WHITE PAPER

Convincing Decision Makers of the Critical Need for Archiving

An Osterman Research White Paper

Published December 2011

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

DO YOU FILE A TAX RETURN?

Archiving electronic content – the processes and technologies associated with retaining electronic content for long periods – is a critical best practice that every company should follow. Retaining important content for the appropriate length of time is necessary to satisfy legal obligations to retain business records; to satisfy regulatory requirements to keep certain types of data, sometimes indefinitely; and to permit access to older data in a centralized content repository that will make it easy for IT, end users and others to meet their content requirements. As well, there are other benefits associated with archiving electronic content, including the ability to make email and other application servers more efficient by offloading older content, speeding backup and recovery processes, and improving an organization's disaster preparedness and their ability to maintain the continuity of the business after natural disasters, power outages and the like.

That said, most companies do not archive their electronic content in a coordinated or meaningful way. Osterman Research has found in numerous market research surveys that only about two in five organizations has a true archiving system – one that will index all content that should be retained for long periods, place this content into archival storage where it cannot be modified, and make it available via robust search tools when data must be extracted from the archive. To be sure, almost all companies perform nightly backups of their content stores, many take periodic snapshots of data for purposes of restoring data if necessary, and many use continuous data protection (CDP) systems to protect their data. However, most companies do not *truly* archive their content.

WHY DON'T MORE COMPANIES ARCHIVE THEIR CONTENT?

The objections to archiving tend to revolve around two major themes:

- Archiving preserves "smoking guns" – that content that might reveal poor judgment on the part of corporate decision makers or rogue employees that could harm a company at trial or during a regulatory audit.

- Archiving is simply too expensive, particularly when there are higher priorities for scarce IT dollars or when economic conditions mean that some things just cannot be funded.

THE GOAL OF THIS WHITE PAPER

This white paper will not attempt to deal with the first objection – the decision of whether or not you should avoid archiving because of the smoking guns in your organization – other than to offer two points of advice: first, don't do things that will get your company into trouble; and second, eliminating all of your incriminating content is futile – someone, somewhere will have a copy of it and it will come back to bite you.

Instead, the goal of this document is to deal with the latter objection to archiving. It will demonstrate that archiving can provide actual, hard cost savings for an organization,

meaning that instead of archiving representing a *cost* of doing business, it will actually be a way of *reducing* your overall costs and pay for itself in a relatively short time.

ABOUT THIS WHITE PAPER

This white paper discusses the various reasons to archive email and other electronic content. However, it goes beyond that to provide some concrete reasons and justification for deploying and maintaining an archiving system, most of which are based on the cost savings that archiving can provide – both direct cost savings and reduced costs arising from lowered risk. Further, information is also provided on the sponsor of this white paper, EdgeWave, and their relevant archiving solutions.

Does Your Organization Need to Archive Electronic Content?

In a word – Yes! You must archive all of your business records and business records that are stored electronically are no exception.

For virtually any company, there are five drivers for archiving, although the importance of these drivers will vary by the size of the organization, the industry in which it participates, the advice of internal and external legal counsel, and the locales in which it operates:

- **Legal Drivers**
  Email and other electronic content stores contain a growing proportion of business records that must be preserved for long periods of time. Further, this content is frequently requested during discovery proceedings because of the Federal Rules of Civil Procedure (FRCP) and state versions of the FRCP. As a result, it is critical that all relevant electronic content be made available for e-discovery purposes.

  Formally enacted in 1975, the FRCP governs court procedures for civil suits filed in the US federal courts. As a result of new amendments to the FRCP that went into effect in December 2006, the discovery of electronically stored information, including email messages, instant messages, word processing files, spreadsheets, presentations and other content, is now a mandatory point of discussion in civil cases. When subpoenaed for information, the responding party has a maximum of 30 days to respond according to Rule 34 of the FRCP.

  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 email sent from senior managers to specific individuals or clients, word processing documents that may

contain corporate policy statements, spreadsheets with auditors' opinions, and so on. 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 it is obligated to do so, it can suffer a variety of serious consequences, ranging from embarrassment to major legal sanctions or heavy fines. Litigants that fail to preserve electronic content 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.

