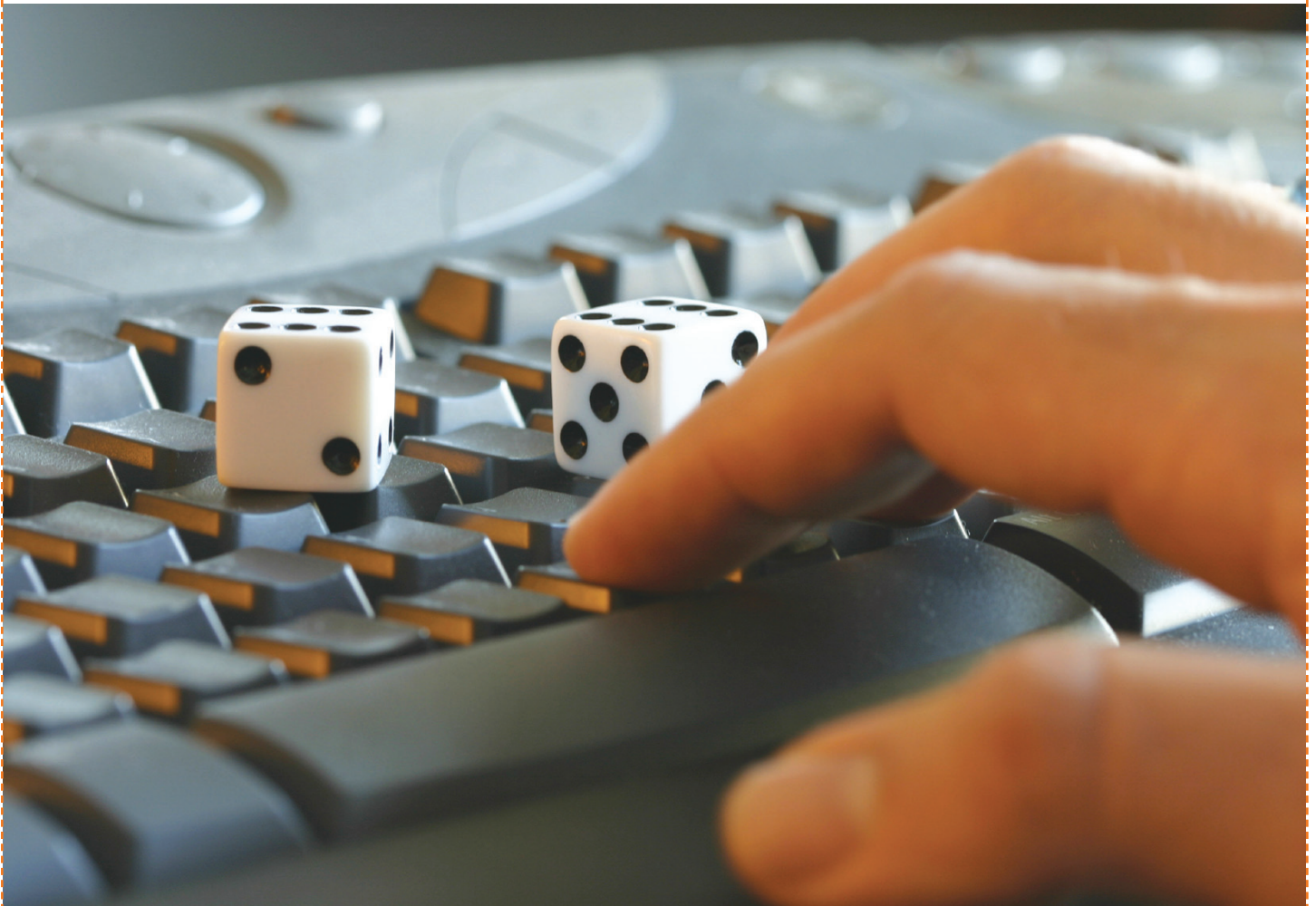


The New Age of Compliance

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



By Osterman Research



Table of Contents

WHY YOU SHOULD READ THIS WHITE PAPER.....	2
The Obligation To Be “Compliant”	2
There Are No “Unregulated” Industries.....	2
What Should You Do?	2
About This White Paper	2
JUST WHAT IS “COMPLIANCE”?	2
There Are Thousands Of Specific Compliance Obligations	2
Legal Obligations To Preserve Data	3
Are Organizations Compliant?.....	3
Challenges Of Achieving And Maintaining Compliance.....	4
THE COMPLIANCE CONTENT MIX	4
What Content Do You Need To Archive?	4
What Happens If You Don’t Archive Properly?	4
Consequences Of Failing To Meet Legal Holds	5
The Nightmarish Cost Of E-Discovery Using Backup Tapes	6
THE WINDS OF CHANGE ARE BLOWING.....	6
We Are In A New Political And Economic ERA.....	6
HOW TO TAKE THE PAIN OUT OF COMPLIANCE	7
Staying On Top Of Compliance With Mimosa	7
Mimosa NearPoint.....	7
Summary	7



WHY YOU SHOULD READ THIS WHITE PAPER

The Obligation To Be “Compliant”

Compliance, in the context of preserving business records stored in e-mail or other electronic repositories, generally focuses on one or both of the following:

- Compliance with specific regulatory or statutory requirements to preserve records for minimum periods. Examples include regulations from the Securities and Exchange Commission specifically focused on, among other things, communications between broker-dealers and their customers; or laws focused on healthcare providers that require them to preserve patient records.
- Legal obligations established by court precedent and/or advice of legal counsel to preserve certain types of records that may be needed as part of a discovery action or that may be helpful in preparing counsel to defend a client in a lawsuit.

There Are No “Unregulated” Industries

It is important for decision makers in any organization, regardless of the organization’s size or the industry in which it participates, to understand that there are not “regulated” industries that must preserve records and “unregulated” industries that can discard their business records with impunity. Rather, there are heavily regulated industries—such as broker-dealers, hedge fund managers and investment advisors—and less heavily regulated industries. In other words, all organizations must be compliant with some level of regulatory or legal obligation to preserve their business records. Because a growing proportion of these records are stored in e-mail and other electronic document repositories, archiving systems designed to preserve these records are gaining increasing importance.

What Should You Do?

Every organization must preserve its business records, regardless of the format in which they are generated or stored. This means that business records stored as e-mails, word processing files, spreadsheets, presentations, real-time conversation threads, database files and other electronic content that contains business records must be preserved for long periods, sometimes indefinitely. As a result, all organizations that must preserve these records should deploy an archiving capability that can scale to its long-term content preservation requirements.

