Fact Sheet: Archiving

Top Five Reasons Why PST Files Can Be an Information Management Risk

Overview

Microsoft® Personal Storage Table (PST) files multiply rapidly as users send and receive email messages, rely on their computers for calendar reminders, and perform other tasks in Microsoft Outlook®. Because these personal folders are stored on individual workstations rather than on a centralized server, they can present significant management challenges and business risks.

Here are five reasons why your organization should consider eliminating PST files.

1. PST files contain business-critical information, yet they are housed locally

The increasing need for organizations to retain, search, and retrieve enterprise email is being undermined by the use of PST files locally, which may contain:

- Personnel data
- Customer information
- Product and marketing plans
- Corporate financial data
- Other critical information

Having these PST files housed on end users' computers makes it almost impossible for corporate IT personnel to store, find, and manage the crucial business information contained in them.

2. PST files have a huge impact on storage and backup

Most users of personal folders have multiple copies of documents within their PST files. Multiply that situation by hundreds of messages per user, and hundreds or thousands of employees, and the impact on enterprise storage requirements is clear.

In addition, any opened PST file requires a full backup, even if the file has only been viewed. The combined size of all employees' PST files can easily reach hundreds of gigabytes, or even terabytes. Therefore, PST files also affect the capacity requirements and performance of enterprise backup servers.

3. PST files are prone to data loss or corruption

When their 2 GB maximum size is pushed to the limit, PST files have a propensity for data corruption. Unfortunately, they also have limited recovery capability, so corruption can result in permanent data loss.

Corruption of local or removable storage media containing personal folders can also result in a permanent loss of critical information if the files are outside of standard backup processes—a situation that is all too common with laptop computers.

Because of their portability, laptop computers housing PST files present another threat to enterprise security. A lost or stolen laptop can result in tactical and brand damage to your business.

Even when PST files are not completely lost, they can cause significant problems. An all-too-common scenario involves users contacting the help desk to save corrupted PST files, thus driving up IT support costs.

4. PST files can be an e-discovery nightmare

Information within a PST file is considered a business record and is thus subject to discovery requirements, just like email. However, the dispersed storage of personal folders makes it very difficult for organizations to safely identify and destroy documents that no longer need to be kept for legal or business reasons.

PST files also add to the cost and effort of litigation discovery. Administrators must ask individual users to manually identify email messages that are relevant to the litigation, put a hold on those messages, and then produce the specified files as needed for discovery. Because locally stored information is difficult to locate and collect, this manner of collection is labor-intensive and prone to errors. Further complicating the process, PST files usually contain substantial amounts of irrelevant or duplicate data. And their ad hoc nature can create pockets of unchecked data that may not be found until after the court's deadline for producing discovery materials.

All of those issues can result in sanctions and penalties when an organization is unable to fully comply with a discovery order.

---

5. PST files can elude enterprise retention policies

Ultimately, any organization that does not address the risk management issues of PST files is in danger of losing critical business information. Organizations that have a fixed data retention period (for example, 90 days), but also allow users to create PST files, inadvertently encourage ad hoc archiving. In these circumstances, individual users may decide to save their data for longer periods than specified by corporate policies. This unmanaged archiving makes it difficult to comply with regulatory requirements, and it could possibly subject your organization to charges of data spoliation (failure to adequately preserve electronic evidence) during litigation.

To fully control and manage corporate information, organizations need to review the usage and risks of personal folders, define a policy regarding their existing and future use, and implement and enforce that policy. Savvy companies are recognizing the benefits of a central archive such as Symantec Enterprise Vault™, which can not only eliminate the need for PST files, but also locate existing ones, ingest data from them that needs to be retained, and then delete the original files.

More information

About Symantec Enterprise Vault™

Symantec Enterprise Vault provides a software-based intelligent archiving platform that stores, manages, and enables the discovery of corporate data from email systems, file server environments, instant messaging platforms, and content management and collaboration systems. Because not all data is created equal, Enterprise Vault uses intelligent classification and retention technologies to capture, categorize, index, and store target data to enforce policies and protect corporate assets—all while reducing storage costs and simplifying management. It also provides specialized applications such as Discovery Accelerator and Compliance Accelerator to mine archived data in support of legal discovery, content compliance, knowledge management, and information security initiatives.

Visit our Web site

www.symantec.com/enterprisevault

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Confidence in a connected world. symantec.

1/08 13583251