Further, an archiving system allows an organization to perform either formal or informal early case assessment activities. For example, if a terminated employee has threatened to sue his or her former employer in a wrongful termination action, senior managers can search the archive for information that will help them determine the potential liability they face. If this assessment of the potential lawsuit results in a determination that the company was indeed wrong in firing the employee (the aforementioned smoking gun), they can instruct legal counsel to pursue a quick legal settlement. If, on the other hand, the assessment results in the discovery of information that supports the appropriateness of the company's decision, that information can be used to convince the ex-employee to drop the case or it can help win the case if it goes to trial. In either case, the archiving system can help the organization to understand its position early on, either avoiding unnecessary legal fees or an adverse judgment, or reducing its costs by proving the sufficiency of its case.

- **Regulatory Compliance**
  There are a large and growing number of regulatory obligations to preserve email. Some of the higher profile requirements are:

  - *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.

    As part of the American Recovery and Reinvestment Act of 2009 (ARRA), the provisions of HIPAA have been significantly expanded. A key component of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). Now, business partners of entities already covered by HIPAA, such as pharmacies, healthcare providers and others, are required to comply with HIPAA provisions. This includes attorneys, accounting firms, external billing companies and others that do business with covered entities. While these business associates were accountable to the covered entities with which they did business under the old HIPAA, these associates are now liable for governmental penalties under the new law.

Related to the point above is that penalties for HIPAA violations have been expanded dramatically. For example, if a covered entity or one of their business associates loses 500 or more patient records, they must notify HHS and a "prominent media outlet" to let them know what has occurred. Fines for violations can now reach as high as $1.5 million per calendar year.

- *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 email -- 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.

- *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 email blasts. The records may be "immediately produced or reproduced on 'micrographic media' [microfilm, microfiche or similar] or by means of 'electronic storage media'.

- *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.

- A small sampling of 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.

The regulations above are but a very small sample of the regulations focused on data retention that impact archiving requirements and practices. Additional regulations are shown in a table later in this report.

Key Data Retention Requirements
North America

Regulation	Retention Rules
Sarbanes Oxley Act	Relevant records must be retained for seven years. Company officers are required to report internal controls and procedures for financial reporting and auditors are required to test the internal control structures. Businesses are required to ensure employees preserve information, both electronic- and paper-based, that would be relevant to the financial reporting processes. Fine and/or jail sentence of up to five years for non-compliance.
Health Insurance Portability and Accountability Act	Safeguard the privacy of Protected Health Information. Non-compliance can result in a fine of up to $25,000 per year for incompliance. Fine of up to $250,000 and a maximum 10 years imprisonment for individuals involved in wrongful conduct with identifiable health information
Securities and Exchange Commission	Retain all records for a minimum of six years, the first two in an easily accessible place.
Federal Rules of Civil Procedure	No mandated length to which records must be retained. Responding party must respond within 30 days of a request for data 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 e-mails relevant to anticipated or ongoing litigation.

Key Data Retention Requirements
Europe

Regulation	Retention Rules
Data Retention Directive	In response to terrorist bombings in London in July 2005, the European Union in December of the same year passed a data-retention directive requiring all telephone and Internet traffic be stored for up to two years.
Data Protection Directive	This 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 EU businesses but also to anyone who uses equipment inside the EU to process data. For example, a U.S.-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).

Key Data Retention Requirements
Asia

Regulation	Retention Rules
Hong Kong Personal Data (Privacy) Ordinance	This regulation ensures personal data is accurate, up-to-date and kept no longer than necessary. Individuals have the right to access their data and to request that their data be corrected if they believe it to be wrong. There are a number of consequences for non-compliance, including a fine of HK$50,000 and a two-year jail term.
Hong Kong Code of Practice on Consumer Credit Card Data	In general, credit card issuers are required to keep consumer account data for five years from when the data was created, or 5 years after account termination.
Japan Personal Information Protection Act	This act ensures the privacy of information that is handled by government and private entities that collect or use personal information of 5,000 or more individuals. Organizations should ensure that personal data are kept secure from loss and unauthorized access and disclosure; notify individuals of how their personal information will be used; and to follow an individual's request for correction to their data. There are a variety of consequences to non-compliance, including a fine of up to 300,000 yen or a maximum six-month prison sentence for individuals who violate an order.

