

# Why Archiving is a Really Good Idea For Legal and Regulatory Compliance

**An Osterman Research White Paper**

*Published May 2010*

**SPONSORED BY**



## Executive Summary

---

### THE NEW ROLE OF ELECTRONIC CONTENT IN THE 21<sup>ST</sup> CENTURY

Virtually all organizations store their business information in a variety of places, including email messages and attachments, shared file systems, corporate document repositories like Microsoft SharePoint, voice mail systems, Lotus Quickr, personal computers and application databases. While this information is crucial to running the business it can also be a source of “risk” to you and your company in a number of ways:

- The Federal Rules of Civil Procedure (FRCP) have ushered in a new era in the management of electronic information. An inability to access current and older electronic information *quickly* and *accurately* can put your company at risk of discarding evidence you might need at trial or for pre-trial review, which ultimately could cost your company hundreds of thousands or millions of dollars.
- Similarly, the growing body of Federal, state and provincial regulations focused on corporate governance mandates that that corporations have policies and controls for the retention, security and expiration of electronic information throughout its lifecycle. A failure to do so can result in significant penalties.
- Good corporate governance – even before lawyers or regulators come knocking – demands that electronic business records be preserved and readily accessible for long periods of time. Therefore, corporations must a) classify this content b) archive this content and c) make it easily searchable.

**In short, the amount of electronic information that you retain – combined with the way you manage it – represents your organization’s level of risk. Manage it well and your risk is minimized; manage it poorly and your risk is increased dramatically – maybe even to the level of threatening your ability to stay in business.**

### ARE YOU REALLY ARCHIVING YOUR DATA?

Many decision makers believe they are “archiving” their data – numerous Osterman Research surveys attest to the fairly large number of companies that claim they are archiving their email and other electronic content. However, when we define archiving as the indexing of inbound, outbound and internally sent content; the transfer or copying of this content to archival storage; and the integration of robust search capabilities that can quickly extract needed content by anyone that needs it, the proportion of companies that report they are archiving falls off significantly.

This disparity is due largely to the use of “quasi-archiving” technologies and processes like nightly backups, continuous data protection (CDP) systems, file systems that take period snapshots of data stores, and the like. While all of these are important and necessary tools and practices, they are not true archiving solutions and cannot be used effectively for e-Discovery, legal holds, regulatory compliance or the various other applications that demand more robust archiving capabilities.

**Make sure that what you think is archiving really is archiving.**

## **ABOUT THIS WHITE PAPER**

This white paper discusses archiving concepts and best practices, the various reasons to archive email and other electronic content, the consequences of not archiving properly, and some important issues to consider when evaluating archiving solutions. Finally, it briefly discusses Unify, the sponsor of this white paper, and its content archiving capabilities.

## **Determining Your Need for Archiving**

---

### **WHY YOU SHOULD FOCUS ON ESI VERSUS ONLY EMAIL**

Email is the place that many organizations start when they deploy an archiving solution – and rightly so. Email in most organizations contains enormous amounts of important and useful content, including purchase orders, contracts, proposals, statements of work, presentations, policy decisions, conversation threads and many other business records.

However, it doesn't stop with email. A large and growing number of repositories also contain important electronic content, or Electronically Stored Information (ESI), such as Microsoft SharePoint, Lotus Quickr, file servers, CRM systems, and various application databases.

### **JUST WHAT IS ESI?**

A number of important and substantive revisions to the FRCP went into effect on December 1, 2006. These changes represented several years of debate at various levels and are having a significant impact on electronic discovery and the management of electronic data within organizations that operate in the United States. In a nutshell, the changes to the FRCP require organizations to manage their data in such a way that this data can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

The amendments to Rules 16, 26, 33, 34, 37, 45 and revisions to Form 35 are aimed specifically at ESI and attempt to deal with the important issues presented by it:

- ESI is normally stored in much greater volume than are hard copy documents.
- ESI is dynamic, in many cases modified simply by turning a computer on and off.
- ESI can be incomprehensible when separated from the systems that created it.
- ESI contains non-apparent information, or metadata, that describes the context of the information and provides other useful and important information.

