



Death to PST Files: The Hidden Costs of Email

A MessageLabs whitepaper highlighting the problems that email archives and PST files can create for organizations and how the right solution can reduce these risks.

Introduction

Email is the lifeblood of modern business. More than three-quarters of an organization's business-critical data is now in email form, according to analyst research.

The problem with PST files

Email is the holder and medium of so much information that nobody likes deleting old messages. Many people use their email system as a personal filing cabinet. Text-only emails do not use much storage but problems start with attachments.

Most companies impose quotas that limit how much storage each associate can use for emails. Without these quotas, server disk drives would overflow and email systems would come crashing down. But they have an unwelcome side effect: users create their own email archives using PST files.

Private, local PST files and personal email archives create a number of problems for businesses that allow them:

- **Attachment multiplication.** Imagine you send a 1MB PowerPoint presentation to ten colleagues and they all move that email into their own PST file. Now there is 10MB of duplicated data.
- **Bloated backups.** If each of those PST files is stored on a company file server and it gets backed up every day and the IT department keeps ten days' worth of backup tapes, the original attachment is now consuming 100MB of backup storage.
- **Slow, inefficient backups.** Instead of backing up a single 1MB file, the IT department has to backup 10MB a day for ten days. This takes more time and money: the more data there is to backup the more tape is required. Ultimately, backup bloat demands more expensive backup devices.
- **Broken backup windows.** Most companies backup overnight but, if backup sets grow too big, there is a risk the backup may not be completed in time, or that it might overrun, slowing down normal IT operations during the working day. Round-the-clock or global operations make it even more important to complete backups quickly.

What is a PST file?

PST stands for Personal Storage Table. A PST file is used by Microsoft Outlook to store email messages, calendar items and other Outlook data. In contrast to normal Microsoft Exchange Server information, which is stored on a server and accessed by Outlook, a PST file is typically stored on a user's local hard disk or (more often in a corporate environment) on a file server. Users often employ PST files to circumvent server storage quotas.

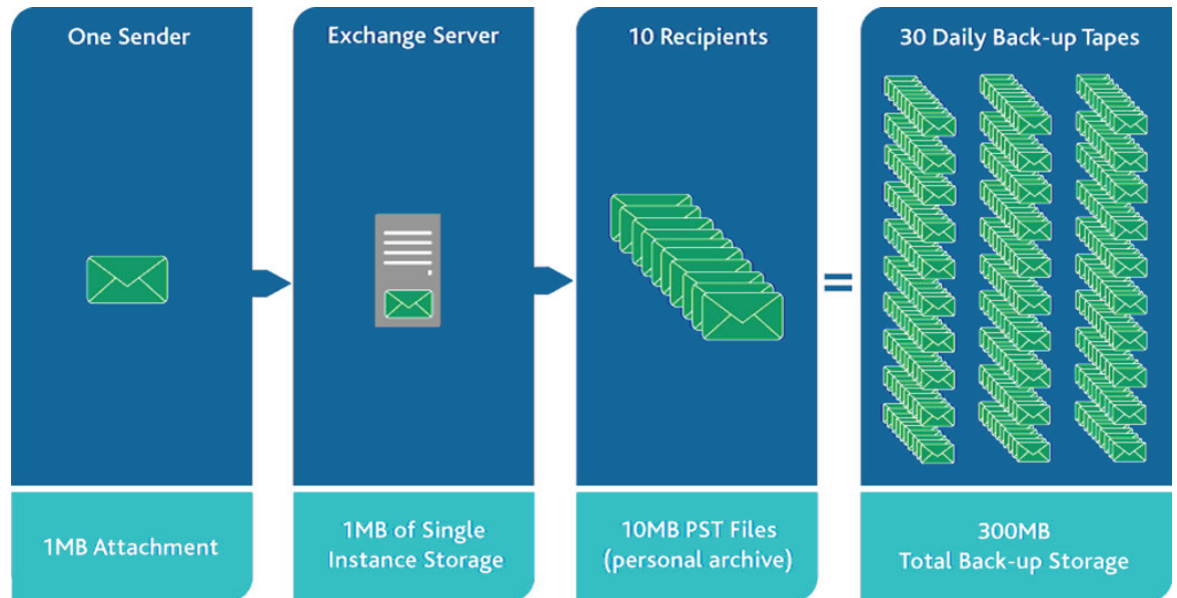
Security risks

The uncontrolled proliferation of PST files poses risks for businesses beyond the IT department.

