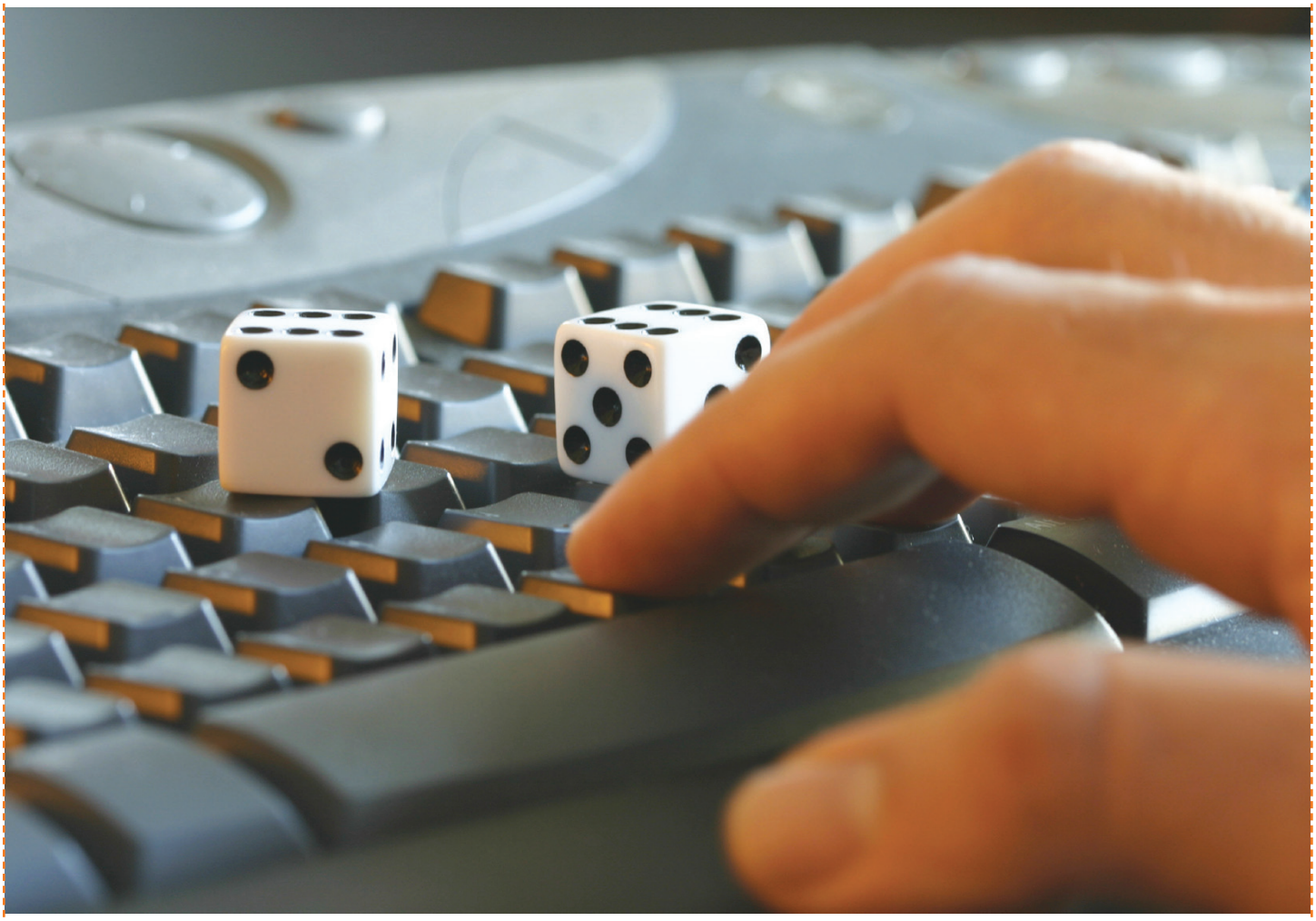
The New Age of Compliance

Preparing your organization for a new era of increased accountability and enforcement