The changes reflect the reality that discovery of email and other ESI is now a routine, yet critical, aspect of every litigated case. First, the amendments treat ESI differently. Second, they require early discussion of and attention to electronic discovery. Third, they address inadvertent production of privileged or protected materials. Fourth, they encourage a two-tiered approach to discovery – deal with reasonably accessible

information and then later with inaccessible data. Finally, they provide a safe harbor from sanctions by imposing a good faith requirement.

**In short, email is a good place to start archiving ESI, but other data types and information repositories must also be archived.**

### **DETERMINING YOUR NEED FOR ARCHIVING**

In determining whether or not your organization has a need to implement content archiving, there are a number of questions that should be asked of decision makers in your organization:

- **Do you have legal obligations to preserve business records?**

For virtually every organization – including those with even just a few employees – the answer is a definitive yes. e-Discovery, driven largely by the changes to the FRCP, is becoming much more important in the context of civil litigation – for example a study by Gibson, Dunn & Crutcher LLP found that courts applied more sanctions in 2009 than they did in 2008. In fact, more than one-half of the opinions issued during the first five months of 2009 focused on consideration of sanctions and 36% of these actually resulted in sanctions. Further, roughly three out of four discovery orders today require email to be produced as part of the discovery process and e-Discovery today represents 35% of the total cost of litigation. Companies that fail to produce emails and other electronic content in a timely or appropriate manner face the risk of paying millions of dollars in sanctions and fines, not to mention loss of corporate reputation, lost revenue and embarrassment.

Closely related to using archiving for e-Discovery is its ability help organizations place holds on data. For example, when a hold on data is required, it is imperative that an organization immediately be able to issue formal notifications to “key players” with a documented confirmation of acceptance and understanding and begin preserving all relevant data, such as all email 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. In the absence of an archiving system, organizations must depend on individual employees’ compliance with a corporate memo – an iffy proposition at best.

- **Do you have regulatory obligations to preserve business records?**

Industries that are heavily regulated, such as broker-dealers or healthcare firms, must meet a variety of statutory requirements with regard to records retention. For example, the SEC imposes requirements on broker-dealers to preserve email and instant messaging communications and to monitor these communications for potential violations.

However, virtually all organizations must satisfy statutory records retention requirements, including broad-based requirements such as the Americans with Disabilities Act, the Age Discrimination in Employment Act and the Occupational Safety and Health Act. For example, the Sarbanes-Oxley Act impacts all public

companies and has been a key issue for regulatory compliance, although there are many other regulatory obligations to retain data, including:

- SEC 17a-4
- FINRA 3010
- Gramm-Leach-Bliley Act
- The Investment Advisors Act of 1940
- FDA 21 CFR Par 11
- OCC Advisory
- HIPAA
- Financial Modernization Act 1999
- Fair Labor Standards Act
- Toxic Substances Control Act

These are just a handful of the literally thousands of local, state, provincial, federal and international regulations focused on data retention. While few of these regulations dictate requirements for electronic data retention, the growing proportion of business records stored electronically means that “data retention” increasingly means “electronic data retention”.

- **Do you also need to tame email storage growth?**

Many Osterman Research surveys over the past several years have clearly demonstrated that growth in messaging storage is the most critical messaging-related problem faced by administrators: roughly 60% of decision-makers in mid-sized and large organizations cite growth in messaging storage as a serious or very serious problem. Messaging storage, driven by increasing use of email, larger attachments and the like, is growing at an average of about 30% per year. This means that a terabyte of storage today will swell to nearly 2.5 terabytes in just three years.

By implementing a properly configured messaging archiving system that replaces messages and attachments with much smaller stubs pointing to stored content in an archive, organizations can dramatically reduce the amount of content stored on ‘live’ messaging servers. The result will be significantly improved messaging server performance, reduced backup windows, enabling new tiers of lower cost storage, elimination of “personal” archiving, and removal (or increase) of user mailbox quotas.