About This White Paper

This white paper examines the current state of regulatory compliance and the impact of non-compliance. It also addresses the current political environment and the shift in the compliance landscape and compliance enforcement for which organizations need to be prepared. Finally, it discusses some best practices that can be applied to

streamline and automate compliance tasks and take some of the pain out of the entire compliance process.

JUST WHAT IS “COMPLIANCE”?

There Are Thousands Of Specific Compliance Obligations

There are a large and growing number of regulatory obligations to preserve e-mail and other types of electronic content. Some of the higher profile requirements are:

- **Sarbanes-Oxley Act of 2002**

The Sarbanes-Oxley Act of 2002 requires all public companies and their auditors to retain such relevant records as audit workpapers, memoranda, correspondence and electronic records—including e-mail—for a period of seven years. Company officers are obliged to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses have to ensure employees preserve information—whether paper- or electronic-based—that would be relevant to the company’s financial reporting.

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

All organizations operating in the healthcare field need to comply with HIPAA to ensure the safety of Protected Health Information. Organizations are required to protect the data from unauthorized users, as well as to retain for six years a broad range of documentation regarding their compliance.

- **Securities and Exchange Commission Rules**

Members of national securities exchanges, brokers and dealers are obliged to preserve all records for a minimum of six years, the first two years in an easily accessible place (SEC Rule 17a-4). The affected records are broad and encompass originals of communications generated and received by individuals within financial institutions, including inter-office memoranda and internal audit working papers. Also included are automated messages sent to all customers, which could include e-mail blasts. The records may be “immediately produced or reproduced on ‘micrographic media’ [microfilm, microfiche or similar] or by means of ‘electronic storage media’.

Among the many other requirements for data retention are FINRA 3010, the Investment Advisors Act of 1940 (hedge funds), the Gramm-Leach-Bliley Act, IDA 29.7, FDA 21 CFR Part 11, OCC Advisory, the Financial Modernization Act 1999, Medicare Conditions of Participation, the Fair Labor Standards Act, the Americans with Disabilities Act, the Toxic Substances Control Act, the UK Companies Act, the UK Company

Law Reform Bill - Electronic Communications, the UK Combined Code on Corporate Governance 2003, the UK Human Rights Act, Basel II, and the Markets in Financial Instruments Directive.