By Tony Bradley
Director of Security
Evangelyze Communications

MIMOSA™ SYSTEMS

Table of Contents

MIMOSA™
SYSTEMS

Abstract

Enterprises of all sizes are or should be familiar with the concept of regulatory compliance. Legislative and industry mandates such as the Federal Rules of Civil Procedure (FRCP), The Freedom of Information Act (FOIA), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) apply to a wide variety of organizations. We have reached a turning point in the effort to protect the integrity of sensitive and confidential information. Organizations that have achieved compliance often fail to maintain the compliance over time, and many organizations simply gamble with customer data and sensitive information rather than investing the time and money in achieving compliance.

This is a new era in compliance. The changing of the guard in Washington DC brought renewed intensity to ensure that networks are secure and data is protected. Federal, State, and local governments are considering new regulatory mandates and looking at ways to improve the enforcement of existing mandates. Now is the time for organizations to proactively stay ahead of that curve and implement solutions and processes that help achieve and maintain regulatory compliance before the compliance police come knocking or they end up the next headline above the fold after a serious regulatory inquiry uncovers major problems in their data retention capabilities. This white paper examines the current state and changing landscape of IT compliance and addresses ways to streamline and automate tasks to achieve and maintain compliance more efficiently.

Introduction

In an ideal world companies would live up to reasonable standards of ethics out of an intrinsic desire to be responsible, socially conscious citizens. However, corporate greed has led entities such as Enron and WorldCom to commit gross fraud which ultimately led to their collapse, cost employees their jobs and cost shareholders billions of dollars.

In this Utopian world, companies entrusted with sensitive or confidential consumer information such as social security numbers and credit card numbers would work proactively to ensure that every precaution is taken to protect that data. Barely a week goes by without a headline related to a network security breach or lost or stolen laptop potentially compromising this data. Cutting corners and saving a dollar has contributed to lax security which has led to massive data breaches such as the compromise of customer data at TJX[1].

The failure of organizations to police themselves and to uphold a reasonable minimum standard for integrity as well as data security has led to a growing stable of federal and state compliance mandates. Most IT administrators are familiar with FRCP, FOIA, SOX, various employment–related regulations and HIPAA to name a few, but becoming familiar with them doesn't always translate to abiding by them. This white paper examines the current state of regulatory compliance and explores why some organizations are willing to risk remaining non-compliant. It also discusses the current political environment and the shift in the compliance landscape and compliance enforcement that organizations need to be prepared for. Finally, you will learn some best practices you can apply to streamline and automate compliance tasks and take some of the pain out of compliance and help your organization achieve and maintain compliance efficiently.

State of Compliance

Although compliance mandates have been around for a while, not every affected organization is compliant with the regulations that might apply to their business. For example, many organizations do not have adequate security controls in place to ensure that pertinent financial data is protected from unauthorized destruction or alteration, and that all audit or review work papers are retained for a period of five years from the end of the fiscal period in which the audit or review was concluded as required by SOX. Failure to comply with SOX and ensure the integrity of audits and financial reports can result in fines up to $1 million (USD) and up to 10 years in prison even if the failure was an accident.

Many organizations do not take the time to understand what compliance requires for them. More importantly, not every organization that achieves compliance remains compliant over the long term.

While the goal of these legislative and industry requirements is to strengthen and improve business related ethics and integrity so customers, investors and employees are protected from unscrupulous or criminal business practices, the audit or checklist mentality that compliance breeds actually has the opposite effect in some cases. In the absence of regulatory compliance mandates, organizations are forced to examine their processes and procedures, data infrastructure and its weaknesses more critically and to consider how to best retain and secure their data assets based on existing procedures and security controls.

Counting on a checklist of controls or audit items may limit the scope of what these organizations consider. The assumption is that if they pass the audit checklist and implement the controls identified in order to be compliant, they will also be secure, but that is not a safe or logical assumption. Passing an audit simply means that you have passed the audit. Remaining compliant over time requires ongoing effort and integration with business processes including regular process refreshes and continued employee training. Centrally managing and securing corporate data requires "C" level support, investment, and employee buy-in.