- **Do you need to establish *defensible* policies between people, systems and processes for the retention, disposition and legal discovery of email and other electronic records?**

An important best practice for any organization in any industry is the creation and enforcement of policies that will protect an organization from charges of spoliation of evidence, charges that it did not preserve records in accordance with regulatory obligations, or charges that its record-keeping practices are not in keeping with industry standards. An archiving system is a key element in helping organizations to identify and preserve records automatically, demonstrate that the archived content

represents true and verifiable copies of the original content, and to comply with statutory and legal obligations to preserve data.

- **Is there content in your email and other data stores from which it would be useful to extract business intelligence?**

The value of preserving corporate knowledge stored in email is undervalued in many organizations. However, email contains more than one-half of the information that individuals use on a daily basis, and a large proportion of corporate email users spend more than two hours per day generating and using content stored in email systems. As a result, an enormous amount of corporate 'memory' is stored in email, making its preservation important. An organization that does not preserve its email content adequately risks the loss of information that it has paid employees to produce.

## **THE BENEFITS OF ARCHIVING**

As discussed throughout this white paper, archiving is much more than preserving the bits sent in email or stored in application databases. Rather, today's archiving is about reducing the risk associated with not being able to proactively manage content. Further, archiving is about managing all of an organization's ESI, not just its email content. Many archiving vendors may be caught flat-footed because they are not focused on the next evolution of the problem – managing the risk associated with all ESI.

### **So, what happens if a company does not proactively manage its data through the right archiving technology?**

- **It cannot satisfy its legal obligations**

Failure to satisfy the Federal Rules of Civil Procedure (FRCP) is but one example of how companies could fall afoul of regulations. Although the FRCP does not set the length of time for preservation of data, only those with a good data retention policy are well positioned to go through litigation with minimal damage. An organization without coherent retention policies could find itself paying major penalties during the discovery process if it promises to produce data that it later discovers was already destroyed. Email archiving, among other things, helps organizations to focus on developing and enforcing data retention policies.

- **It cannot satisfy its legal hold requirements**

If an organization is not able to adequately issue notifications and place a hold on data when required, it could encounter a variety of serious consequences, ranging from embarrassment to serious legal sanctions, fines or damage to its brand. Litigants that fail to preserve email 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.

Also, companies responding to a subpoena may argue that the information is inaccessible due to the burden and cost of producing it. While cost shifting defers this argument to some extent, the court may still demand it if it agrees that the requesting party has good cause to view the data. A poorly managed retention

policy could also result in the inadvertent disclosure of privileged or proprietary materials to the requesting party.

- **It cannot satisfy its regulatory obligations**

There have been numerous cases in which organizations have failed to preserve business records in accordance with regulatory obligations. The result of running afoul of the requirements of the SEC, FINRA or some other regulator has resulted in the levying of large fines in some cases, although many companies would rather live with the relatively low probability of fines but wish to avoid the negative publicity that may follow. However, given the new administration's stated desire to significantly up the ante in the context of banking and other regulations, a "living with the fines" approach may be short lived.

### **LAWSUITS ARE VERY EXPENSIVE TO ADDRESS**

Recent history has shown that lawsuits involving data retention affect companies of all sizes and that companies with poor data retention policies can endure damaging 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 emails 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 emails when they provided the defense lawyers with copies of 78,000 emails.

- ***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 emails 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.

### **SATISFYING OBLIGATIONS USING BACKUP TAPES IS NOT FUN**

Going through backup tapes to look for data in response to a regulatory audit or an e-Discovery exercise is not only expensive, it is also extremely time consuming:

- The first task is locating 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 email, or approximately 56 million printed pages of text.
- The FRCP mandates that companies keep data from email servers, backup systems, offsite tapes and personal information stores. The cost of sifting through this media averages \$500 to \$1,000 per gigabyte, according to published reports. This could amount to a six- or seven-figure cost for even small organizations that could generate several terabytes of such data.