- Financial Industry Regulatory Authority (FINRA)**
 FINRA is a non-governmental regulator formed in 2007 by the merger of various functions of the New York Stock Exchange and the National Association of Securities Dealers. FINRA manages a wide variety of rules that are imposed upon the more than 5,000 brokerage firms and nearly 675,000 registered representatives it oversees.
- Model Requirements for the Management of Electronic Records (MoReq)**
 MoReq is a specification, originally developed in 2001, that defines the functional requirements for the manner in which electronic records are managed in an Electronic Records Management System. MoReq has been used widely in Europe and has been updated with MoReq2.

The regulations above are but a very small sample of the regulations focused on data retention that impact archiving requirements and practices.

Legal Obligations To Preserve Data

E-mail contains a growing proportion of business records that must be preserved for long periods. Further, e-mail is increasingly requested during discovery proceedings because of the Federal Rules of Civil Procedure (FRCP) and related issues. As a result, it is critical that e-mail be made available for legal discovery purposes.

Formally enacted in 1975, the FRCP governs court procedures for civil suits filed in the US federal courts. It states that the discovery of electronically stored information, including e-mail messages, instant messages, word processing files, spreadsheets, and so on, is now a mandatory point of discussion. When subpoenaed for information, the responding party has a maximum of 30 days to respond according to Rule 34.

The current version (2007) of the rules requires the responding party to “[...] produce documents as they are kept in the ordinary course of business [...]” Rule 34: 34(b)(2)(E)(i). This means that if the responding party uses data online and searches it electronically, they cannot supply that data as hard copy. The amendment also requires opposing parties to discuss e-discovery issues within 120 days of a lawsuit’s filing.

When a hold on data is required, it is imperative that an organization immediately be able to begin preserving all relevant data, such as all e-mail sent from senior managers to specific individuals or clients. An archiving system allows organizations to immediately place a hold on data when requested by a court or on the advice of legal counsel.

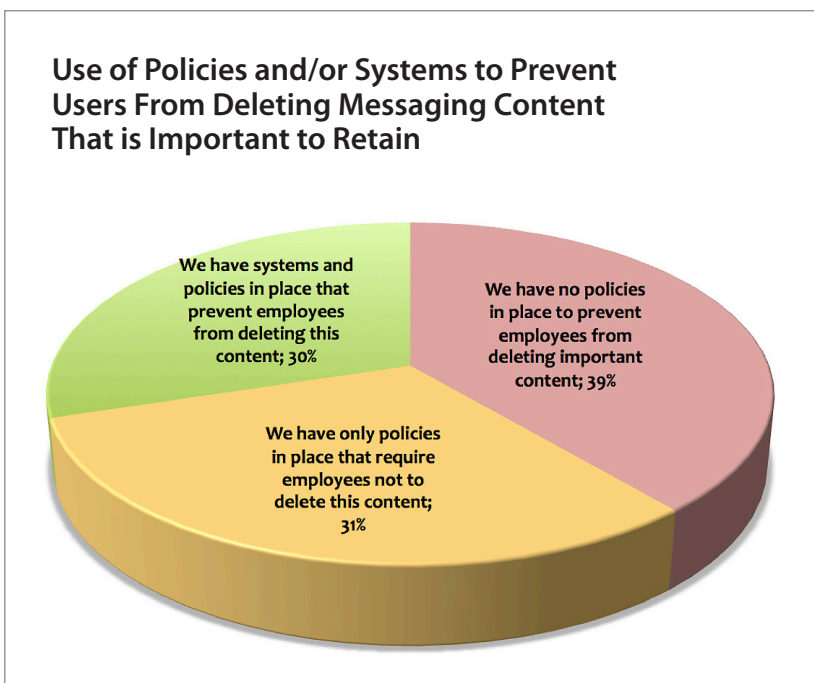
If an organization is not able to adequately place a hold on data when required, it can encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions or fines. Litigants that fail to preserve e-mail properly are subject to a wide variety of consequences, including brand damage, additional costs for third-parties to review or search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant’s failure to produce data as evidence of culpability.

