Barracuda®

A Guide to PST Files

How Managing Your PSTs Will Benefit Your Business

White Paper

Introduction

PST files are widely used in many organizations and often contain business-critical or sensitive data, but they are frequently completely unmanaged and can present a significant risk to the organization as well as causing ongoing issues for IT support teams.

In this White Paper we take a look at these files and the problems they can cause. We then discuss the options for addressing these problems, and conclude with a summary of the benefits an organization can realize by managing PST files.

What Are PST Files?

An unfamiliar term to those outside of IT, they are often known as Outlook Archives or Personal Archives, and are typically created by Outlook when the "Auto Archive" function is enabled. PST is actually an acronym for "Personal Storage Table" but that term is not often used.

The auto-archive function in Outlook allows users to bypass the mailbox quota limits which IT departments may enforce as a result of size limitations with their central Exchange server. This feature was turned on by default in Outlook 2003 and 2007, and generated PSTs as container files to store email locally for the user.

Where Are They Located?

PST files can be located almost anywhere. By default, Outlook will create them on a user's desktop or laptop, however that does not stop them being located on corporate servers, removable media such as USB and flash drives etc., or even home PCs.

Are They Secure?

This depends on a number of factors, but normally they are not.

PST files are highly portable, as they can be disconnected from Outlook and copied or moved to another Outlook client with ease, and they are also widely used as a great way of moving email data between people and/or organizations quickly. They can be password protected, although a simple search on the internet will find any number of programs that can crack these passwords.

Are They Reliable?

PSTs are notoriously unreliable, as they were never designed to hold the amount of email data they often do today. Users keep pouring more emails into them, blissfully unaware of the risk this poses to their data, and 10 or 15% of an IT department's daily helpdesk calls can be taken up with looking after these files.

Due to their size, they are also susceptible to internal corruption if they are located on a network share or accessed over a network, and Microsoft specifically advise against accessing them this way.

Are They Always Available?

The perception for a lot of users is yes, but this is not always the case, as Outlook must have access to the location where the PST file is stored. This is fine for office-based users who have the same access to either local or network storage, however if the user has the ability to work from different desktops or locations they may not be able to always access their PSTs. Also, if the user uses Outlook Web Access (OWA) then they cannot gain access to their files.

PST files can easily be disconnected by users from their Outlook profile, either inadvertently via a failure such as a power outage or PC crash, or by the user 'closing' them. For some users this is standard practice when they are managing a number of PST files, and these PSTs can be reopened at any time as long as the user knows their location. But for most users, once the PST is 'closed' it is either forgotten about or they cannot find it again, thereby creating an 'orphaned' PST. Orphaned PST files can still contain valuable business information that may need to be preserved and made available.

Are They Backed Up?

This depends on their location and how the IT department is managing them. If they are located on desktops and laptops there is a high probability they fall outside the corporate backup strategy, and are therefore not protected. If however they are located on network shares, then the chances are they are being backed up. However, this in itself brings a set of new challenges for the IT department.

Do Companies Still Use Them?

Yes - as many companies will copy a former employee's mailbox to a PST as a method of retention. These practices can change from time to time or be overlooked, so consistency may be a problem. Companies also frequently use them for passing large amounts of email data around between locations or even between organizations.

Do Employees Still Use Them?

Yes - although, there is a high chance they don't know it. Many workers favor the "Auto Archive" as a way to organize and keep older emails without understanding the risks, particularly if their mailbox is restricted by quota limits.

Do PSTs Fall Under Compliance and Legal Hold Requirements?

The PST file itself does not, as it is merely a container, but the emails and attachments that are stored within the file do. Since most legal discovery occurs sometime after the alleged incident, not knowing the location or indeed the owner of PSTs can make legal hold and compliance problematic.

Which IT Projects Can PST Files Impact?

Office 365 Migration

Where organizations are looking to move the overhead of their office applications to Microsoft's online platform, PST files should be considered either as part of that migration or certainly straight after. Consolidating all email data into the online Exchange environment will not only enhance the end user experience and productivity but also ensure that any legacy email data is protected.

Desktop Refresh

When considering a refresh to either new hardware or a virtual environment the impact of PST files should not be under estimated. They can be located anywhere in the desktop environment, and end users are likely to lose access to them if they are not identified and handled correctly. Without careful consideration a large amount of valuable business data could be at risk of being lost.

eDiscovery and eDisclosure

Situations may arise where an organization needs to identify all historical information (including emails) that is relevant to a particular issue or request. In this situation email contained within PST files is difficult to identify and retrieve because the location of the files may not be known or their contents are available only to their end-user.

Corporate Compliance

Best practice is often jeopardized by PST files because they typically contain emails which should be managed according to corporate compliance policies, but have fallen outside the scope due to their location. It is important to note that Defensible Compliance dictates that all known sources need to have a consistent policy applied to them.

How Big is the PST Problem?

Across the organizations we work with, we see an average of between two and four PST files per active mailbox, ranging in size from a couple of Megabytes up to many Gigabytes.

A typical PST file may contain 10,000 individual messages with attachments, which normally represents around 1 GB of data. In storage terms this doesn't sound like a lot, but multiply this by the number of mailboxes and triple that figure (with the average number of PSTs per mailbox being three) and the scale of the problem can be seen.

Consider too that these emails may contain business critical data such as supplier contracts, customer orders and research data, so the size of PST files is not always the biggest problem. In practice most enterprises have thousands of PSTs littered throughout their infrastructure going unseen and unprotected.

How Do We Find Out if We Have a PST Problem?