- **Organizational amnesia.** Every email that disappears into the black hole of PST files takes a piece of the company's knowledge with it. If the PST file's owner leaves the company, there is a risk that the information in the PST file will never be brought back under company control.
- **No oversight.** Information in PSTs does not get stored and disposed of according to consistent company policies. This can give lawyers headaches.
- **Legal liabilities.** If a company needs to keep a formal archive of emails sent and received to comply with regulations, PST files represent a gap in the record. An email stored in a properly managed email server can be a vital defense in a lawsuit, but how do you know what's on 1,000 different ad hoc PST files? Even without a legal dimension, the inability to locate a critical email quickly could be commercially disastrous.
- **Laptop loss.** A PST file stored on a laptop is unlikely to be encrypted. So, if the laptop was lost or stolen, a thief would have ready access to the email stored on it. This might include information

Email is the lifeblood of modern business. More than three-quarters of an organization's business-critical data is now in email form, according to analyst research.

The hidden cost of PST files



that is covered by the Data Protection Act and other regulations. For example, In February 2007, the BBC reported that the Financial Services Authority fined the Nationwide Business Society £980,000* because of the theft of an employee's laptop containing customer information .

The MessageLabs Archiving Service

The MessageLabs Archiving Service stores users' attachments in a secure, offsite data center. It replaces attachments with an HTML link to the file in MessageLabs offsite archive. This is a process called "attachment stubbing."

Users still have access to the attachments by simply clicking on the link, but they no longer use up their storage quota. In turn, this eliminates the main reason that users create PST files. Once archiving is in place, the IT department can prevent the creation of new PST files and help users migrate data in existing PST files to the new archive.

The MessageLabs Archiving Service can also archive emails themselves, creating a well-managed, encrypted, searchable database of every company email. Companies can set policies about what is archived and who can access the archive.

The benefits are clear:

- Give users virtually unlimited mailbox quotas, eliminating the need for PST files
- Reduce backup sizes and increase backup performance
- Slow the demand for new in-house storage and backup equipment
- Keep control of critical company information; everything stays on the company mail server and in the MessageLabs Archiving Service
- Create a searchable, secure and, above all, comprehensive archive of all the company's emails

Our own experience

Here at MessageLabs, we take our own medicine. We use our MessageLabs Archiving Service. Before we implemented it, we were backing up 648GB every day and 32 percent was PST files. With our solution in place some mailboxes shrunk by more than 80 percent. Getting rid of this overhead has speeded up backups and given us better control over our email systems.

*Equivalent to \$1,940,596.00 USD
<http://news.bbc.co.uk/1/hi/business/6360715.stm>

Installing the system was painless. There are two parts. First, there is a slim appliance – a small server – that links the company email server with the MessageLabs Archiving Services. The other part is the offsite archive itself. It's managed by MessageLabs with guaranteed service level agreements for availability and search response time. The appliance pulls emails and attachments out of the server, encrypts them and sends them to us for online storage.

As our internal systems manager put it, "A couple of my associates set this up. It was easy. It only took a couple of hours. I wish we had done it sooner."

To learn more about the MessageLabs Archiving service visit us online at <http://www.messagelabs.com/products/archiving/>.

Most companies backup overnight but, if backup sets grow too big, there is a risk the backup may not be completed in time, or that it might overrun, slowing down normal IT operations during the working day.





Americas

AMERICAS HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION

7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
T +1 952 830 1000
F +1 952 831 8118

Asia Pacific

HONG KONG

1601
Tower II
89 Queensway
Admiralty
Hong Kong
T +852 2111 3650
F +852 2111 9061

AUSTRALIA

Level 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

SINGAPORE

Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
T +65 6232 2855
F +65 6232 2300

Europe

HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON

3rd Floor
1 Great Portland Street
London, W1W 8PZ
United Kingdom
T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS

Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG

Culliganlaan 1B
B-1831 Diegem
Belgium
T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH

FeringasträÙe 9
85774 Unterföhring
Munich
Germany
T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999