Are Organizations Compliant?

Although compliance mandates have been around for quite some time, not every affected organization is compliant with the regulations that might apply to their business or industry. For example:

- A February 2009 Osterman Research survey found that 29% of organizations do not have an e-mail retention policy¹.
- The same survey found that only about one-third of mid-sized and large organizations are fully protected from the loss of important content that they should retain, as shown in the following figure.

¹E-mail Archiving Market Trends, 2009-2012



Challenges Of Achieving And Maintaining Compliance

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. Some decision makers may opt to conduct a return-on-investment analysis that compares the cost of compliance versus the benefits of being compliant and may opt to forego the deployment of a compliance solution.

Further complicating the decision process is that many organizations fall under more than one set of regulatory requirements. A publicly traded company in the healthcare industry that employs 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 all of their regulatory requirements and approach compliance as a whole rather than conducting separate and conflicting compliance analyses.

At the Federal, state and local government levels, government agencies and related entities have their own compliance issues. They must comply with the US Freedom of Information Act (FOIA) or various state specific open records/sunshine laws that require that they retain virtually all records related to the running of the government. These records must be provided on-demand to relevant parties.

THE COMPLIANCE CONTENT MIX

What Content Do You Need To Archive?

It is important to note that most regulations or legal decisions do not explicitly call out the media on which business records are stored, but rather only that business records and other relevant content be produced when required. However, as noted above, because a growing proportion of business records are created in and stored in electronic systems (most often e-mail), the archival of electronic content is becoming more important over time. Among the types of electronic content that must be preserved are the following:

- **E-mail**
Between 70% and 90% of all business correspondence in a typical company is e-mail-based. From compliance with regulations to the role of e-mail in legal cases, good e-mail preservation is key to meeting a company's obligations to preserve business records.
- **Instant messaging conversations**
As instant messaging moves from being a consumer-focused chat tool to becoming a useful business tool for internal and external communications, organizations

must consider archiving these messages. A full 20% of respondents to a February 2009 Osterman Research survey said they had a need to archive instant messaging now, while 28% said they would have a need to do so in 12 months. The growth of Microsoft Office Communications Server (OCS) and IBM Lotus Same-time, among many other real-time communications systems, will further increase the need to preserve content generated by and stored in these systems.

- **Electronic files**

A growing proportion of business records are created in desktop productivity applications, including word processing files, spreadsheets, presentation development programs and the like. Because most of these files are never printed, and because many of them contain business records that should be preserved for long periods of time, it is critical to preserve these files in an archival system.

- **SharePoint and other collaborative data**

Archiving can be used to address some of the reported limitations of Microsoft SharePoint, such as the lack of replication and the fact that SharePoint files and metadata are stored in an SQL database, which can increase backup and recovery times as more files are created.

- **Other data types**

There are a growing number of systems that generate and store electronic data, much of which contains business records. As a result, organizations have an obligation to preserve these records.

What Happens If You Don't Archive Properly?

History has clearly demonstrated that lawsuits involving data retention affect organizations of all sizes, and that those with poor data retention policies can endure severe consequences. The sample cases below illustrate that both defendants and plaintiffs could lose cases and damage their reputations if they fail to produce data through e-discovery in a timely manner:

- ***Zubulake v. UBS Warburg, 02-cv-1243, U.S. District Court for the Southern District of New York***

The three-year Zubulake sexual discrimination suit is a landmark case in the United States for its wide range of e-discovery issues. UBS was required, at its own expense, to produce all electronic materials relevant to the case. During the e-discovery process, it was discovered that certain backup tapes were missing and that e-mails had been deleted. The court also found that UBS had failed to comply with its own retention policy. UBS was ordered to pay the plaintiff \$29.3 million.

- ***Rhoads Industries Inc v. Building Materials Corp. of America, 2:070-cv-04756, U.S. District Court for Pennsylvania Eastern***

This case is an example where the plaintiff's lawyers accidentally turned over more than 800 privileged e-mails when they provided the defense lawyers with copies of 78,000 e-mails.

- ***Keithley v. The Home Store.Com Inc., 3:03-cv-00447, U.S. District Court for Northern California***

In describing the defendant's approach to discovery as "lackadaisical", the court in this patent infringement suit found that Home Store.com failed to maintain a written litigation hold policy when backup tapes were written over. The defendant produced other data only when faced with possible sanctions. The judge also found the defendant failed to preserve evidence until one year after the plaintiff filed the complaint and three years after the defendant received a demand letter threatening litigation.