Email archiving enables organizations to store old emails, 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 lower the cost of storage and improve email server performance. When used with e-Discovery tools, email archiving software can enable organizations to search millions of email messages, calendar items and other messaging documents in a matter of seconds.

It is important to note that the benefits of a good archiving solution can actually provide cost savings that are greater than the cost of the system itself. For example, savings in staff time, reduced expenditures for external legal counsel, lower Tier 1 storage costs, reduced backup costs, faster migrations to new platforms and the like can all result in rapid payback for the archiving system and a net gain for the organization.

## **What Can the Right Archiving Capabilities Do For Your Company?**

---

### **YOU CAN BE MORE PROACTIVE AND LITIGATION-READY**

One of the important benefits of good archiving technology is that it permits senior managers and other decision makers to take a more proactive approach to e-Discovery and to litigation in general. For example:

- The right archiving technology can allow IT managers, compliance officers and Legal Counsel to develop and enforce policies on an ongoing, evolutionary basis in an effort to stay ahead of specific legal obligations. Instead of being forced into a defensive posture each time a legal action is received, legal counsel can employ an offensive strategy, armed with better and more complete information.
- It can allow corporate supervision of employee email to look for potential policy violations and then take appropriate action, such as reminding employees of existing policies or refining policies to cover new issues.
- It can permit organizations to automatically preserve and expire data according to policies rather than keeping all data – this will show corporate enforcement of established policies and mitigate risk in legal discovery across information that could rightly have been expired.
- An archiving capability that permits easy and regular access to archived data for the purpose of managing and improving the business gives decision makers an important tool they need in proactively addressing issues before they have the opportunity to become actionable. By contrast, a reactive archiving system that requires IT intervention in accessing, and that is practical to use only when responding to a major event like an e-Discovery request, puts decision makers at a decided disadvantage.

**The bottom line is that reactive data collection is a poor business practice and does nothing to manage risk – archiving is a proactive approach that truly manages corporate risk.**

### **YOU CAN SOFTEN THE IMPACT OF LAWSUITS AND REGULATORY PROBLEMS**

The right archiving technology can help an organization to be proactive in two important ways:

- Avoiding lawsuits altogether by ensuring that, through the use of management review or an analytics-based system, corporate policies are being followed on an ongoing (and, perhaps, near real-time) basis. This allows an organization to monitor employee behavior for potentially actionable statements or activities, and to adjust corporate policies on-the-fly to minimize the potential for legal action.
- In the event a legal action has already been started, a good archiving system can help an organization to perform assessment of its position early in a case, sometimes to an organization's advantage over the opposition. This might include reviewing the likelihood of victory very early in the case, allowing an organization either to settle quickly and avoid significant legal fees or an adverse judgment; or giving decision makers confidence that they can prevail and thereby minimize the likelihood of an adverse judgment.

In short, good archiving helps decision makers to make the right decisions armed with better information than they otherwise would not have.

## **REDUCING COST AND BURDEN**

A properly specified and configured archiving solution can help an organization reduce its overall costs of email and records management. These benefits include:

- **Dramatically lower costs for e-Discovery**  
For example, after deploying Unify's archiving technology, decision makers from a major financial services company in the United States reported that the *first* use of the system for an e-Discovery exercise more than paid the entire cost of deploying the system.
- **Lowering direct and indirect costs**  
Driving down other related costs such as legal judgments, fines, and public relations damage from negative publicity.
- **Peace of mind**  
The peace of mind that comes from knowing all of the information that might be needed for e-Discovery, a regulatory audit or a legal hold will be easily available when needed.

## **IMPROVING OPERATIONAL AND STORAGE EFFICIENCIES**

An added benefit of a good archiving solution is its ability to reduce storage management problems. Osterman Research has found that most of the leading problems involved in managing email systems are focused on storage-related problems, such as large attachments sent through email, increasing use of attachments and email itself, and storing content on live email servers. The right archiving, litigation hold and e-Discovery solutions can dramatically reduce storage costs and provide a number of other email management benefits.

