterprise faces risks if these documents are stolen or shared with others. For example, if information used to support a patent application is disclosed before the patent is granted, it can threaten the validity of the patent as

¹ *Computerworld*, January 26, 2006

well as millions of dollars of research and development effort.

- **Loss of customer information:** Whether key statistics or names and identifying information of actual customers, there are information property risks. The loss of some customer-related information—such as Social Security numbers in the U.S.—can place the enterprise in legal risk as well.
- **Violations of government regulations:** Legislation such as the Health Insurance Portability and Accountability Act (HIPPA) require an organization to protect the security of certain key data and the Sarbanes-Oxley Act (SOX) calls for material financial-related issues to be reported to the SEC. In addition to government regulations, many other organizations have governance provisions relating to the protection of sensitive information. For example, New York Stock Exchange rule 303a.10 states that all employees of listed companies must maintain the confidentiality of all non-public information.

This list can go on, but there are many areas where an enterprise can suffer anything from legal liability, to loss of information assets and public embarrassment when faced with the loss of critical information assets. The process of monitoring and managing this critical data and information is known as content protection management, a key internal control vulnerability area that should not be overlooked.

INTERNAL CONTROLS AND SOX SECTION 404 REQUIREMENTS

Besides prohibiting external auditors from having their own consultants install the applications they are to subsequently audit, SOX shifts the responsibility for the accuracy and integrity of internal controls back to the enterprise and its senior management. The enterprise is now responsible for understanding and documenting its key processes and then performing tests of those processes to determine that they are operating effectively. SOX requires the enterprise to maintain an effective system of documented internal controls, to test those controls to determine that they are working, and then to pass the results of those tests of their internal controls to their external auditors who will use them to produce their audited financial reports. Any breakdown in this internal controls evaluation process could cause the internal controls deficiency to be reported in the annual financial reports and risk a potential enforcement action.

As we have previously mentioned, the SEC regulations referenced by the SOX legislation require the enterprise to “provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statement.” The term “registrant’s assets” includes both traditional “hard” assets such as plants and equipment and “soft” digital assets such as the previously mentioned customer lists, product specifications, or any of the many forms of data and information found within various IT files and systems. Registrant refers to an enterprise with securities filed with SEC and, thus, subject to SOX.

Wedded too closely to financial accounting issues, enterprise managers often take too narrow a view of this concept of assets. They too often think of their organization’s assets only in terms of the traditional hard assets that can easily be recorded on the balance sheet, and too often ignore their many valuable forms of soft, digital assets. As the economy increasingly becomes more knowledge-driven, these “soft” digital assets are increasingly important in terms of ability to innovate, time-to-market and competitive advantage. Confidential intellectual property content such as research findings, new product designs, manufacturing processes, source code embedded in products or test results are also important types of enterprise assets. These intellectual property assets are increasingly stored in digital format and are susceptible to being easily transmitted outside the organization—either by accident or through malicious intent. An enterprise is responsible, under SOX, for monitoring the usage of all of these assets and then reporting on any inappropriate activities surrounding them.

The SOX assessment of internal controls—including controls over both traditional hard and digital soft assets—is known as a Section 404 review. Although the SOX legislation calls for continuous monitoring, these reviews are too often just tied to the quarterly and annual financial reporting process and tend to focus on the hard assets. With the legislation becoming effective and with some time for establishing compliance, many enterprises have just become

Section 404 compliant, but have not yet established continuous monitoring processes. We should see much more attention to this continuous monitoring process in the periods going forward.

SOX SECTION 302 REQUIREMENTS

Another equally important part of SOX and one that includes the same previously mentioned content protection concerns is SOX Section 302. This is a requirement that key management—usually the CEO and CFO—must disclose whether there were any significant changes in the enterprise’s internal controls within 90 days of their financial report filings. This places a legal responsibility on the CEO or CFO to formally make declarations regarding any internal control weaknesses or breakdowns prior to the financial report filings. As an example, if an organization suffered a significant loss of new product design documents through a leakage incident, the CEO or CFO is required to disclose that potentially materially significant event prior to filing financial reports as part of Section 302 requirement. Failure to disclose such an event could even result—at the extreme—in criminal actions against the responsible enterprise officer.