The IT department will have a good idea if PST files exist with their organization, but the scale of the problem will be less clear.

An initial search will certainly give an indication of the problem, and this may be enough, but in our experience more information is required. For example, you will need to consider the actual data size compared to the on-disk size. You will also need to identify who owns the data in each PST file, which is especially important for all those lost or orphaned PSTs.

Once you have this information, careful consideration will need to be given as to what to do with each PST file.

Can IT Departments Manage PST Files?

Yes, with the right strategy and tools - although this does not mean that they are currently being managed. For a long time PST files have been the thorn in the side of IT departments. PSTs have served a purpose for many years for both the user and the IT department with either the associated risks to the business being invisible, or a blind eye being turned to the risks being taken.

IT administrators have several options available to them, including:

- Migrating the data back into Exchange or Office 365, then deleting them
- Moving them all to a central network server
- Ingesting the data into a third party archiving solution, then deleting them
- Simply living with the existence of PST files

Why Can't Users Manage Their Own PST Files?

By their very nature PSTs are created by the end-user, so it is therefore fair to say that by default the user has ended up managing them, but with varying degrees of success. The more alert user will have made ad-hoc copies of their PSTs on network shares or removable disks, which provides them with some level of backup or protection. But apart from the potential security risk this presents, it can also lead to data duplication.

So should users manage their PST files? The simple answer is no, they should not be burdened with ensuring business critical data is protected. This responsibility falls at the door of IT departments who are better equipped to do so.

Indiscriminate deletion of information could mean the organization falls foul of various laws if data pertaining to litigation or investigation is involved, resulting in fines and bad publicity.

What Tools Are Available for Managing PST Files?

A number of archiving solutions include embedded PST management tools, however these have limited functionality and offer varying degrees of success.

Organizations should consider the value of stand-alone PST Management tools. These range from Microsoft's free PST Capture tool to enterprise-class solutions such as Barracuda's own PST Enterprise, which can meet the demands of more complex PST migration projects.

Microsoft's Tool is Free – Is That Not Enough?

Microsoft have attempted to solve the problem with their PST Capture application, which addresses the challenges of legacy PST files by ingesting the data from these files back into the user's mailbox. The problem with this is that PST Capture doesn't scale to the typical size of PST problem that many larger companies face.

The Microsoft PST Capture tool is also only a partial solution, and requires a great deal of manual intervention. In particular it doesn't cover the work involved in finding and organizing PSTs, or deleting PSTs after they have been processed, so unless you are a company with less than 100 mailboxes, deployment of a third party solution such as PST Enterprise is advised.

What Features Should a PST Management Tool Provide?

Key features should include:

- Discovery of PST files wherever they exist across the organization, whether this is on local or network drives, or even on removable storage.
- Determining and assigning an owner for each PST file.
- Removing passwords from protected files.
- Migrating data selectively, based on the file contents or the age of the data.
- Providing a choice of target locations to move data to, such as to the primary or archive mailbox, to a network server, or to a third-party archive solution.
- Deleting files once they have been processed.

All these features should include a high degree of automation. In particular, locating PSTs on remote desktops and laptops is a time-consuming task, so the tool should automate this process without involving or impacting end users.

Can't PST Files Just be Deleted?

Many PST files are simply collections of old and obsolete emails which are candidates for deletion. However the PST file properties not only restrict access but also fail to provide details on what the file actually contains or how old the emails within it are.

An organization must consider whether it is prepared to live with the consequences of deleting these files without understanding the type and value of the information contained within them. In particular, if it has a corporate retention policy then it should ensure that it complies with this at an individual item level for each email within each PST file.

Which of Those Options is Best?

The choice will depend on the three key factors of risk, performance and cost:

RISK	PERFORMANCE	COST
How much value the historical data holds to your business. What risk is involved by deleting it without adhering to the corporate retention policies?	The impact on Exchange, the impact on your users and the impact on business working practices, particularly for users working remotely.	How much money can you commit to the project both in the short and long term with regards to storage and personnel?

These decisions are individual to each company, and will normally fall within the overall company retention and discovery requirements that facilitate governance and best practice.

The key is to have a consistent, automated, scalable practice that solves the problem, backed up by an audit trail of the activity.

Will the PST Problem Ever Go Away?

The latest versions of Exchange have better capacity management, and the need for PSTs has been negated with the addition of in place archiving. There is also the option of adopting third party archiving solutions, which allow organizations to better streamline and manage their email environments.

It is still important to consider historical PSTs and the data that resides within them. Ultimately, removing PST files will have a positive effect on all downstream processes, as well as eliminating much of the legal risk and uncertainty in unmanaged containers of email data sitting on your corporate servers and on end user machines.

The emergence of big data, and the realization by enterprises that to retain a competitive edge they need to be able to analyze and realize value from all their data, makes PST management a business driver and not just an IT requirement.

Conclusion – The Benefits of Managing PST Files

Reduce Risk

- Eliminate risks associated with unmanaged email data.
- Protect against end user and intellectual property data loss.
- Implement robust data retention and defensible deletion policies.
- Ensure compliance with Freedom of Information, Data Protection and other regulations.

Improve Performance

- Reduce backup and restore times for business-critical file servers.
- Quicker retrieval of centrally stored information.
- Remove obstacles for projects such as hardware upgrades, BYOD, VDI or Office 365 migration.

Reduce Costs

- Reduce IT support overheads.
- Streamline processes for eDiscovery and other disclosure requests.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.

US 1.1 • Copyright 2016 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008
408-342-5400/888-268-4772 (US & Canada) • barracuda.com