## **What Should You Do Next?**

---

### **UNDERSTAND WHY E-DISCOVERY AND REGULATORY COMPLIANCE ISSUES ARE IMPORTANT TO YOUR BUSINESS**

First and foremost, decision makers must understand the importance of e-Discovery and regulatory compliance as it relates to the business in which they are currently engaged or might be engaged in the future. For example, senior business decision makers, legal counsel, IT managers and others should understand the current legal decisions focused on the company's ESI (Electronically Stored Information), its data retention and legal holds, including the types of records that should be retained, for how long they should be retained and so forth.

Similarly, heavily regulated organizations must understand the relevant obligations to preserve data. Financial services organizations operating in the United States, for example, must fully comply with SEC and FINRA requirements for data retention, supervision of content and other requirements. Energy-related companies must comply with FERC requirements. Healthcare organizations must comply with HIPAA, Medicare and other requirements.

In short, while all organizations must comply with legal obligations to preserve data, there are specific regulatory requirements that impact different industries and to varying degrees.

### **ESTABLISH RETENTION AND DELETION CYCLES FOR ALL CONTENT**

Next, it is important for decision makers to establish retention and deletion cycles for every type of content that will need to be retained. Some diverse examples of the requirements to retain data include:

- Section 802 of the Sarbanes-Oxley Act requires that accountants in certain situations “shall maintain all audit or review workpapers for a period of five years from the end of the fiscal period in which the audit or review was concluded.”
- The FRCP does not prescribe a mandated length of time for which records must be retained. The responding party must respond within 30 days of a request for data that is issued. Parties must present data as they are kept in the ordinary course of business [Rule 34(a)(d)(1)(B)]. Court-ordered sanctions are available for failing to preserve emails relevant to anticipated or ongoing litigation.
- The US Internal Revenue Service requires that “all employment tax records [be kept] for at least four years after the date that the tax becomes due or is paid, whichever is later.”
- Revenue Canada requires that some records, such as copies of all Board minutes and annual audited financial statements “be kept for the duration of the life of your organization plus an additional period not less than two years from the dissolution date.”
- The EU Data Protection Directive was originally implemented in 1995 to protect the data of individuals and the free movement of such data. The rules are applicable not only to businesses in the European Union, but also to anyone who uses equipment inside the EU to process data. For example, a US-based online retailer serving customers in the EU would need to follow the regulation if they process personal data and use EU-based equipment to process that data (i.e. the customer's computer).
- The California Fair Employment and Housing Act (FEHA) requires employers and employment agencies to maintain and preserve any and all applications, personnel, membership or employment referral records and files for a minimum of two years.

Also, companies involved in employment-based legal complaints are not permitted to destroy records until all appeals or related proceedings are terminated.

These are just a few of the literally thousands of requirements to retain various types of business records. The specific statutory and legal obligations to which an organization must adhere depend on a variety of factors, including the industry in which an organization operates, the geographical locations in which it has offices and conducts

business, the advice of legal counsel, best practices established by industry organizations and industry peers, recent legal decisions, and other factors.

### **MAINTAINING THE STATUS QUO IS AN OPTION – BUT A BAD ONE**

After establishing the importance of planning for e-Discovery and regulatory compliance, and after understanding specific data retention and deletion obligations for various types of data, one option is to maintain the status quo in which most organizations find themselves and not deploy an archiving solution. Some organizations today do not archive their email or other electronic content, instead relying on backup tapes, disk-based backup or paper records to satisfy e-Discovery, regulatory compliance and other obligations. Further, a handful of organizations actually purge electronic records on a regular basis to avoid the perceived high costs and difficulties associated with archiving, instead relying on their hope that doing nothing will be the best defense in the event of lawsuit or regulatory audit. Some organizations, in fact, believe it is cheaper to bear the cost of regulatory fines and adverse legal judgments rather than archive.