[1] Oct 24, 2007. Scope of TJX Data Breach Doubles. *http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9043944*

That said, organizations face a variety of challenges with achieving and maintaining regulatory compliance, not the least of which is cost. It takes an investment of money, personnel and man-hours to assess the data infrastructure and implement processes, procedures and automation to ensure compliance. A best practice is for the company to look at an ROI or NPV cost justification. Does it make financial sense to take on these additional costs to become compliant? You will have to compare the expected cost of bringing your company into compliance to the possible costs if you don't. These costs include government imposed fines, legal actions, loss of contracts, negative PR, lowered shareholder equity etc. Not being in compliance raises your company's risk of the above mentioned consequences among others.

Second, many organizations fall under more than one set of regulatory requirements. A publicly traded company in the health care industry that employees more than 20 people and that accepts credit card payments would have to comply with SOX, HIPAA, various employment regulations and PCI DSS simultaneously. It is important for organizations in this situation to fully understand these regulatory requirements and approach compliance as a whole rather than conducting separate and conflicting compliance projects.

At the Federal, State and local levels, government agencies and related entities have their own compliance issues. They must comply with the Freedom of Information Act (FOIA) or various state specific open records laws which requires that they retain virtually all records related to the running of the government and provide them on request to citizens or other parties. Governments tend to have healthy bureaucracies and red tape which generates lots of related documentation that could be requested by citizens. The job of archiving all of that data and retrieving it when requested is a herculean task that places a tremendous cost burden on these organizations, many of which are underfunded to begin with.

Compliance Gamble

While federal and state governments and some industries have developed these compliance mandates in an attempt to create a baseline and ensure that all affected organizations live up to at least a minimum acceptable standard for protecting and providing data, the compliance standards have generally lacked enforcement. In the past it was cheaper to pay a small fine if caught than to spend the money to come into compliance.

They can then make assumptions about what the costs or penalties associated with non-compliance might be and weigh them against the costs of achieving and maintaining compliance. Even if they determine that compliance is cheaper than non-compliance, compliance is a guaranteed cost while non-compliance still has a fair probability of resulting in no costs whatsoever.

For many companies it was a calculated, but acceptable, risk. The apparent lack of enforcement and lack of significant consequences for getting caught made them think twice about investing in compliance. The low probability of being caught combined with the minimal consequences if they did lead many companies to choose that as an acceptable gamble.

The Winds of Change

The days of gambling with compliance may be coming to an end. The recent changing of the guard in Washington DC has brought with it some promise of increased enforcement of existing as well as new regulations. Recent events with the banking industry and cases such as the Bernie Madoff ponzi scheme that lost investors $50 Billion have drawn significant attention to the gaps that still exist with compliance enforcement.

The United States Congress has a number of pending bills which may impact the state of compliance and how compliance is enforced, as well as strengthening the penalties for non-compliance. Legislation like these should put organizations on notice that gambling with compliance is about to get more risky and more expensive. Here are some examples of pending legislation:

- **H.R. 1797** (*http://www.govtrack.us/congress/billtext.xpd?bill=h111-1797*): Dubbed the 'Compete Act of 2009', it seeks to update SOX, including modifying relevant portions of Section 404 which contains the provisions related to network security and data integrity.

- **Physician Payments Sunshine Act of 2009** (*http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S6054*): It would place new compliance burdens on the medical industry to monitor and disclose the financial relationship between physicians and the medical device and pharmaceutical industries.

The Barack Obama presidency has also brought with it the promise of modernizing and computerizing our health care industry as one piece of cutting medical costs and helping the industry to operate more efficiently. In February of this year Barack Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA). Title XIII of ARRA, dubbed the Health Information Technology for Economic and Clinical Health (HITECH) Act takes effect in February of 2010 and includes expanded enforcement and increased penalties for HIPAA compliance.

