

Top 10 Concerns: Legacy Archiving Solutions

ZL TECHNOLOGIES, INC.
WHITE PAPER





Table of Contents

Introduction 2
 Survey Sample 2
 Survey Results..... 5
 Conclusion 8
 About ZL Technologies..... 9

List of Figures

Figure 1: Number of Survey Respondents 3
Figure 2: Surveyed Corporations by Industry..... 3
Figure 3: Surveyed Companies' Satisfaction with Current Email Archiving Solutions 3
Figure 4: Surveyed Companies by Industry 4
Figure 5: Surveyed Companies by Region 4
Figure 6: Surveyed Companies by Size..... 5
Figure 7: Top 10 Concerns with Legacy Email Archiving Solutions 5

Introduction

The term “email archiving” has been co-opted and applied to different markets and applications over the past few years. Simple, single-function archiving applications were sufficient to address a basic market need, which generally revolved around mailbox management or server offloading. Such applications were designed to handle one or two departments, and only mail deemed valuable enough to keep, not an entire corporations’ email for up to seven years.

Offloading applications focused on restoration of individual email at the user level. They weren’t designed for immediate or complete capture, let alone global viewing of the archive. Compliance applications evolved to meet retention and surveillance regulations where complete or immediate capture was a base requirement, with supervisory oversight and review of mail at a corporate level necessary. Discovery applications grew out of the need to search across corporate email to quickly, and cost effectively, produce email and attachments in response to a legal subpoena. Because the basic capture and data management requirements differed for each need, stand-alone applications were developed, in widget fashion, to address the different markets.

Today, the email archiving marketplace is in the throes of a convergence, but the original requirements are so different that legacy archiving solutions designed for one specific market need have not been able to seamlessly extend their primary functionality to cover the other areas. In addition to the change from “archiving some” to “archiving all” email, corporations now need additional features that weren’t part of original archiving requirements, such as audit trails, search and retrieval, pre- and post-review of emails, and extensive corporate retention and management policies. Worse yet, when archiving demands increase exponentially from archiving under 1,000 mailboxes to over 5,000, or 10,000... legacy archiving solutions simply cannot scale to handle those volumes for compliance, legal discovery, or mailbox management, let alone a combination of the three.

ZL conducted this survey to determine exactly what is causing the most headaches among corporations that deployed legacy email archiving solutions more than 2 years ago. Some of these issues may be relatively simple to fix, but others may require further consideration as to whether their solution can continue to meet the mounting needs of the corporation.

Survey Sample

This survey examines the results of an internal survey conducted by ZL Technologies, Inc. between May and August 2006. The survey was conducted across 145 companies, representing a total of 864,523 users. Corporations surveyed were not current customers of ZL Technologies at the time of the survey.