Key Data Retention Requirements
State, Provincial and Local

Regulation	Retention Rules
California Education Code	The code mandates a minimum of four-year retention policy for records but one year for emails.
California amendment to FRCP	California has a different view to the judge in the Zubulake case who ruled that electronic information could be deemed inaccessible if the cost of recovery is too high and if the resulting information may not be useful. California's e-discovery amendments appear to presume that all ESI is accessible, leading lawyers to note: "California's deviation from the federal rules […] indicates California's recognition that Zubulake is outdated due to technological advancements."
California Fair Employment and Housing Act (FEHA)	Code 12946 of this act 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.
Florida 119.01(1)(e)	"Providing access to public records by remote electronic means is an additional method of access that agencies should strive to provide to the extent feasible. If an agency provides access to public records by remote electronic means, such access should be provided in the most cost-effective and efficient manner available to the agency providing the information."
Louisiana Public Records Act	Public records include "information contained in electronic data processing equipment".
Massachusetts SPR Bulletin No. 1-99, last revised May 21, 2003	The commonwealth requires all its government officials to retain all business-related email messages and metadata and that such messages are considered public records. Massachusetts also requires retention of the message's metadata. Messages have to be retained and printed and filed in accordance with the agency's paper filing procedures. Large messages should be stored electronically.

Key Data Retention Requirements
State, Provincial and Local
(concluded)

Regulation	Retention Rules
Missouri Sunshine Law	A request can be made of any email record if the email requested was focused on public business and was sent to two or more recipients.
Ohio Publics Records Act	Requesters can ask to see public records kept by government agencies. Such records can be stored in a variety of media including email, voice mail and video. The requester has the right to choose the medium -- paper, film, electronic file, etc -- they would like the record to be duplicated. This means the agency has to organize and maintain its records so the request can be fulfilled promptly and at no cost during regular business hours, or to provide copies at cost within a reasonable period of time. The Ohio Supreme Court determined that a public office has a duty to recover contents of deleted emails and provide access to them.
Oregon ORS 192.410(6)	Includes email as a public record for purposes of the states open records statutes, but voicemail is specifically excluded as a public record.

- **Storage Management**
  A company does not have to have billions of documents to experience significant email storage growth. The dual drivers of cheaper disk storage and the increased size of email messages, thanks to attachments such as images and videos, is fueling the electronic content storage explosion. Messaging storage is growing at roughly 30% annually, which means that a terabyte of storage today will swell to nearly 2.5 terabytes in just three years.

  The implications of rapid storage growth can be significant. For example, the total cost of storage – including its acquisition, deployment, configuration, maintenance and power consumption – is anywhere from five to eight times the cost of the storage hardware itself.

  Archiving can be a very useful tool in reducing the volume of storage on email servers and in other electronic repositories, such as SharePoint or Quickr. One way to use archiving as a storage management tool is through the use of stubbing, in which email messages are replaced with "stubs" – roughly 10Kb links that point to content that has been migrated from users' mailboxes to the archive. When a user clicks on a stub, the message and attachment are retrieved from the archive and presented to the user as though the message were still in their mailbox. An alternative is to stub only attachments, leaving the message itself intact and replacing the attachment with a link. As with email stubbing, when a user clicks on the link, the attachment is retrieved from the archive. Another alternative is to migrate emails and attachments to the archive without the use of stubbing, allowing users to search for content directly from the archive.

  Regardless of the particular method used, the advantages of using archiving to control storage growth include removing large amounts of content from "live"

content stores like email servers or SharePoint servers and placing it on less expensive archival storage, as well as reducing the time required for both backups and restores.

- **End-User Self Service**
  Most IT staff members would wholeheartedly agree with the notion that users asking them to recover missing or deleted emails, files and other content is among the less pleasant aspects of their jobs. Aside from the difficulty associated with recovering this content, the time it requires takes away from other tasks that would allow IT to be more productive and contribute more to the company.

  An appropriately designed archiving capability allows IT staff to put users in charge of recovering their own missing or deleted content, freeing IT from the burden of doing this for them. This can result in significant cost savings, as discussed later in this white paper, as well as recovery of IT time that otherwise would be spent on this important, but unproductive, task.

- **Knowledge Management / Data Mining**
  As employees rely on email, collaboration tools and other content repositories as the primary tools they use to do work, it is important for companies to be able to extract business intelligence from the content that employees generate. Some archiving systems enable customers to quickly locate emails up to 15 years old and extract information, such as the identity of users' email correspondents or reports they generated. This could be useful, for example, when a new employee is required to trace back correspondence and other content between his or her predecessor and a customer. There are also sophisticated tools that can perform automated, large-scale retrieval and rigorous in-depth analysis of archived content, adding to the value of what archiving can offer a company.