While maintaining the status quo is an option, there are two fundamental flaws with this approach:

- It does not allow for proactive and sound adherence to good corporate governance principles. By contrast, a company that follows best practices for corporate governance is going to be in a better position not only to reduce the risk of legal or regulatory actions, but also to garner additional business. For example, a bank that responds to an RFP from a large, prospective customer can cite its good corporate governance and information management as a competitive differentiator compared to another provider that merely uses archiving to support a defensive posture.
- Even in the highly unlikely event that a lawsuit or an audit never occurs in an organization, growing quantities of electronic storage will continue to vex storage and email managers and drive up overall IT costs. Archiving could help with both, alleviating most of the leading problems in managing email systems, for example, and lowering the overall cost of storage.

### **DEPLOY TOOLS THAT WILL ENABLE YOU TO BE PROACTIVE**

The better approach, then, is to deploy an archiving solution that will help an organization to be proactive in the context of its e-Discovery and regulatory compliance obligations, and that will simultaneously help it to solve its IT and storage management problems. The key considerations on which an organization will need to focus are discussed in the next section of this white paper.

## **Key Issues to Consider When Selecting an Archiving Solution**

---

There are a number of important issues that decision makers should consider when selecting a new archiving solution or when replacing an existing solution.

### **SCALABILITY IS AN ISSUE, EVEN FOR SMALLER COMPANIES**

How scalable should an archive be? That depends to a large extent on the amount of electronic content generated, received and stored by users in the organization; and on how long the content must be stored. For example, assume that a) each individual in an organization of 5,000 users sends and receives 25,000 emails annually, b) 40% of these emails must be retained, c) they must be retained for seven years, and d) each user generates two gigabytes of other archivable content each year that also must be retained for seven years. Based on these assumptions, an organization will need to archive 350 million emails and 68.4 terabytes of content over those seven years. That represents an enormous amount of content that will require a very robust and scalable archiving system to manage.

However, it is also important to consider that growing use of attachments, greater use of multimedia and video, larger presentations, and the like will increase storage requirements over time, perhaps making even the best long term estimates too conservative. Further, increased corporate governance requirements and greater government oversight as a result of the financial meltdown that started in late 2008 will likely increase retention periods and the breadth of data types that must be retained.

An important point to consider here is the underlying technology used for the archive.

For example, the use of a relational database management system (RDBMS) in an archiving solution can significantly increase the overall cost of the archive. So while relational databases serve transactional content management systems well they do not perform well for archiving technologies, so this is an important distinction when selecting an archiving solution.

### **HOW MUCH AND HOW FAST WILL YOU WANT TO SEARCH?**

Even a small organization can build enormous stores of archivable content. In order to respond quickly to an e-Discovery request or a regulatory audit, or simply to allow senior managers or legal counsel to conduct preliminary searches, performance will have to be very robust. Some archiving solutions that have been underspecified or that do not employ sufficiently robust search technology will not be able to meet some organizations' search requirements for the complexity of searches or the timeframe in which results are needed.

### **WHAT LONG-TERM PRESERVATION REQUIREMENTS WILL YOU HAVE?**

Many organizations must retain data for at least three years, but some must retain data for much longer periods. For example, securities dealers must retain data for a minimum of six years, healthcare organizations must retain some data for the life of their patients plus two years, while some manufacturing organizations must retain data

for at least 30 years. As a result, decision makers should select an archiving solution that will retain information and employ system processes that guarantee content and data accessibility for the longest conceivable period, something not all archiving solutions are designed to do.

The length of time that content must be retained has significant implications on the choice of archiving technology. For example, will data that is archived in 2010 and that must be retained for 30 years be readable by archiving systems in 2040? Will the data formats used today still be supported by the end of your required retention period? Will the archiving vendor from which you purchase technology today still be around in a few years? An archive vendor should be able to satisfy all of these requirements.