Total number of Corporations	145
Total number of Users Represented	864,523

Figure 1: Number of Survey Respondents

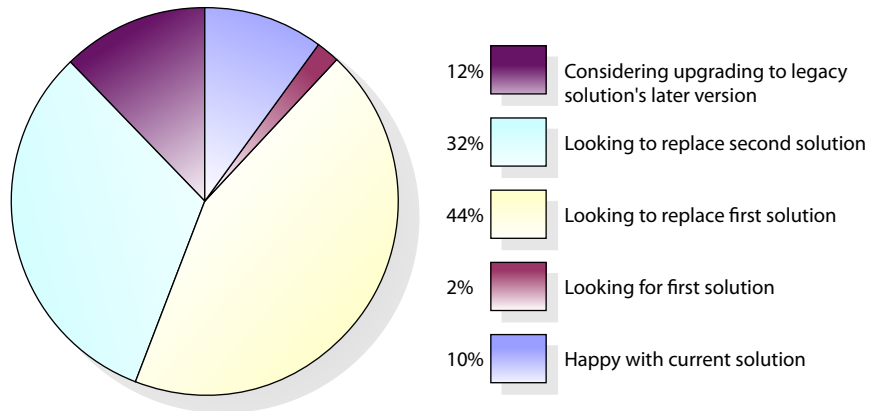


Figure 2: Surveyed Corporations by Industry

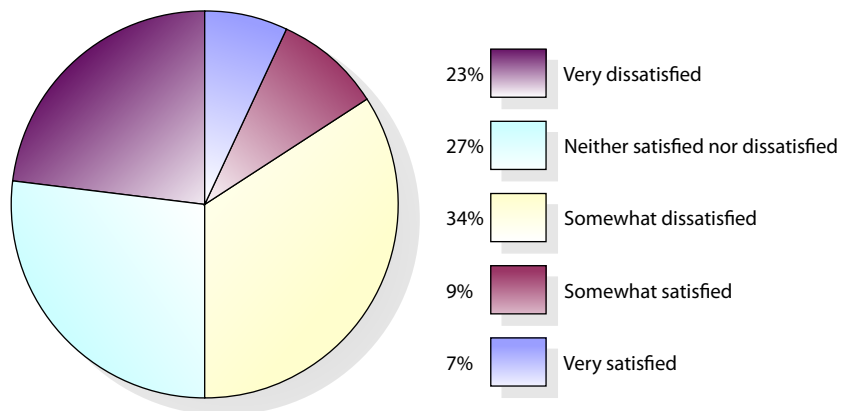


Figure 3: Surveyed Companies' Satisfaction with Current Email Archiving Solutions (out of 142 companies)