Cost Justifying the Deployment of Archiving

JUSTIFYING ARCHIVING TO YOUR BOSS(ES)

One of the most important considerations in the process of selecting an archiving solution is to first justify the need for archiving to senior decision makers, since not everyone agrees that email and other content archiving is a sound business practice. For example, roughly one in eight IT decision makers believes that deleting all email content on a regular basis is the least risky option, since it reduces the likelihood that incriminating evidence will be found during legal discovery, a regulatory audit, etc.

If you're trying to justify archiving, there are some hard cost savings that any organization can realize by deploying the right archiving capability, whether hosted or on-premise. Further, there are some additional savings and risk mitigation issues that archiving can also provide – these are discussed in the next section.

In the following examples, we will use the following assumptions:

- Fully burdened IT staff member salary: $80,000

- External legal counsel fees: $200 per hour (average of attorneys and paralegals)

SCENARIO 1: E-DISCOVERY OR REGULATORY AUDIT

- **Without archiving**

  Just about every organization of any size will need to go through an e-discovery exercise at some point, either directly as a litigant in a legal action or in support of another organization that is directly involved in a lawsuit. Further, heavily regulated organizations like broker-dealers will periodically need to respond to regulatory requests for information. These types of requests, which today are a key component of most legal or regulatory actions because of the large and growing proportion of business records stored electronically, have become a fact of life for most organizations.

  Let's say that a 500-seat organization must respond to an e-discovery or regulatory audit request and all of its electronic content is stored on 500 backup tapes. Further, let's assume that IT will spend 30 minutes loading each tape into a recovery server and copying the data to a central repository for processing by legal staff. Another 24 hours of IT staff time will be required to address issues like corrupted .PST files, tapes that cannot be read, etc. Let's also assume that legal staff will require 320 person-hours to search through this repository for relevant content (the equivalent of one person working full time for eight weeks). This figure can vary widely based on the type of data through which legal must search, but this figure is based on a real-world example.

  Using the assumptions above, an organization will spend 250 person-hours of IT staff time at a total cost of $10,538 (250 hours x $38.46/hour) to recover the data from the backup tapes. Further, the cost of legal staff will be $64,000 (320 hours x $200 per hour), yielding a total labor cost of $74,538 for just a single e-discovery exercise or a regulatory audit.

- **With archiving**

  Now, let's assume that the organization has an archiving system that can be accessed by legal staff directly. Although archiving systems can vary widely in price based on their feature set, licensing costs and other factors, let's assume a three-year cost of $120 per seat (including acquisition, support and maintenance costs), or $60,000 for the entire organization. We'll further assume that an organization will need to go through 10 e-discovery or regulatory audit requests over a three-year period. If we spread the cost of the archiving system over just these requests, that results in a cost per request of $6,000 for the archiving system.

  Using the same assumptions as in the example above, we can eliminate the IT cost, since the legal staff can access the archive directly without any involvement from IT. Further, because the archived information has already been indexed before being archived, searching across the archive will be much simpler and faster. If we conservatively assume that the legal staff time will be halved when using an archive, the legal labor cost will be $32,000 (160 hours x $200 per hour), although in many cases the reduction in time spent by legal will be significantly lower than this.

Based on these assumptions, the cost of a single e-discovery exercise or regulatory audit will be $38,000 ($32,000 in labor and $6,000 for the archiving system), resulting in a net savings per request of $36,538. Based on the rather conservative assumption of 10 e-discovery requests every three years, that results in a total savings of about $365,000 over a three-year period.

SCENARIO 2: SETTLING A LEGAL ACTION BEFORE GOING TO TRIAL

- **Without archiving**

  Let's assume a similar situation to the one above – a sort of informal discovery conducted by senior management and external legal counsel as part of an early assessment of a potential lawsuit. This is the type of exercise that might be conducted if management suspected that some situation – such as a faulty product that injured a customer or an employee terminated under difficult circumstances – might result in a lawsuit. This action would probably be less extensive than the e-discovery example above and, for purposes of this example, would involve searching only through 100 backup tapes.