### **WHAT PLATFORMS SHOULD YOUR ARCHIVING SOLUTION SUPPORT?**

Another very important consideration is the support provided for various messaging platforms and operating systems. This is particularly important for larger organizations that might use multiple messaging platforms, including Microsoft Exchange and IBM Lotus Notes/Domino or multiple server operating systems, such as Windows and Solaris. While there are certainly other messaging platforms and operating systems in use, these are among the most widely deployed.

Further, an archiving solution should be able to manage all of the data types an organization currently uses or may use in the future. This might include Exchange .PST files, .RGE (Mac Entourage) files, Lotus Notes email databases, instant messaging conversations, desktop files, SAP databases, CRM databases other host system output such as PCL5, Extended Binary Coded Decimal Interchange Code, etc.

### **WHO WILL BE USING THE SOLUTION?**

This is also an important consideration, since it will determine who has ready access to the archive: technically oriented staff only, such as IT technicians; or non-technically oriented staff that might include legal counsel, senior managers and external counsel who are given legal hold capabilities. For obvious reasons, an archiving solution should be relatively easy to use so that business users can use the system without much handholding by IT staff, extensive training and the like. It is also important to have available a system that externalizes complex query function into an easy to use application requiring no knowledge of complex Booleans to set up a search query. Complexity can lead not only to underuse of the archiving technology and an organization not realizing the full value of its investment in it, as well as mistakes that could lead to important content being overlooked or not produced in a timely manner.

### **THE BENEFITS OF A SINGLE CORPORATE PLATFORM FOR YOUR ARCHIVING REQUIREMENTS**

Most organizations deploy an archiving solution to manage email, but quickly realize that all electronic content should be archived and made available for legal, regulatory and other purposes; not to mention the benefits that they will realize in the context of overall storage requirements if an archiving system is used to manage this content. Email is but one of the growing number of data types that contains business records and so must be archived along with documents created by users employing desktop productivity applications, documents stored in collaboration systems and repositories,

reports automatically generated by CRM systems, instant messaging conversations, voicemail, etc. All of these data stores and types can contain business records and so must be archived.

Having a single system to archive all of this content makes it much easier to manage information, since only one policy engine is required to manage corporate data retention policies instead of multiple applications across different systems, each of which is focused on a particular silo of content. Further, searching the archive is much easier and less prone to error if a single interface can be used to set up search queries across all of the data types that might contain relevant information. Further, overall costs are reduced because users that might need to access the archive can be trained on a single system instead of multiple ones, and potential compatibilities between the output formats of different solutions are eliminated.

### **CONSIDER YOUR NEED FOR LARGE DATABASE TABLE ARCHIVING**

Databases are generated by a large number of business applications and data in them is constantly changing. This data must be captured in state and should be retained according to the retention rules established for other types of ESI.

Large Database Table Archiving (LDTA), particularly for those organizations that will have extremely large quantities of data stored in databases, will need to focus on the right tools that can extract archivable data from operational databases.

## **Summary**

---

Virtually every organization – regardless of its size or the industry in which it operates – has legal and regulatory obligations to preserve electronic content, ranging from email to user-generated documents to content generated by automated systems. Further, the rapid growth of electronic content in most organizations necessitates the use of systems that can manage this content effectively and in a manner that can reduce overall storage and IT management costs.

Archiving of ESI can address these requirements. A properly specified, configured and managed archiving solution can help an organization satisfy its legal and regulatory obligations, contain or lower storage costs, and can significantly reduce the risk associated with managing electronic information.

## About Unify

---

Unify leads the advancement of industrial-strength archiving solutions to help companies manage risk and preserve the exploding volume of electronic records that have accumulated over the course of an organization's lifetime.

Designed for today's fluid, ever-changing business and regulatory climate, Unify helps reshape the way companies archive, discover and preserve the information assets stored in email, transactional systems, databases and social media systems scattered across the enterprise. With Unify for the first time, companies have complete protection and coverage of all data sources in a single, unified global repository.

Hundreds of the world's most-demanding customers trust Unify to help them confidently preserve data for legal discovery, regulatory compliance and corporate knowledge. Visit [Unify.com](http://Unify.com) to learn more.

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.