The clock is ticking. If you are one of the companies that has been gambling with compliance now is the time to take action and work to achieve and maintain compliance before the provisions of the HITECH Act and other legislative and industry mandates expand and increase enforcement efforts.

Even companies that have worked to achieve compliance may not be effectively maintaining compliance. Many organizations approach compliance with a 'checklist mentality' and do the bare minimum necessary to pass the initial compliance audit. They fail to look beyond the initial compliance to ensure that systems and data remain compliant on a day to day basis and implement a business culture that fosters compliance.

Companies need to view compliance as an integral part of business processes rather than a checklist or a moment in time. The compliance landscape is changing and now is the time for organizations to take proactive steps to stay ahead of the curve.

Taking the Pain Out of Compliance

The need to archive and retain electronic records including email communications, employee day to day work files, Microsoft SharePoint records and many others for regulatory compliance requirements will continue to grow. The sheer volume and intensive nature of managing, monitoring, storing and retrieving electronic data can be a daunting challenge for any organization.

One way to take the pain out of compliance is to invest in the types of solutions that help automate and streamline compliance efforts. Using technology to manage tasks which are repetitive and can be automated both reduces the overall costs associated with compliance and helps to ensure compliance more efficiently.

Automating Data Retention

Mimosa Systems NearPoint platform provides a content archiving solution that can help companies automate the process of retaining, managing and archiving critical information such as Exchange Mail data, individual PST files, Windows File System data, and SharePoint content.

Mimosa NearPoint streamlines data retention regulatory compliance by performing continuous and scheduled capture of data including Exchange mailbox data and, metadata, Windows File System, and SharePoint content.

The Mimosa NearPoint's Multi-Node Grid Architecture is the most scalable architecture in the content archive industry and is provided standard in the NearPoint solution. Utilizing a superscalar or superpipelined grid, NearPoint can support systems ranging from 100 mailboxes to hundreds of thousands of mailboxes in a single system. The modular architecture allows servers and storage to be added or taken away as required to match performance challenges, without breaking the logical consistency of the archive information. Archive storage capacity grows on demand automatically, and default configuration and wizard-driven menus simplify deployment and management.

Improving Efficiency of Data Identification and Retrieval

Discovery has long been a part of the legal and regulatory process. The process of information disclosure at the start of a legal proceeding requires entities to furnish all relevant documents and communication to opposing counsel. In the Internet age that has evolved into eDiscovery, or electronic discovery.

With most business communication and documentation being done digitally, eDiscovery has become an integral part of corporate litigation strategy. It is a costly, time consuming process where matters often hinge on digital communications such as emails, collaboration documents, and online transactions.

Mimosa NearPoint helps organizations address legal and regulatory eDiscovery requirements more efficiently. The Mimosa eDiscovery solution in conjunction with the NearPoint Content Archive goes beyond searching basic email to include virtually all aspects of Exchange, Windows File System and SharePoint information.

The eDiscovery functionality within NearPoint allows complex searches to be conducted of 'who', 'what', 'when', and/or 'where' across each and every mailbox, File System and SharePoint repository. It can also be used to reconstruct a complete view of complex events such as email conversation threads and user behavior that can be valuable for litigation and regulatory investigation efforts.

One of the most unique features of NearPoint's eDiscovery functionality is that multiple users or auditors can collaborate on search efforts and be able to review each other's work. This capability mirrors real-world conditions routinely found in legal offices where multiple lawyers work together and combine their efforts to collaborate on a case.

The days of successfully playing Russian roulette with compliance requirements are numbered and organizations need to take action now to stay ahead of the curve and avoid being targeted by new enforcement efforts and increased penalties. Mimosa Systems NearPoint Content Archive solutions will help companies achieve and maintain compliance efficiently and effectively.

MIMOSA™ SYSTEMS

Mimosa Systems Inc. | 3200 Coronado Drive, Santa Clara, CA 95054 | www.mimosasystems.com | 408-970-9070