- ***Qualcomm v. Broadcom 3:05-cv-01958, U.S. District Court for Southern California***

The patent case between Qualcomm and Broadcom illustrates that plaintiffs could lose if they fail to produce evidence in a timely manner. Qualcomm attorneys failed to hand over data, which included 200,000 pages of e-mails and other correspondence, until four months after the trial. As a result, the judge held that several Qualcomm patents should be rendered invalid. Qualcomm was ordered to pay all of Broadcom's litigation fees of about \$10 million.

- ***Testa v. Wal-Mart Stores, Inc.***

On February 2, 1993, a truck driver for a tropical fish wholesaler delivered merchandise to a new Wal-Mart store in Hinsdale, New Hampshire. During the delivery, the truck driver slipped on the icy delivery ramp, was injured and threatened to sue Wal-Mart. A Wal-Mart employee documented the incident in a formal report, including the truck driver's threat to take legal action. Further, another Wal-Mart employee had contacted the tropical fish wholesaler the day before noting that because the store was opening the next day, it would not accept deliveries, which is why the company had not cleared the delivery ramp of ice and snow. Both the report and the phone record were retained for 24 months in accordance with Wal-Mart's records retention policy.

However, slightly more than 26 months later, the truck driver sued Wal-Mart in federal district court and was awarded just over \$55,000 by a jury. Because Wal-Mart had destroyed the records of the incident and the telephone call to the wholesaler from the day before—after retaining them for 24 months—the judge instructed the jury, in part, that it might be able to infer

that Wal-Mart's destruction of these records was because the Messaging Archiving and Document Management Market Trends, 2008-2011 company, "having known that a lawsuit was pending, destroyed certain records and did so because...[it]...knew the records to be harmful to its own case."

- ***Lorraine v. Markel American Insurance Co.***

An important case that deals with the authenticity of electronically stored information is *Lorraine v. Markel American Insurance Co.* [2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007)]. This case involved a dispute between the owner of a ship that had been struck by lightning and the insurer of the ship. Although the insurance company paid for the damages, the ship's owner subsequently found additional damage and made a second claim, which the insurance company disputed. During arbitration, the damages awarded to the plaintiff were reduced by \$22,000. While both parties presented e-mail evidence during arbitration, Chief Magistrate Judge Paul W. Grimm who presided over the case found that the e-mail evidence presented could not be authenticated and so was not admissible.

Consequences Of Failing To Meet Legal Holds

If an organization is not able to adequately place a hold on data when required, it can encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions or fines. Litigants that fail to preserve e-mail properly are subject to a wide variety of consequences, including brand damage, additional costs for third-parties to review or search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant's failure to produce data as evidence of culpability.

A classic case in this regard is that of Intel. During 2005, AMD sued the company for alleged antitrust violations. Intel instructed certain employees whose e-mails might be relevant to preserve this content, and it migrated these employees to an e-mail server that would automatically preserve the relevant e-mails. However, because some employees did not comply with the hold order; coupled with IT a) not migrating the employee accounts, b) recycling backup tapes and c) not turning off the auto-delete function that deleted e-mail after 35 days; not all of the relevant e-mails were held. As a result, Intel lost its argument that its internal interviews about missing e-mails were protected by attorney-client privilege, and so had to divulge some of this content to AMD.

Also, while companies responding to a subpoena may argue that the information is inaccessible due to the burden and cost of producing it, the court may still demand it if it agrees that the requesting party has good cause to view the data. The result might be that an organization must produce this content regardless of the cost of doing so.

The Nightmarish Cost Of E-Discovery Using Backup Tapes

Sifting through backup tapes for e-discovery is not only expensive, but also can be extraordinarily time consuming:

- The first task is finding the tapes, and in many companies the tapes could be locked in a number of closets or storage lockers. Sometimes these tapes are missing labels and use a naming convention that is not known to anyone other than the person who labeled them—and that person may have left the company.
- Reviewing information on backup tapes is no easy task. For example, a compressed LTO-3 tape can hold 750 gigabytes of e-mail, or approximately 56 million printed pages of text.
- The FRCP mandates that companies keep data from Exchange servers, backup systems, offsite tapes and .PST files. The cost of sifting through this media averages \$500 to \$1,000 per gigabyte, according to published reports. This could amount to a six- and seven-figure cost for even small organizations that could generate several terabytes of such data. However, the cost can be much higher: for example, In the case of *Bank of America v. SR International Business Insurance Co. Ltd.*, it was estimated that the cost to produce e-mails from 350 to 400 backup tapes would be anywhere from \$3,750 to \$4,300 per tape.