SOX AND CONTENT PROTECTION CONTROLS

As we have seen, a significant loss or leakage of key financial or other significant content could be easily considered to be a significant internal control weakness to the enterprise that is required to be disclosed following SOX rules. To protect from such a disclosure, the enterprise must have effective policies and monitoring processes—i.e. content protection controls—in place to prevent or detect such an event. In addition, there should be appropriate risk management controls such that the impacts of any loss can be quickly assessed. If significant, they should be communicated up through the enterprise chain of command for proper action or potential disclosure.

To date, most SOX disclosures have covered financial or accounting issues such as an enterprise’s failure to recognize certain types of financial obligations or the improper booking of sales revenue. Security and data integrity problems have been kept within the enterprise, not considered necessary for formal, public disclosures. This could very much change in the event of significant damage from the loss of information assets. If some organization had lost, through an outbound content breach, a large set of information covering a planned financial transaction, that loss should have been identified as a significant internal control weakness and should have been disclosed. If a large enough breach, the investment public might be very well asking questions about why the matter had not been disclosed and why the SEC had not been asking appropriate questions.

A major content security internal controls breach, as described, could very much change everyone’s attention to the SOX disclosure rules. This could very much change the duties and responsibilities of an enterprise’s security specialists, IT management, internal audit, and senior financial management. This situation is not unlike the fall of Enron when there were lots of questions, among others, about why did Enron’s Audit Committee as well as its external auditors miss all of this? Of course, the outcome was a large set of new rules that became parts of SOX. For the possible significant content security internal controls breach, we already have the rules in place. A major incident would just direct a lot of attention to enforcing those rules.

Many enterprises today have established effective information security control procedures as part of an effective IT application controls environment as well as for their SOX Section 404 requirements. Those established control procedures, however, often do not give sufficient attention to this significant area of protecting sensitive content. Traditional risk management professionals too often think more in terms of published procedures and paper documents, while IT professionals may be aware of some of the automated tools available but have not installed them.

With the ever-increasing risks of significant data losses and leaks, an enterprise should consider installing effective content protection controls and tools. Because of the overall risks facing an enterprise, content protection controls

should be installed at a level to keep the organization in compliance the SOX Section 404 rules and to promote good organizational governance procedures.

IMPLEMENTING EFFECTIVE CONTENT PROTECTION CONTROLS

To effectively protect sensitive content in a compliant manner, an enterprise must implement a set of policies and an automated technology solution to continuously monitor enforcement of those policies. Because of the many and varied lines of business and types of digital assets used, there is no single path to content protection that fits all situations. However, an enterprise that is looking to implement effective content protection controls should consider the following steps:

❖ Identify high-value content at risk

There are multiple areas where an enterprise might have significant levels of unprotected information assets where they do not realize their significance or legal importance. A good first step is to understand and document these various types of information assets and the current control procedures in place. A corporate risk management function, with their emphasis on risk likelihood and significances, can help here. However, risk functions too often think primarily in terms of risks for hard assets rather than the soft or data assets that may impact an enterprise. A team involving risk management, IT and internal audit might be appropriate here. While SOX rules almost too often consider internal controls and data assets in terms of financial controls, any content protection survey should consider all data assets—financial and operational.

❖ Implement digital asset classification rules

Any content protection survey will almost always result in a long list of information assets for the enterprise that could be at risk. Using risk management techniques, an enterprise should look at all of the identified data assets and decide which are the most vulnerable and should receive priority for content protection controls. The legal department as well as risk management can provide some guidance here. Special scrutiny should be given to content stored in a document management or content management system since this is likely to be of high value. Since an enterprise will almost certainly not be able to establish content protection controls over all data assets, they should have a formal, documented record outlining why they decided one set of content assets are at a higher, more immediate corrective actions level than others. This is essential if there is ever a SOX compliance or legal liability issue in the future.

❖ Select and implement appropriate content protection technology

Sensitive content losses or leakage incidents can occur at many levels including accidentally posting sensitive information on a public web site or e-mailing sensitive information to a personal, web mail account. Traditional IT control procedures such as identity management and access control lists are necessary, but not sufficient. Several new and very promising automated tools are becoming available to monitor and control content risks and vulnerabilities. Analysts refer to these tools as content monitoring and filtering tools or as information leak prevention tools. Typically, these tools register or fingerprint sensitive content stored in the file system or in content management repositories. Installed at an organization's Internet gateway, they then monitor all of the content flowing out of organization and on to the Internet. If someone attempts to transmit sensitive information, through any content protocol, the tool will detect it and invoke a management-defined policy. Policy actions may include alerting, logging and actual blocking of the attempted transmission.

