



Mirrored Storage, Inc.

Data Backup and Compliance Legislation - SOX

White Paper presented by:

Mirrored Storage, Inc.

ONLINE BACKUP SOFTWARE

<http://MirroredStorage.com>

Introduction

The amount of data used by today's businesses has increased exponentially from just five years ago. Corporate scandal, international unrest, and glaring security flaws in computer operating systems and software applications have resulted in a much more intense and detailed analysis of data as it enters and leaves the enterprise. Fortune 500 companies have been vilified in the press for reckless data stewardship, and in some cases of outright fabrication of financial and performance reports. In extreme cases, executives are now lounging in Federal facilities, denying to the bitter end that they had any knowledge of the blatant misrepresentation for which they were held accountable.

The private information stores of several prestigious organizations, some of them very sensitive and personal in nature, have been lost, misplaced, or accessed by hackers – the details of the events becoming fodder for an indignant news media.

Corporate America, already under varying degrees of competitive and performance pressure, is now faced with compliance legislation and disclosure requirements that seek to right some of the wrongs done to consumers, investors, and employees alike. What follows is an analysis of the major pieces of process and data management compliance legislation, with a specific focus on the critical role that data availability plays in all of them. Access and process controls, internal and third party audits, reporting requirements and penalties for non-compliance are just a few of the areas that will be addressed on a per-measure basis.

Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act, commonly referred to as 'SOX', was signed into law on July 30th 2002, and introduced highly significant legislative changes to financial practice and corporate governance regulation. It introduced stringent new rules with the stated objective: "to protect

investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws"¹.

The legislation came about after a round of highly-publicized corporate scandals rocked the corporate world in the opening years of the new millennium; the most notable of these included the Enron collapse and subsequent revelations of accounting irregularities at WorldCom.

At the risk of oversimplifying a landmark piece of legislation and speaking strictly as it relates to information technology, data backup, management processes and disclosures, the act contains several key sections.

Sections 103 and 104 are closely related, and provide details about the length of term (7 years) that accounting and auditing entities must retain all documents and data relating to audit reports of companies required to comply with SOX. While the physical paperwork can be maintained in various ways, electronic backup of digital records is highly advisable considering that investigators usually demand all versions of documents in their analysis. With encrypted, secure offsite backup of these files, they are protected from prying eyes or malicious intent, and virtually any version of a file can be retrieved very quickly for comparison, and for building the paper trail that proves that control processes were properly followed.

Section 105 addresses the confidential nature of the accounting and audit files prepared for and received by an organization's board of directors. Again, digital backup copies are the best bet for preserving these files because they can be encrypted and compressed prior to storage, and with the best remote backup solutions, remain encrypted and compressed in storage until they are restored to the original source location. This makes it virtually impossible for the contents of these sensitive documents to become known to, or to be 'restored' by anyone other than authorized individuals – clearly a critical piece of the compliance puzzle with regards to accounting and auditing firms.

Section 302 of the eleven-section law is entitled Corporate Responsibility for Financial Reports and is important because it places the responsibility of attesting to the content, accuracy, and (perhaps most importantly) the authenticity of financial reports issued by that organization squarely on the shoulders of executive management and the board of directors at public companies.

Section 404 also involves the placement of additional responsibility on senior management and corporate officers, but has implications that extend deep into the rank-and-file of the company as well. Initially, Section 404 seems to simply require an addendum to the company's annual report. This addendum, referred to as an internal control report, states that management is responsible for maintaining an "adequate internal control structure", and is also to include an assessment by management of the control structure's effectiveness².

The loss of data from any critical systems during the reporting processes can send the entire compliance scramble into a tailspin, and at the very least the corporate stewards will be required to log this deficiency in their periodic reports. In light of the contempt with which Congress has met previous corporate cover-up activity, the permanent loss of potentially revealing data in this manner could well be seen as a federal-level 'dog ate my homework' plea.

Unfortunately, the media can act as a catalyst for speculation, spinning what might truly be an unfortunate event into a story that sends investors scrambling.

The bottom line? Compliance with Sarbanes Oxley depends heavily on reports created from sensitive data, without even the appearance of impropriety in its compilation. These reports must be generated from actual, factual data, with strict access and process safeguards all along the way and executive-authorized documentation to attest to the existence of and adherence to these safeguards. Remotely backing up the data that is crucial to the creation of these reports insures that localized hazards such as fire, theft, or opportunistic or vindictive employees are neutralized and that the mission critical reports can be drawn from original data.

Data Backup Software and Services – Access controlled Data Insurance

To be clear, there is no single software product or information technology service that can make an organization fully compliant with any of this legislation. The respective laws are complex and far-reaching, and were designed to enforce a level of integrity in operations and corporate philosophy that cannot be pulled from a box or jewel case. Remote Backup Software, through its ability to maintain secure copies of critical, sensitive data in a protected location, and to have them available for quick restore for required reporting or disclosure, addresses several of the criteria of compliance with all of them.

As enforcement of these laws increases, so does the need to have your data, and that of your clients, properly secured. Are you a member of the 'circle of trust' as referenced in GLB? Are you a HIPAA 'covered entity' or a business partner of one? Can you guarantee availability of critical reporting data for your SOX clients? It is time for IT service companies and businesses of all types to get serious about data security – and remote backup of data is a crucial and cost-effective component in compliance, business continuity, and disaster recovery planning.

Acknowledgements and Sources:

¹Sarbanes Oxley Act Forum, posting, online at sarbanes-oxley-forum.com

²American Institute of Certified Public Accountants, Summary of Sarbanes-Oxley Act of 2002 (Interpretation), online at aicpa.org

Media Contact information:
John Neibel, President & Founder
[Mirrored Storage, Inc.](http://MirroredStorage.com)
P. 214-550-0550

Copyright © 2009, 2010 & 2011, [Mirrored Storage, Inc.](http://MirroredStorage.com) Any reuse without the expressed written permission of [Mirrored Storage, Inc.](http://MirroredStorage.com) is prohibited.