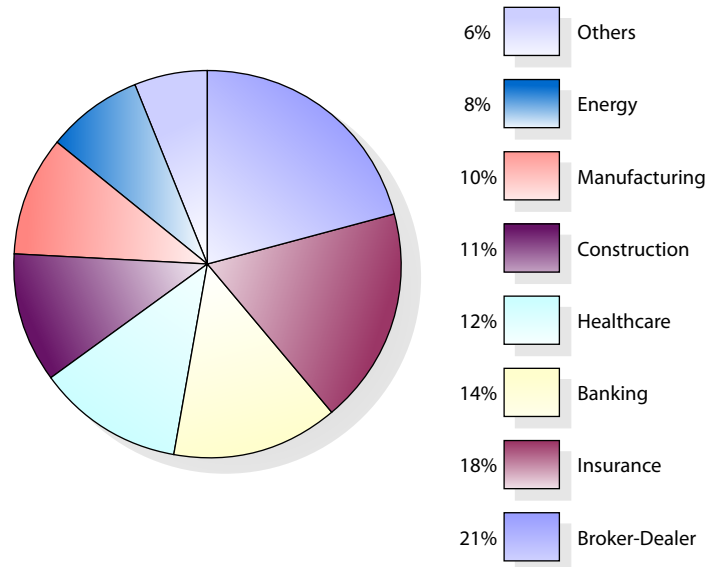


Figure 4: Surveyed Companies by Industry

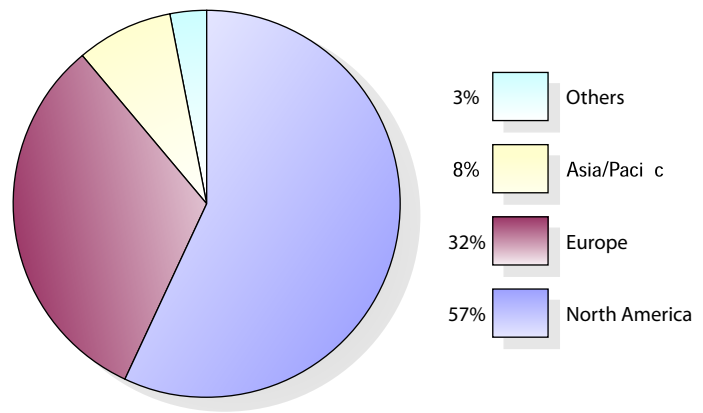


Figure 5: Surveyed Companies by Region

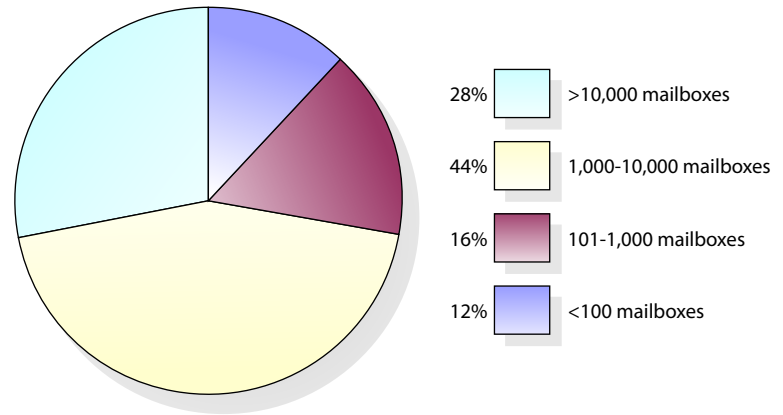


Figure 6: Surveyed Companies by Size

Survey Results

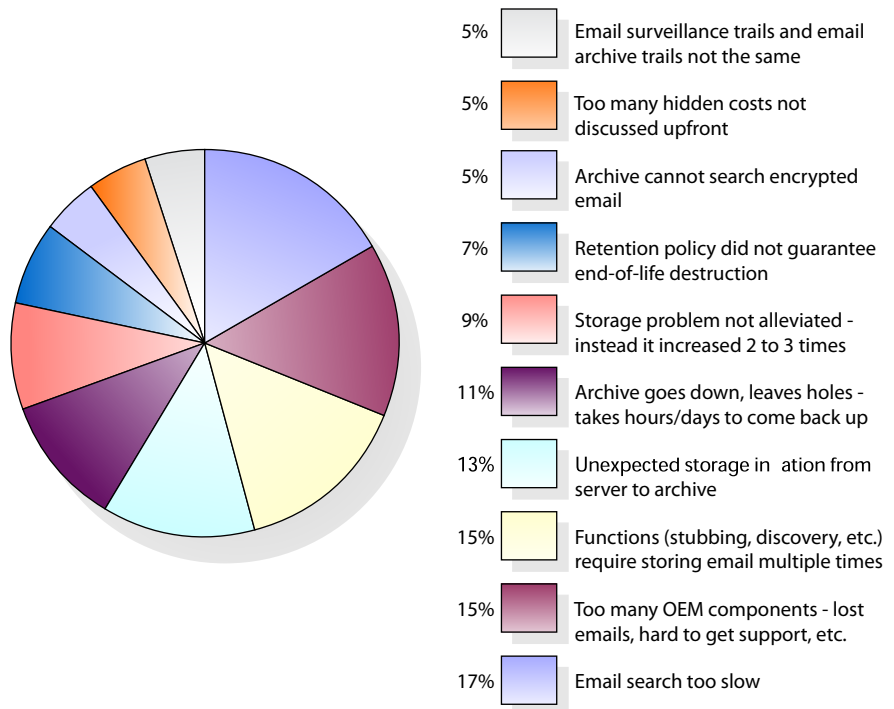


Figure 7: Top 10 Concerns with Legacy Email Archiving Solutions (out of 142 corporations)

1. 17% – Email search is too slow – too slow in retrievals, too slow in refinements, and inconsistent in results.



- Searching through the archive could take 15 minutes to a full day.
 - Compliance with regulations and discovery requests can require emails to be produced in as little as a few hours. If companies are too slow or unable to produce them, they can be charged with failure to comply. Some respondents said they had to set up a query at the end of the day so it could run overnight.
- 2. 15% – Third parties used for critical components – vendors use OEM components for critical parts and when things break, it leads to finger-pointing and poor support experience.**
- Many legacy vendors have to OEM components such as the search engine, or gateway capture, in order to have a “full solution” that can perform mailbox management, compliance, and legal discovery functionality. This results in a “Frankenstein” archive, or a black box, which may contain pieces that have been end-of-life’d, or aren’t well supported by the archive vendor or their creator.
- 3. 15% – Duplicated storage – even if the same vendor, compliance/discovery and mailbox management need separate storage.**
- Double or triple functionality means double or triple the storage. Legacy archiving vendors, which originally offered Mailbox Management/stubbing functionality, were designed to capture emails from the user mailbox at the time they would be stubbed (6 months, 1 year later, etc.).
 - To add further functionality such as compliance, legacy vendors have to layer journal capture on top of the stubbing function. Discovery applications and some review modules require companies to store the mail again, separately, in a database or stand-alone folder. Each capture method is independent of the other, and keeps emails in separate stores to perform the various functions, thereby storing a single message multiple times.
- 4. 13% – Unable to read archived email – proprietary archive format cannot be read when archive system goes down or is replaced.**
- As a result of the proprietary format in which the emails were stored, and the lack of true global Single-Instance-Storage, some companies experienced 1.5 to 2 times storage inflation from the email server to the archive. Ex: A 2GB email server could inflate to 3.5GB at the archive level due to proprietary email formatting and proprietary email “wrappers”.