  In this example, let's assume that 20 such exercises will be conducted over a three-year period, each one at a cost of $14,908 (one-fifth the cost of a full e-discovery exercise). The total labor cost of these early case assessments, therefore, would be $298,152 over a three-year period.

- **With archiving**

  Now, let's assume that an archiving system could be used to conduct these early case assessments. Using the same assumptions as shown above (20% of the effort of a full-blown e-discovery or regulatory audit exercise), the total cost of legal staff examining content from the archive will be $6,400. Add to this the cost of the archiving system ($60,000) spread out over 20 early case assessments and the total cost per assessment will be $9,400, or a total three-year cost of $188,000. The net savings from the use of an archiving system, then, will be $110,152 over three years.

SCENARIO 3: END-USER SELF SERVICE

- **Without archiving**

  Users periodically delete content that they will need at some point. This content might be a word processing document they have taken a considerable amount of time to write, an email with an important communication from a customer, or a financial spreadsheet. For purposes of this example, let's again assume a 500-person organization and each employee needs to recover just one document per month. This results in a total of 6,000 documents that need to be recovered each year (500 employees x one document per month x 12 months). Let's further assume that IT requires an average of 30 minutes to recover each document from a backup tape.

  Assuming that IT even has the bandwidth to recover all of these documents, IT staff members will spend a total of 3,000 hours annually (6,000 documents x 30 minutes per document) recovering this content. The total IT cost of document recovery, therefore, will be $115,385, the equivalent of 1.44 full-time IT staff members.

- **With archiving**
  Now, let's assume that the organization has deployed an archiving system that has been configured to allow individual users to access their own archived content. If we assume that five minutes will be required to recover a document and that the average employee salary is identical to that of IT staff members, then the total cost of employees recovering their own documents will be $19,231 annually (6,000 documents x five minutes of recovery per document). The total annual savings compared to IT recovering the documents will be $96,154. Factor in the cost of the archiving system (average of $20,000 per year) and the cost savings from end-user access to the archive is still a significant $76,154 per year.

SUMMING UP

The examples of cost savings with an archiving system discussed are summarized in the following table.

Savings Provided From the Use of an Archiving System for Various Tasks in an Organization of 500 users

Task	Without Archiving	With Archiving	Savings
Conducting one e-discovery exercise or going through a regulatory audit	$74,538	$38,000	**$36,538**
Settling one legal action before going to trial	$14,908	$9,400	**$5,508**
End-user self service to older content for a period of one year	$115,385	$19,231	**$96,154**

If we assume that each of the scenarios discussed above would apply to a typical 500-person organization, then an archiving system that cost $60,000 per seat over a three-year period would end up saving an organization a total of $884,002 (across all three scenarios) during that period for a net savings of $824,002 over three years. Even if we assume that an archiving system would cost three times our estimate of $120 per seat over three years, or $360 ($10 per seat per month), the cost savings would still be a very substantial $524,002 over three years.

Other Justifications for Archiving

In addition to the justifications for archiving based on quantifiable cost savings, there are a variety of important justifications that are not as readily quantifiable or as predictable. For example:

- An inability to produce all required content during e-discovery can result in sanctions directed against the party that cannot produce the necessary content. This might represent nothing more than incurring a judge's ire during legal proceedings, or it could result in significant sanctions. For example, in *Keithley v. Homestore, Inc.*[1],

[1] Kevin Keithley v. The Home Store.com, Inc., 2008 U.S. Dist. LEXIS 61741 (August 12, 2008)

Keithley won on summary judgment, but still had to pay $283,000 in fees for its failure to produce required electronic evidence. In *Qualcomm, Inc. v. Broadcom Corporation*[2], Qualcomm initially prevailed, but it was later discovered that thousands of emails were not produced during the case. As a result, the Court awarded $8.5 million in attorney's fees and costs against Qualcomm. In some cases, judges have instructed juries that a party's inability to produce required content can be considered evidence of culpability.

- An inability to produce data on demand can result in the loss of reputation, brand damage or lost opportunities for future revenue. If, for example, a broker-dealer is sanctioned by the Securities and Exchange Commission for its failure to retain and produce data, the negative press that could result can harm the company's reputation with its shareholders and prospective customers.