E-mail archiving enables organizations to store old e-mails, large attachments and redundant messages in a central repository that is easily accessible. This frees up space on existing servers for other business applications, and helps to speed up e-mail server backups and restores. When used with e-discovery tools, e-mail archiving software can enable organizations to search millions of e-mail messages, calendar items and other messaging documents in a matter of seconds.

THE WINDS OF CHANGE ARE BLOWING

We Are In A New Political And Economic ERA

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 in the banking industry, coupled with cases like that of the Bernie Madoff ponzi scheme, have drawn significant attention to the gaps that still exist with compliance enforcement.

The United States Congress has a number of pending bills that may impact the state of compliance and how compliance is enforced, as well as strengthening the penalties for

non-compliance. Legislation like this should put organizations on notice that gambling with compliance is about to get more risky and more expensive. Here are but a few examples of pending or recently passed legislation:

- **H.R. 1797**
Dubbed the 'Compete Act of 2009', this House bill seeks to update Sarbanes-Oxley, including modifying relevant portions of Section 404 that contain the provisions related to network security and data integrity².
- **Physician Payments Sunshine Act of 2009**
This bill would place new compliance burdens on the medical industry to monitor and disclose the financial relationship between physicians and the medical device and pharmaceutical industries³.
- **HITECH Act**
The Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the American Recovery and Reinvestment Act of 2009 that was passed into law in February 2009. Among other things this Act requires physicians using electronic health records to be able to track each time that their patient's information has been disclosed, a requirement that goes well beyond previous obligations. Any breach of information impacting 500 or more patients must be reported to every patient in a physician's practice, a local media outlet and the Secretary of Health and Human Services. Further, fines can reach as high as \$1.5 million⁴.
- **North Carolina Pesticide Board**
The State of North Carolina Pesticide Board enacted new records-keeping requirements for the application of various pesticides, as well as revised rules on the length of time these records must be kept⁵.
- **A Challenge to SOX**
One of the more interesting potential changes to US regulations is that the US Supreme Court has opted to decide on a Constitutional challenge to Sarbanes-Oxley although, as of this writing, there is no indication of how the Court will rule.

While it is impossible to determine with certainty what the ultimate impact of the new administration will be, it is safe to assume that the banking crisis and recent bankruptcies at major companies will spur regulators to increase the level of enforcement for existing regulations and will motivate legislators to enact more requirements.

² <http://www.govtrack.us/congress/billtext.xpd?bill=h111-1797>

³ http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=56054

⁴ <http://www.aafp.org/online/en/home/publications/news/news-now/government-medicine/20090318hipaa-security-rules.html>

⁵ <http://wncgreennews.blogspot.com/2009/05/new-pesticide-record-keeping-regulation.html>

HOW TO TAKE THE PAIN OUT OF COMPLIANCE

Staying On Top Of Compliance With Mimosa

The need to archive and retain electronic records including e-mail 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 will help to automate and streamline compliance efforts. Using technology to automate activities like legal holds and archival of business records both reduces the overall costs associated with compliance and helps to ensure compliance.

Mimosa NearPoint

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. Using 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.

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

The e-discovery 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 e-mail conversation threads and user behavior that can be valuable for litigation and regulatory investigation efforts.

One of the most unique features of NearPoint's e-discovery 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.

Summary

Compliance should be a critical component of any organization's data management plan. Whether complying with a specific statutory obligation to preserve business records, or complying with legal counsel's opinion on what might be important content during an e-discovery exercise, organizations of all sizes should preserve their business records. Because a growing proportion of these records are stored electronically in repositories that include e-mail, collaboration systems, file systems and real-time communications tools, it makes for any organization to archive necessary content from these systems electronically. A failure to archive this content can have serious financial and other consequences, almost all of which are more costly than the archiving system and its maintenance.