- The larger problem at hand is that the proprietary archive format cannot be read when the archive system goes down, or is replaced.
- 5. 11% – Unstable archive, unreliable record – after 2+ years the archive struggles with volumes and keeps crashing, creating gaps in the record.**
- When the archive is down or offline, there is no guarantee that it is capturing emails sent/received during that time (if the archive didn't crash the email server) for future search and discovery. This results in an unstable archive and unreliable record after struggling for years with volume problems and constant crashes that leave gaps in records.
 - Also, some legacy vendors “empty” the journal box before confirming that records have been ingested. If the system crashes while processing emails, the messages disappear into cyberspace and leave a time gap in the archive.
- 6. 9% – Mail storage increased, not decreased – inefficient archive storage, increases storage hit 2 to 3 times.**
- Mail storage increased, not decreased, as a result of inefficient archive storage. A few legacy archive solutions encase messages in a proprietary wrapper that inflates the message size in the archive. Emails may indeed be offloaded or compressed, but when their size is first increased, this only aggravates storage size problems.
 - Further, respondents reported inflation due to extra copies (html or text) being stored with the original message. A 10K message ingested into the archive increases in size up to 2-3 times, significantly inflating the archive storage.
- 7. 7% – Retention policy did not guarantee the end-of-life destruction of emails.**
- False retention policies – emails are not deleted at the end-of-life, even when policies claim guaranteed disposition.
 - Email goes through a 4-stage lifecycle (capture, short-term retention, long-term retention and end-of-life deletion), but most legacy archives only handle the first three. Most legacy archives can enforce retention policies, but are not able to actually delete the messages once the policy has expired. Worse, some systems can delete the email but retain the index, proving the email existed but was in fact deleted – increasing liability.
- 8. 5% – Archive cannot search across encrypted emails.**



- Emails encrypted in transit to meet HIPAA and GLBA compliance cannot be indexed unless the archive has the keys to decrypt the emails, or the emails are previously decrypted and archived as clear text. If the archive cannot index the encrypted emails, the messages cannot be found in the archive. Such a black hole jeopardizes SEC/NASD/SOX compliance.

9. 5% – Too many large hidden costs not discussed upfront.

- These include hidden installation/deployment/support fees and having to purchase mandatory professional service (maintenance, training etc.) and large migration fees.

10. 3% – Outbound email audit trails to not match journal audit trail.

- Outbound email audit trails that do not match the email server's journal audit trail present conflicting information about actions taken on emails with compliance violations.
- Companies that use journal-only archives but want to add pre-review and surveillance/content filter functionality have to purchase stand-alone solutions. The journal record will log messages as ok and sent in the archive – even if the stand-alone content filter caught and quarantined the message. Conflict resolution only occurs after the problem is caught, usually during an audit; by reconciling the different audit trails from the archive journal and content filter.

Conclusion

The confluence of markets and increases in email archiving demands has exposed the flaws of legacy archiving solutions. Many organizations are dissatisfied and looking to replace their old products with a new, highly-scalable and available, feature-rich solution that can unify the functionality of archiving for storage, regulatory compliance and discovery/corporate governance today, as well as meet tomorrow's needs. Today, over 80% of legacy email archiving solutions fails to live up to expectations. Over 60% of ZL's customers to date are replacement customers, choosing ZL Technologies to replace EMC/Legato, CA/iLumin, Symantec/Veritas/KVS, ZANTAZ, and others.

Learn more about why a Top 5 Global Bank and a Top 5 US Bank chose ZL to replace their incumbent solutions, and why Morgan Keegan decided on ZL after 2 failed email archiving installations. Contact ZL Technologies by visiting us online at www.ZLTI.com or send us an email at sales@ZLTI.com.



About ZL Technologies

Established in 1999, ZL Technologies, Inc. (ZL) provides cutting-edge enterprise software solutions for email archiving, regulatory compliance, litigation support, corporate governance, content management, file archiving, and secure email. ZL's flagship product, the Unified Archive, offers comprehensive email and file archiving and management for companies using Lotus Notes/Domino, Microsoft Exchange, Bloomberg, and others. The suite provides a highly flexible framework that is fully scalable, enabling organizations of all sizes to meet legal discovery, compliance, and storage management requirements. With a proven track record and an impressive list of clients, including Walgreens, Bank of New York Mellon, Pacific Life, and Morgan Keegan, among other top global institutions, ZL has emerged as the premier provider of email archiving and compliance solutions. For more information, please visit www.ZLTI.com