- As noted earlier, if an organization must go through an e-discovery exercise or a regulatory audit using only backup tapes or some other "quasi-archive", a substantial amount of time can be spent responding to the request for information. In addition to the direct cost associated with IT and legal staff extracting and poring through the data, there is also an opportunity cost associated with doing so. The result can be delays in other projects, postponement of infrastructure upgrades and the like, any of which can have consequences that may be difficult to quantify, but are nonetheless impactful.

- One of the primary functional benefits of an archiving system is its ability to act as a repository for older electronic content that might otherwise be stored on email servers or file servers. By migrating older content to an archive, email, file and other servers can operate more efficiently, backup windows for these servers are shortened, and restores can be accomplished much more quickly. For example, if 1,000 users are served by an email server that has gone down and the restoration process can be shortened by just one hour because an archiving system has permitted the data store to be smaller, that can result in a significantly lower productivity loss for those users.

The bottom line is that archiving is, at its core, not a cost of doing business, but a viable means of reducing costs.

[2] No. 05-CV-1958-B(BLM), 2007 WL 2296441 (S.D. Cal. August 6, 2007)

Sponsor of This White Paper

EdgeWave
15333 Avenue of Science
San Diego, CA 92128

+1 858 676 2277
www.edgewave.com

ePRISM EMAIL ARCHIVE

EdgeWave Email Archive is a secure enterprise SaaS solution for storage management that retains email in an unalterable state to help meet compliance requirements, provide litigation support and meet corporate best practices guidelines. EdgeWave's policy-based archiving and built-in reporting features combine with easy-to-use management tools that assure archived messages are indexed and easy to retrieve whenever you need them.

ePrism's email archiving offers a rich feature set including support for client software integration, email stubbing to maximize server storage, mobile archive access, litigation support tools, centralizing, importing all historical emails and more. It supports all major messaging servers including Exchange, Domino, GroupWise, and Linux-based environments and can be deployed easily with minimal resource expenditures. Archived email is hosted in a secure environment with industry-leading archiving performance, high availability, and disaster recovery. Data is encrypted as it leaves your corporate networks, to be stored in our secure archive with 128-bit encryption.

UNRIVALLED SECURITY AND PRIVACY

ePrism Archive secures data at three levels, physical infrastructure, data encryption, and the application layer, to assure that data is always secured in transit and at rest. Our data storage is secured via industry standard encryption. There is never any co-mingling of archived data between customers. At the application layer, we use Secure Socket Layers (SSL) to encrypt all communication between the web browser and the data center, and a processing pipeline that insures performance and data privacy among all customer accounts.

EASE-OF-USE AND LOW TCO

As a pure hosted service, ePrism Archive is easy to use and requires no software installation. Deployment can be immediate and migrating your data into the cloud shrinks internal storage and maintenance costs by reallocating or eliminating on-premise or hosted servers. The simple and intuitive web-based interface makes rapid search and retrieval easy.

FASTEST SEARCH AND RETRIEVAL

ePrism Archive uses cloud-compute infrastructure for scalability and reliability. A unique and differentiated cloud-compute software stack harnesses on-demand CPU and geographically dispersed storage to power archival functions for data ingestion, indexing, search, eDiscovery and export. The EdgeWave system uses map-reduce style parallel processing to search very large data sets in sub-second response times. Parallel processing is only possible with cloud-compute CPU, because of its ability to scale up in real-time. This makes every search experience rapid with no waiting for jobs to

complete.

THE ePRISM SUITE OF COMPREHENSIVE SOLUTIONS FOR EMAIL SECURITY

- **Email Filter** – a completely hosted solution that safeguards corporate networks from spam, viruses, and criminal malware on both inbound and outbound mail streams. Includes *Zero Minute Defense* for protection from emerging threats in real-time.

- **Data Loss Protection** – keeps sensitive data from leaving the security of your network.

- **Email Encryption** – Confirms the secure delivery of corporate email in accordance with industry or regulatory requirements or corporate security policies.

- **Email Continuity** – delivers rapid failover during planned or unplanned outages to maintain uninterrupted mission-critical business communications.

ABOUT EDGEWAVE

EdgeWave™ develops and markets innovative Secure Content Management (SCM) solutions including iPrism Web Security and the ePrism Email Security Suite. EdgeWave innovative technologies deliver comprehensive protection with unrivalled ease of deployment and the lowest TCO on the market. The company's award winning solutions can be delivered as hosted, on-premises, and hybrid services.