While products may vary in their capabilities, there are several critical requirements for effective content protection:

- Content Format Support: Ability to fingerprint and detect the large number of different file formats used for content in the modern enterprise including engineering drawings, image files, rich media and industry-specific application formats.

- **Derivative Work Detection:** Ability to accurately detect fragments of the original content that may be cut out and transmitted.
- **Language Independence:** Ability to fingerprint and accurately detect content written in any language and character set (including non-Roman character sets such as Japanese)
- **Content Repository Support:** Ability to register content to be protected from all storage locations and repositories including file systems, document management systems and content management systems.
- **Defensible Audit Trail:** Audit trail and reporting capabilities that meet robust auditing standards.
- **Flexible Policy Definition:** Ability to easily define policies that meet the organization's business needs.
- **Appliance Packaging:** Software and hardware bundled together for ease of installation, optimum performance and lower total cost of ownership over the lifespan of the system.

❖ **Create a culture of content compliance**

The installation and management of content protection technology is key to establishing an effective set of internal controls in this area. Violations can be monitored and investigated with any significant breakdowns appropriately reported. Appropriate content protection technology should improve an enterprise's overall internal controls structure, as outlined in SOX requirements.

However, in addition to implementing content protection technology, an enterprise needs to clearly define its content protection policies and procedures to all stakeholders – employees, vendors, and others. This is similar to employee Code of Conduct rules where a rules violator cannot claim the “I didn't know that was a rule” type of excuse in matters that were clearly addressed in the Code.

While an enterprise will want to establish some strong content protection controls such as encryption for certain kinds of data, there will always be situations where critical data can be stolen or leaked. The rules as to what types of content are sensitive and how they can be copied or captured should be defined as clearly as possible. All stakeholders should be asked to acknowledge that they have read and understand these content protection rules and they agree to abide by them. SOX guidance and good management techniques emphasize the importance of what are called “tone at the top” types of messages—the CEO and CFO who talk about the importance of following these key rules. With IT security providing some guidance, the CFO or other senior officers should voice their concerns both about content protection risks and vulnerabilities and the need for everyone to follow good internal control procedures here.

CONCLUSION

As Stanford's Professor Mendelson notes at the beginning of this paper, there is a direct thread which connects the protection of corporate information assets with a firm's market value. Employees, management and the board of directors all have a duty to protect such assets and to avoid the reputation damage, lawsuits, regulatory fines and concomitant loss of market value that can result when a significant information breach occurs.

This connection between the protection of proprietary information assets and financial performance is beginning to be recognized by regulatory bodies and by statute. This paper argues that the existing scope of Sarbanes-Oxley and its associated regulations requires corporations to develop effective internal controls for protecting their key digital assets in a number of areas. We refer to these controls as "Content Protection Controls".

Successfully implementing content protection controls is a three-step process demanding commitment and resources at the very highest level of management to:

- Define content protection policies.
- Educate employees.
- Monitor and audit policy compliance.

Fortunately, a new class of content protection technology is now available to help automate this process and make it cost effective. This technology assists managers in identifying sensitive information and developing policies to protect it. It then automatically monitors content flows and reports incidents of policy violations. Alerts of serious violations can be automatically sent to key corporate managers in the information security, legal, internal audit, and privacy and compliance functions. Trend reports can be used to fine-tune policies and demonstrate their increasing effectiveness over time. The technology can even help automate the education function—by informing employees that they have violated a corporate policy and suggesting how to be compliant in the future.

Companies that have deployed content protection technology have found that it delivers several key benefits:

- Changes the behavior of trusted employees to prevent accidental disclosures.
- Helps identify and fix poor business processes that unnecessarily expose sensitive data.
- Prevents industrial espionage by identifying and thwarting its perpetrators.
- Prevents costly and embarrassing compliance incidents.
- Measures and improves the efficacy of content protection policies.

For additional information,
please contact Code Green Networks at:

3975 Freedom Circle, Suite 900
Santa Clara, CA 95054
408.213.2300
408.213.2301 (fax)
info@codegreennetworks.com
www.codegreennetworks.com



www.altaware.com
sales@altaware.com
(866) 833-4070
Your Code Green Networks Reseller

The Code Green Networks name, logo and products are trademarks of Code Green Networks, Inc. All other company and product names, brands or service names are trademarks of their respective owners.

Notice: This document is for information purposes only and does not set forth any warranty, expressed or implied, concerning product, product feature or service offered or to be offered by Code Green Networks Inc. All information is subject to change.